A HOLISTIC, RISK, AND FUTURES BASED APPROACH TO DECEPTION: TECHNOLOGICAL CONVERGENCE AND EMERGING PATTERNS OF CONFLICT

Iain Douglas Reid

A thesis submitted in partial fulfilment of the requirements of the University of Lincoln for the degree of Doctor of Philosophy

February 2016

Abstract

Modern challenges in forensic and security domains require greater insight and flexibility into the ways deception can be identified and responded to. Deception is common across interactions and understanding how mindset, motive and context affects deception is critical. Research has focussed upon how deception manifests in interpersonal interactions and has sought to identify behaviours indicative of truth-telling and deceit. The growth of mediated communication has further increased challenges in ensuring information is credible. Deception in military environments has focussed on planning deception, where approaches have been developed to deceive others, but rarely examined from counter-deception perspectives. To address these challenges this thesis advocates a holistic approach to deception detection, whereby strategies will be tailored to match context. In accordance with an *in vivo* approach to research, a critical review of literature related to deception and related areas was conducted leading to the initial development of a theoretical holistic model of deception detection comprising a deception framework and an individual differences (deceiver and target) framework. Following model development, validation with Subject Matter Experts (SMEs) was conducted. Explanatory thematic analysis of interviews conducted with SMEs (n=19) led to the development of meta-themes related to the '*deceiver*', their '*intent*; '*strategies and tactics*' of deception, '*interpretation*' by the target and '*target*' decision-making strengths and vulnerabilities. These findings led to the development of the Holistic Model of Deception, an approach where detection strategies are tailored to match the context of an interaction, whether interpersonal or mediated. Understanding the impact of culture on decision-making in deception detection and in particular the cues used to detect deception in interpersonal and mediated environments is required for understanding human behaviour in a globalised world. Interviews were conducted with Western (n=22) and Eastern (n=16) participants before being subject to explanatory and comparative thematic analysis identified twelve cross-cultural strategies for assessing credibility and one culturally specific strategy used by Western participants. Risk assessment and management techniques have been used to assess risks posed in forensic and security environments; however, such approaches have not been applied to deception detection. The Deception Assessment Real-Time Nexus©2015 and Deception Risk Assessment Technique©2015 were developed as an early warning tool and a Structured Professional Judgement risk assessment and management technique. The Deception Risk Assessment Technique©2015 outlines multiple ways of identifying and

managing threats posed by deception and is employable across individuals and groups. In developing the futures-based approach to deception detection, reactive, active and proactive approaches to deception were reviewed, followed by an examination of scenario planning utility and methodology from futures and strategic forecasting research. Adopting the qualitative 'intuitive logics' methodology ten scenarios were developed of potential future threats involving deception. Risk assessment of two scenarios was conducted to show the value of a risk assessment approach to deception detection and management. In conclusion, this thesis has developed a Holistic Model of Deception, explored the links between interpersonal and mediated strategies for detecting deception, formulated a risk assessment and management approach to deception detection and developed future scenarios of threats involving deception.

Acknowledgements

I wish to thank my supervisors Dr Lynsey Gozna and Dr Julian Boon for all their support and encouragement throughout my studies, for developing my interests in deception, applied research, critical thinking and the need to understand what is truly psychological! Thanks to my research sponsors, the University of Lincoln, and in particular, to George Brander for his guidance and advice throughout my studies.

On a personal level I wish to thank my family, my parents Robert and Julie, my brother Alisdair, my dog Bracken (for the constant demands for attention and cuddles), and my grandparents Bob and May, Peter and Mavis and Connie for all their support and encouragement throughout my studies – the roast dinners were always a bonus! My friends back home in the south (looking at you Becca Harrison, my fellow aspiring academic!) and my friends across the School of Psychology and the wider PhD community at Lincoln for all the mutual support and adventures together.

Contents

List of Figures

List of Tables

Presentations

Reid, I. D., Gozna, L. F., & Boon, J. C. W. (2012). *Towards a Holistic Model of Deception Detection: The Challenge of the Cyber Chameleon*. Poster presented at the 2nd MILDEC Symposium, Cranfield University, UK, 7-8 November.

Reid, I. D. (2013). *Towards a Holistic Approach to Deception: Theoretical Developments.* Paper presented at the School of Psychology Postgraduate Research Conference, University of Lincoln, UK, 3 May.

Reid, I. D., & Gozna, L. F. (2014). *Lies and Deceit: Applying Thematic Analysis to Deception Research.* Poster presented at the University of Lincoln Postgraduate Research Conference, University of Lincoln, UK, 3 April.

Reid, I. D., Gozna, L. F., & Boon, J. C. W. (2015). *Deception and cyber-deception detection: Exploring the effect of culture.* Paper presented at Decepticon: International Conference on Deceptive Behavior, University of Cambridge, Cambridge, UK, 24-26 August.

Reid, I. D., Gozna, L. F., & Boon, J. C. W. (2015). *A holistic model of deception detection: Theoretical developments and practitioner applications.* Poster presented at Decepticon: International Conference on Deceptive Behavior, University of Cambridge, Cambridge, UK, 24-26 August.

Abbreviations

ACID – Assessment Criteria Indicative of Deception

ACH – Analysis of Competing Hypotheses

ACH-CD – Analysis of Competing Hypotheses – Counter-Deception

ACH-SL – Analysis of Competing Hypotheses – Subjective Logic

APA – American Psychiatric Association

BPD – Borderline Personality Disorder

CAI – CHAMELEON Approach to Interviewing

CAPP – Comprehensive Assessment of Psychopathic Personality

CBCA – Criteria Based Content Analysis

CBRN – Chemical, Biological, Radiological and Nuclear

CI – Counter-Intelligence

CMC – Computer-Mediated Communication

CO – Chameleon Offender

COMINT – Communications Intelligence

DACP - Deception Analysis Cognitive Process

DARN – Deception Assessment Real-Time Nexus

DCDC – Development, Concepts and Doctrine Centre

DDT – Dangerous Decisions Theory

DSM-IV-TR - Diagnostic and Statistical Manual of Mental Disorders

DRAT – Deception Risk Assessment Technique

DRE – Differential Recall Enhancement

EI – Emotional Intelligence

F2f – Face-to-Face

HCR-20 – Historical-Clinical-Risk Management V^3

HMD – Holistic Model of Deception

HPD – Histrionic Personality Disorder

HUMINT – Human Intelligence

IDT – Interpersonal Deception Theory

IEDs – Improvised Explosive Devices

IMINT – Image Intelligence

IS – Islamic State

ISTAR – Intelligence, Surveillance, Target Acquisition and Reconnaissance

ISR – Intelligence, Surveillance and Reconnaissance

JOA – Joint Operations Area

JDP – Joint Doctrine Publication

LIWC – Linguistic Inquiry and Word Count

MO – Modus Operandi

MoE – Measures of Effectiveness

NPD – Narcissistic Personality Disorder

OCGs – Organised Crime Groups

OPSEC – Operational Security

OSINT – Open Source Intelligence

PIT – Prominence Interpretation Theory

PSYOPS – Psychological Operations

RI – Reality Interview

RM – Reality Monitoring

SAM – Stalking Assessment and Management

SIDE – Social Identity/Deindividuation

SMEs – Subject Matter Experts

SOCMINT – Social Media Intelligence

SPJ – Structured Professional Judgement

SUE – Strategic Use of Evidence

SVA – Statement Validity Analysis

TADMUS – Tactical Decision Making Under Stress

Chapter 1: Introduction

"*One who knows the enemy and knows himself will not be endangered in a hundred engagements*" – Sun Tzu

Introducing and Defining Deception:

Psychological research into deception has seen a large growth over recent decades and in particular since the start of the Twenty-First Century where greater emphasis has been placed on identifying deception to mitigate threats across forensic and security environments. Much of this research has focussed upon deception in interpersonal interactions with research into deception in mediated environments relatively neglected considering the impact of technology in everyday behaviour. In contrast research into military deception has arisen from studying historical incidences of deception and has sought to identify the key strategies and tactics which were used to deceive the target.

In order to study deception, deception must first be defined. In a common definition of deception taken from interpersonal deception research Vrij (2008, p. 15) defines deception as *"a successful or unsuccessful deliberate attempt, without forewarning, to create in another a belief which the communicator considers to be untrue"*. This definition covers a wide range of deceptive behaviours occurring in interpersonal interactions, whether the deception is low or high-stakes and acknowledges that an act may only be considered deceptive if it is deliberate rather than accidental. One proposed definition of online deception is "*the intentional control of information in a technologically mediated message to create a false belief in the receiver of the message*" (Hancock, 2009). Such a definition is readily applicable to mediated environments; however, the changing nature of communication may require a non-specific definition that can be applied across multiple domains. In defining deception related to the military, UK Joint Doctrine Publication 3-80.1 (JDP 3-80.1) defines deception as "*deliberate measures that manipulate the perceptions and condition the behavior of an opponent, in order to achieve and exploit an advantage*" (DCDC, 2007). JDP 3-80.1 states that the aim of the deception is not to deceive the adversary but to exploit the effect of deceiving the

adversary. However, this definition does not focus upon deception specifically and seems equally applicable to defining influence.

The current research revises the Vrij (2008) definition to define deception as *"a deliberate attempt, without forewarning, to create in another a belief which the communicator considers to be untrue, with the aim of influencing the receivers' mindset (manner of thinking structured by their attitudes, personality and culture) and/or behaviour".* This definition is applicable across interpersonal and mediated communication, whether the communication is verbal, paralinguistic, non-verbal or physical, and emphasises that the aim of deception is to change the receiver's behaviour through implanting or enabling the target to generate a false belief, ensuring applicability to online and military environments.

In strategic, operational and tactical environments there is a need to accurately identify deception to reduce threats posed to the UK and allies. Traditional and current approaches to deception have focussed primarily on identifying and increasing the number of cues indicative of deceptive behaviour within an interpersonal context (Granhag, Vrij & Verschuere, 2015). New approaches to deception detection focus upon eliciting behavioural differences between truth-tellers and deceivers (Granhag et al., 2015); however, 100% accuracy rates remain elusive and such approaches neglect the surrounding context under which deception occurs. Deception cannot be avoided, indeed deception will occur whenever and wherever adversaries are seeking an advantage (Bell, 2003; Whaley, 1982) therefore deception should be anticipated as occurring across a range of environments and greater understanding of how deception emerges and is responded to in complex environments is required. The need to prevent and manage potential conflict is discussed by Flavin (2013) and such an approach may be applied to deception where threat from deception may be prevented through its detection by a variety of techniques. Potential deception may be further managed through monitoring or actively looking for further behaviour to confirm or refute adversary deception.

Scientist-Practitioner Model:

The scientist-practitioner model is founded on the premise that trained practitioners should be knowledgeable in both research and practice (Douglas, Cox & Webster, 1999; Jones & Mehr, 2007). Adapting this approach to forensic and security environments there is a strong requirement that research is shaped by practitioners'

requirements, and that their practice is subsequently informed by research. There are three key assumptions of the scientist-practitioner model (Jones & Mehr, 2007). The first assumption is that practitioners with skills and knowledge related to research will be effective in their performance (Jones & Mehr, 2007). The second assumption is that research is key to the construction of a scientific database (Jones & Mehr, 2007). The final assumption is that direct involvement in practice by researchers will result in studies on important social issues (Jones & Mehr, 2007). Practitioners should use validated methods of assessment where such methods exist, if they do not then the practitioner should apply scientific principles to develop or improve the efficiency of methods to address challenging behaviour (Shapiro, 2002). The scientist-practitioner model was initially developed for the treatment of adults with mental health problems (Shapiro, 2002), but this model is readily transferrable to understanding challenging human behaviour across applied settings (Gozna & Prendergast, 2008) making it particularly useful for the application of psychological approaches to deception in military environments.

Applying Social Science to Defence Science:

The application of research into deception and its detection from social and behavioural sciences to defence science is required to increase understanding and capabilities in defence environments. Through adopting an *in vivo* holistic approach (Boon & Gozna, 2009) focussing on a wide-range of human behaviours and surrounding contexts, a greater theoretical and practical input may be made towards understanding the deception process in defence science.

Psychological research has begun to generate further understanding of how deception is conducted (Henderson, 2007, Henderson et al., 2007; Henderson & Lee, 2008) and how deception may be countered in military environments (Helman, 2007; Henderson & Pascual, 2008; Smith, Johnston & Paris, 2004). Whilst research in investigative interviewing has sought to aid human intelligence (HUMINT) interviewing in military environments to improve the quality of information generated and reduce reliance on controversial and ineffective interrogation tactics (Evans, Meissner, Brandon, Russano & Kleinman, 2010; Fallon, 2014). The current research applies psychological research to develop a model of deception applicable to interpersonal, online and military environments.

Overview:

The thesis introduces the topic of deception and the challenges of detecting deception in a world where communication is interchangeable between in-real-life and online modes, across strategic environments. A theoretical model of deception is then presented to the reader, followed by its refinement and validation by Subject Matter Experts (SMEs), the development of scenarios of potential future threats involving deception, and the development of a screening tool and risk assessment and risk management tool.

A review of the literature surrounding interpersonal deception (see Chapter 2) explores theories of deception; the strategies which individuals, whether truth-tellers or deceivers, use to appear credible to others; why individuals are argued to be poor at detecting deception due to the cues used to detect deception, decision-making biases and the countermeasures which individuals use; methods of detecting deception across verbal, and non-verbal behaviour, differential recall enhancement (DRE) approaches; the effect of personality and individual differences on deception; the impact of culture on deception; holistic approaches to deception; and the application of the CHAMELEON approach towards deception.

Online deception research had been relatively neglected over the past two decades considering the widespread usage of technology in everyday behaviour. A review of the literature on online deception (see Chapter 3) discusses forms of and motives for online deception; theories of online communication and impression formation and how these may differ from in-real-life; how deception may be detected online, including the effect of culture; and adversary behaviour online.

A review of the literature surrounding military deception (see Chapter 4) examines taxonomies of deception and the deception planning process; the importance of understanding the target of deception; historical examples of how deception has successfully been used; decision making biases effecting military deception detection; and detecting military deception.

Following the review of relevant literature a theoretical holistic model of deception was developed (see Chapter 5), this model was then validated and refined through interviews with SMEs (see Chapter 6) resulting in a holistic model of deception examining the deceiver, their intent, the tactics used to deceive others, how information is interpreted by the target, and key characteristics of the target. As global societies become increasingly connected in in-real-life and online interactions, there is

a growing need for understanding how individuals across cultures make credibility judgements and the processes involved in making such judgements (see Chapter 7).

A new approach to deception and its mitigation is outlined, where deception is examined from a risk perspective (see Chapter 8). Such an approach is highly relevant for deception in strategic environments with multiple forms of deception occur. Through identifying adversary attempts at deception then steps may be taken to increase resilience against threat. To date deception detection has focussed upon simply identifying when deception is occurring in interactions and the development of techniques to aid this process. Such approaches have focussed upon the interaction outside of the surrounding context from which deception occurs. Future threats affecting UK interests may emerge from the increase in global uncertainty and a more proactive approach to deception detection is required to deal with such challenges (see Chapter 9). The implications of this thesis are discussed and recommendations made for further development of a risk assessment approach to deception (see Chapter 10). The aims of this thesis are:

- To develop a Holistic Model of Deception, that will be applicable across interpersonal, online and military environments.
- To explore cultural similarities and differences in how credibility is assessed in-real-life and online environments, and increase understanding in potential vulnerabilities in these strategies.
- To develop a screening tool for deception that can be applied in strategic environments, and once a potential threat is detected will lead to a full-scale risk assessment of deception and the deployment of risk management strategies to counter any identified threats.
- To develop a proactive approach to deception detection through designing risk management strategies that are applicable to future threat scenarios.

Chapter 2: Interpersonal Deception.

Introduction:

The field of interpersonal deception research examines behaviours across forensic and non-forensic environments. In summary, research to date has sought to examine the strategies individuals use that enables them to maintain credibility whilst deceiving, the ability of practitioners in detecting deceit, verbal, non-verbal, and physiological deception detection and more recently, holistic approaches to improve deception detection ability across a range of practitioner groups.

In everyday life people automatically use small lies requiring little cognitive effort to create favourable impressions, avoid embarrassment and maintain social interactions (Bond & DePaulo, 2006). Serious lies are usually associated with protecting an individual's reputation and involve a greater cognitive effort (Bond & DePaulo, 2006; Vrij & Mann, 2004) and are relevant when considering the motivation of a range of individuals and groups who may hold malign intent or wish to manipulate the impression they present to a particular audience. To compound the difficulties of lie detection there are no identifiable verbal, non-verbal or paralinguistic behaviours that are direct signs of deceit (Ekman, 2001) although some behavioural leakage may suggest that a person is committing an act of deception.

One challenge has been the low levels of deception detection accuracy identified by numerous studies (Ekman & O'Sullivan, 1991; Hartwig, Granhag, Strömwall & Andersson, 2004; Hartwig, Granhag, Strömwall & Kronkvist, 2006; Porter, Woodworth & Birt, 2000), with overall accuracy approximately 54% (Bond & DePaulo, 2006). However, artificial laboratory conditions in addition to populations which are largely university students cannot reflect the reality of detecting deception in high-stakes environments (Boon & Gozna, 2009; Park, Levine, McCornack, Morrison & Ferrara, 2002; Van Koppen, 2012).

Theories of Deception

Deception in interaction has been presented via two main theoretical approaches: firstly, Zuckerman, DePaulo and Rosenthal (1981) argued that liars are affected by arousal, emotions, cognitive load and they will attempt to control their behaviour; and secondly, Interpersonal Deception Theory (IDT - Buller & Burgoon, 1996) states that displays of emotion may not be so apparent in conversational

interactions where the deceiver and receiver adapt their behaviour according to conversational changes. For example, liars may increase their verbal and non-verbal involvement throughout conversation to appear more credible (Burgoon, Buller, White, Afifi & Buslig, 1999). Deceivers may respond to target suspicions and adapt their behaviour to appear more truthful, although this may prove more difficult in online environments (Burgoon, Buller & Floyd, 2001; Burgoon & Qin, 2006).

Deceivers' Strategies

Impression management involves the regulation by deceivers and truth-tellers of verbal and non-verbal behaviour to create and communicate a favourable impression to others (Hartwig, Granhag, Strömwall & Doering, 2010). Regardless of intent to deceive, individuals require such abilities to appear credible (DePaulo, 1992). Individual differences will influence how we appear to others, for example, people who are more expressive and confident appear more favourable to others (DePaulo, 1992). Ultimately there is a high level of skill involved in presenting emotions that people are not really feeling (DePaulo, 1992).

Deceivers and truth-tellers are assumed to engage in different cognitive processes to appear credible, manage and report events, and that deceptions are outright fabrications (Leins, Fisher & Ross, 2012). In interviews, liars need to provide enough detail to make their story sound plausible but avoid suspicion (Hines et al., 2010). Liars are more likely than truth-tellers to have prepared strategies to appear honest in interviews (Hartwig et al., 2010; Strömwall, Hartwig & Granhag, 2006; Vrij, Mann, Leal & Granhag, 2010), whereas truth-tellers believe their innocence will be identified by 'telling the story how it happened' (Hartwig, Granhag & Strömwall, 2007). Through keeping an account simple (Hartwig et al., 2007; Hartwig et al., 2010; Strömwall et al., 2006) liars supply fewer details than truth-tellers (Strömwall et al., 2006), reducing anxiety and cognitive demand in recalling events and decreasing chances of contradicting or incriminating themselves (Dando & Bull, 2011; Hartwig et al., 2007; Hines et al., 2010; Vrij, Mann, Leal & Granhag, 2010).

Deception strategies identified in research examining mock suspects included keeping the statement detailed, consistent, avoiding lying, denying guilt, playing the role of innocent and pleasant and unrehearsed and no hesitation (Hartwig et al., 2007; Strömwall et al., 2006). When asking liars to use their own strategies in 'recalling' an event, Leins, Fisher and Ross (2012) found that liars reported a previously

experienced event, followed by reporting a plausible story, reporting what people normally do and employed various other strategies which are not specified by the authors. The events that participants described from past experience were events they did frequently, recently and were routine or typical (Leins, Fisher & Ross, 2012). Such deceptive strategies appear to focus on presenting a credible image to the target, which may be effective in deceiving those unaware of such strategies. Truthful strategies relate to keeping statements realistic, telling the truth like it happened, firmly denying guilt, being cooperative, being spontaneous and coping with the uncertainty of the questions posed (Hartwig et al., 2007; Strömwall et al., 2006). Nonverbal impression management strategies for liars and truth-tellers (Strömwall et al., 2006) relate to reducing movement (Hartwig et al., 2007), maintaining eye contact (Hines et al., 2010), appearing calm and relaxed (Hartwig et al., 2007; Hines et al., 2010) and controlling vocal behaviour. However, real-life suspects have different motives and contexts for their actions and may use different strategies based upon different experiences and knowledge of the justice system and such strategies will change in mediated environments.

Experienced offenders may use different strategies to non-offenders in interviews to appear credible, including general verbal strategies, general nonverbal strategies and specific interview strategies (Strömwall & Willén, 2011). Principle strategies include staying close to the truth, information management and having no strategy. However offenders differ in their deception planning highlighting a distinction between the opportunities for careful planning versus a need to appear natural and spontaneous without having to risk forgetting a lie (Strömwall & Willén, 2011). Furthermore, some offenders chose not to disclose information to force the interviewer to divulge evidence thereby assisting the offender's realistic narrative. This suggests that real-world suspects may use strategies learned from previous encounters with the justice system emphasising the need for real-world research.

Why people are bad at detecting lies

There are 'wizards' of deception detection who are experts at detecting deceit across different situations and behaviours with approximately 80-90% accuracy (O'Sullivan & Ekman, 2004); however deception detection accuracy for the majority of people, including professionals, is mainly poor at approximately 54% accuracy (Anderson, DePaulo & Ansfield, 2002; Bond & DePaulo, 2006; Hartwig, Granhag,

Strömwall & Vrij, 2004). Bond and DePaulo (2006) claim that deception detection studies with accuracy rates higher than 70% may actually be subject to natural variance. However, the majority of studies examining deception detection have used artificial paradigms that do not reflect real-world interactions and strategies used to detect deception, thus behavioural cues to deception related to high-stakes environments may not be aroused (Helman, 2007), potentially distorting actual ability to detect deception creating an apparent level of chance. Deception research generally fails to consider lies that remain undetected – resulting in an overgeneralisation of those cues that are identified as indicative (Colwell, Miller, Miller & Lyons, 2006; Hartwig, Granhag, Strömwall & Andersson, 2004). Furthermore, it may be hard to accurately assess veracity due to the complex nature of deception, lack of distinctions between overt truths and overt deceptions (Bond & Speller, 2009) and cognitive and heuristic biases in decision-making (DCDC, 2007; Henderson et al., 2007).

Cues to Deception

Many cues assumed to be indicative of deception are often not or there are only weak links between behaviour and cues (Anderson et al., 2002; Colwell et al., 2006; Davis & Markus, 2006; Hartwig & Bond, 2011; Helman, 2007) and these may be hard to accurately distinguish in real time (Helman, 2007). Genuine cues to deception are few whilst perceived cues to deception are identified and generalised to deceptive behaviours even when irrelevant (DePaulo & Morris, 2004). Further, perceived audio/visual cues are more confidently assessed even when incorrect (Davis & Markus, 2006).

The accuracy of lie detection appears to be based upon the predictability of a person's actual and perceived deceptiveness gained from behavioural cues and matches of cue-based predictions of actual and apparent deception (Hartwig & Bond, 2011). The authors identified a strong correlation between perceived cues to deception and actual cues to deception, suggesting that, in contrast to previous research, people rely on the right cues. Rather there is a general lack of valid behavioural cues to deception. However, this meta-analysis was conducted primarily on low-stakes laboratory research where high-stakes deception cues may not be elicited and these findings may not reflect strategies that people really use to detect deception (Park et al., 2002).

Decision-Making Biases

Decision-making biases affect our ability to accurately assess veracity. Truth biases can result in suspicious beliefs not being acted upon (Bond & DePaulo, 2006; Granhag & Strömwall, 2000) and misattribution of received information (O'Sullivan, 2003) and conversely lie biases can result in negative confirmation bias (Granhag & Strömwall, 2000; Hartwig, Granhag, Strömwall & Andersson, 2004). Further demeanour biases also affect credibility judgements (Bond & DePaulo, 2006; Hurst & Oswald, 2011; Masip, Garrido & Herrero, 2004). In forensic and military domains there is a heightened awareness of deception to counter risk suggesting potential for biases.

Intuition can impede accurate decision making (Porter & ten Brinke, 2008b; Porter, England, Juodis, ten Brinke & Wilson, 2008) however this will depend largely on the skill of the person identifying deceit. Dangerous Decisions Theory (DDT; Porter & ten Brinke, 2009) proposes that judgements of trustworthiness occur almost instantaneously when we view a new face (ten Brinke & Porter, 2011b; Willis & Todorov, 2006), and this is subjectively experienced as intuition, although these judgements may be incorrect. Short interactions may not enable the establishment of baseline behaviour to judge deception and result in intuition effecting judgements (ten Brinke & Porter, 2011b). Intuition in judgements may have developed from strategies assessing danger and 'fight or flight' responses (Cannon, 1915). This creates challenges for making judgements of credibility and requires further evidence to be gathered to effectively gauge an individual's behaviour on first exposure.

Motivation for detecting deceit affects the accuracy of veracity judgements with motivated individuals performing poorly compared to less motivated counterparts (Porter, McCabe, Woodworth & Peace, 2007). This appears to be the result of high motivation leading to reliance on stereotypical nonverbal rather than actual verbal cues to deception, although this may be overcome through providing feedback on genuine cues to deception (Porter et al., 2007).

Methods of detecting deception

In principle there are three different ways to measure if someone is lying: their verbal behaviour; their non-verbal and paralinguistic behaviour; and their physiological behaviour (Granhag et al., 2015). For the purpose of the present

research, only that which is relevant to interpersonal and online interactions is considered and discussed.

Verbal Deception Detection

Verbal deception detection can apply to a range of interactions, whether interpersonal or online, thus techniques may be transferrable to military contexts. Techniques include Statement Validity Analysis (SVA), Reality Monitoring (RM), Linguistic Inquiry and Word Count (LIWC), and more recent approaches focussing on plausibility and detail of narrative.

SVA is used to assess the veracity of statements and focuses on behaviours that truth-tellers are more likely to perform than deceivers (Rassin, 2000). SVA involves a review of relevant information, a semi-structured interview, CBCA and a Validity Checklist which assesses the validity of the CBCA findings (Akehurst, Manton & Quandte, 2011; Brown, 2010; Vrij, 2008 - See Appendix 2.1 for an overview of CBCA criteria). Akehurst et al. (2011) found that in truthful accounts CBCA criteria most often seen were: admitting a lack of memory, unstructured production and contextual embedding. Level of support for CBCA criteria varies, for example, unstructured production, contextual embedding, quantity of details, and reproduction of conversation appear in more than half of studies involving CBCA (Porter & ten Brinke, 2010). Limitations to SVA include: scoring, reliability of criteria, establishment of ground truth, effects of interview style on inclusion of CBCA criteria, lack of a standardized training program (Akehurst et al., 2011; Brown, 2010; Vrij, 2005), vulnerability to countermeasures (Vrij, 2005; Vrij, Kneller & Mann, 2000), an awareness of individual differences and personality, and allegations that misidentify the perpetrator or mix deception and truth are harder to identify (Vrij, 2005).

RM proposes that recollections of real experiences are developed from perceptual processes and are more likely to have aspects of perceptual, contextual and affective information, whilst recollections of false experiences developed from our imagination will be cognitive in nature and focus on our thoughts and reasoning enabling a distinction between truthful and deceptive accounts (Bond & Lee, 2005; Masip, Sporer, Garrido & Herrero, 2005; Sporer, 2004; Vrij, 2008 - See Appendix 2.2

for an overview of RM criteria). RM has shown similar levels of deception detection accuracy to SVA, however, it also has similar limitations and may be vulnerable to countermeasures, age and personality traits (Colwell, Hiscock-Anisman & Fede, 2013). Colwell et al. (2013) argue that differences between truthful and deceptive accounts are due to interviewing techniques rather than RM theory and differences between real and imagined events may dissipate over time (Johnson, Foley, Suengas & Raye, 1988). This has relevance for the investigation of crimes that become 'cold case reviews' where historical evidence is relied upon and relevant suspects and witnesses are interviewed years following an event.

LIWC (Pennebaker, Booth & Francis, 2007) is a technique for analysing conversations in order to understand people's underlying thoughts, motives and emotions (Newman, Pennebaker, Berry & Richards, 2003). LIWC categorises words into dimensions of standard language, psychological processes, principles of relativity, and personal concerns (Bond & Lee, 2005). In deceptive statements elements that enable differentiation from truth are a reduction in self-reference, references to others, number of exclusive words, an increase in motion words and negative emotion words (Bond & Lee, 2005). However there is a requirement for further work into the validity and reliability of LIWC to ensure that it is an effective method for detecting deception in on and offline verbal content.

Non-Verbal Deception Detection

Non-verbal deception detection methods focus on a consideration of facial expressions, micro-expressions (Ekman, 2001), and arm, hand and finger movements (DePaulo et al., 2003); however, non-verbal cues are potentially rare and do not guarantee deception. Instead confirmation is required that cues are related to deceit rather than other cognitive and emotional processes.

Micro-expressions are facial expressions that are considered to appear for less than a quarter of a second and expose our true emotions (Ekman, 2001). A micro-expression may suggest that a person is manipulating their behaviour and may be deceiving. Detecting these expressions will be challenging in operational environments, for example, train stations, where expressions may be explained by a number of reasons and practitioners may have difficulty in accurately detecting these expressions (McGuffog, Green & Crombie, 2004). Porter and ten Brinke (2010)

report variations in the occurrence of facial expressions, with some expressions appearing in the upper or lower face, some emotions easier to fake than others, micro-expressions showing for longer than anticipated, occurring more in high intensity emotional displays, appearing in truthful and deceptive accounts and less frequent than anticipated (Porter, Korva & Baker, 2011; Porter & ten Brinke, 2008; Porter, ten Brinke & Wallace, 2012; ten Brinke, MacDonald, Porter & O'Connor, 2011; ten Brinke & Porter, 2011a). It is likely that individual differences will occur in the ways such expressions manifest across people and there may be numerous mitigating factors explaining a facial expression (Porter et al., 2012).

Increased cognitive load may lead to a reduction in illustrators (DePaulo et al., 2003; Frank, 2007; ten Brinke & Porter, 2011a), which may make deceivers appear tense (DePaulo et al., 2003) whilst truth-tellers will increase their illustrators to emphasise their verbal content (Navarro, 2003) although a reduction in bodily movement to counter stereotypes regarding liar's nervous fidgeting enhances credibility (Porter & ten Brinke, 2010). It is unclear whether non-student groups exhibit greater or fewer illustrator cues to deception (Porter & ten Brinke, 2010). Offenders may increase self-manipulators during fabricated stories suggesting that deceivers' usage of these behaviours is context dependent or a strategy to distract receivers from verbal content (Porter et al., 2008). It is important to understand the baseline of normal behaviour before we can make judgements about deception based upon changes in non-verbal behaviour.

Differential Recall Enhancement (DRE) Approaches

DRE (Colwell et al., 2013) approaches focus on maximising behavioural differences between liars' and truth-tellers through the use of cognitive mnemonics, questioning strategy and use of evidence, for example, ACID (e.g. Colwell et al., 2013), SUE (e.g. Hartwig et al., 2006), and cognitive approaches (e.g. Vrij, Mann, Leal & Fisher, 2010). DRE helps truth-tellers to remember and provide more detailed and verbose statements whilst deceivers work harder to maintain credibility and over rely on short, carefully constructed narratives (Colwell et al., 2013). The mnemonic section of investigative interviewing increases deception detection accuracy by 10 to 27 % (Colwell et al., 2013), although it may be limited in application to online and military environments, whilst requiring evidence to challenge suspects' narrative.

The cognitive load approach seeks to increase behavioural differences between liars and truth-tellers through asking cognitively demanding and unanticipated questions to circumvent deceivers' preparations (Granhag & Vrij, 2010; Vrij et al., 2009; Vrij, Granhag et al., 2011a). Cognitively demanding questions have focussed on reverse order recall (Vrij, Leal, Mann & Fisher, 2011; Vrij, Mann, Fisher, Leal, Milne & Bull, 2008) and maintenance of eye contact (Vrij, Mann, Leal & Fisher, 2010). Unanticipated questions have focussed on sketch drawing (Leins, Fisher & Vrij, 2012; Leins, Fisher, Vrij, Leal & Mann, 2011; Vrij, Leal, Mann, Warmelink et al., 2010; Vrij et al., 2009), spatial questions, temporal questions and planning (Vrij, 2015b) and the Devil's Advocate approach (Leal, Vrij, Mann & Fisher, 2010) to enhance behavioural differences between truth-tellers and liars. However, automatic assignation of participants to lying and truth-telling conditions and provision of alibis for deceivers may reduce motive and context for their actions. As these techniques affect both verbal and non-verbal behaviours it suggests that they can be applied to examining multiple-cues to deception, although validation in applied settings is required. Exploring how countermeasures may affect these approaches is also required. For example deceivers put forward convincing false beliefs and this may be hard to detect, as seen by the history of 'green' on 'blue' attacks in Afghanistan (DeAnda, 2012) and testimony related to the July 7th bomber who was able to appear 'normal' to a school friend days before the attack (Boon, 2012).

The SUE approach attempts to counter suspects' strategies by allowing suspects a period of free recall before challenging them with varying strengths of evidence which may highlight inconsistencies in suspects' accounts (Hartwig et al., 2011; Hartwig et al., 2007; Hartwig et al., 2006). Stepwise revelation of evidence requires liars to adapt their narrative to incoming evidence sacrificing within-statement consistency to maintain statement-evidence consistency, revealing cues to deception (Granhag, Strömwall, Willén & Hartwig, 2012). In real-world interviews suspects may use strategies based upon knowledge of the criminal justice system, suggesting that SUE requires further validation in applied settings to ensure viability.

Tactical interviewing of suspects (Dando & Bull, 2011) builds on the SUE approach by examining which strategy of information disclosure during an interview is most effective in increasing behavioural differences between liars and truth-tellers (early, tactically or late). Dando and Bull (2011) found that tactical interviewing enables interviewers to more accurately make veracity assessments and interviewees

found the tactical interview more cognitively demanding than control and strategic interviews, whist disrupting deceiver's narratives (Dando & Bull, 2011). However, this approach has similar criticisms to that of SUE and may have limited applicability to online and military domains.

The ACID approach analyses the admittance of potential errors, the length of responses and RM criteria associated with differences due to memory, impression management, and unique contextual and internal/external details as they appear during a US police investigative interview (Colwell, 2007; Colwell et al., 2013). The Reality Interview (RI) emphasises increasing the interviewee's cognitive load to elicit cues to deception and challenging impression management strategies (Colwell, 2007; Colwell, Hiscock-Anisman, Memon, Taylor & Prewett, 2007). The ACID approach has been shown to accurately classify 86.8% of statements (78.9% truthful and 94.7% deceptive) (Colwell, 2007; Colwell, Hiscock & Memon, 2002). The credibility assessment aspect of ACID found that deceptive statements are shorter, less detailed and had fewer details in response to the mnemonic parts of RI, whilst honest statements were longer, more detailed, contained more affective details and had more details in response to the mnemonic parts of RI, and honest reporters were also more likely to admit possible error (Ansarra et al., 2011; Colwell, 2007; Colwell et al., 2007). The type-token ration (TTR) is the ratio of unique words in a statement to the total number of words in a statement, with the premise that liars use more unique words to enhance their credibility, whilst truth-tellers have fewer (Morgan, Colwell & Hazlett, 2011; Suckle-Nelson et al., 2010). Colwell et al. (2013) state that ACID will not work when questioning people about their attitudes, future intentions, what a person may be hiding, and when the respondent actually believes or is mistaken in what they are saying. One limitation is that the research engaged in so far has been laboratory based (Colwell et al., 2013), suggesting that ACID needs to be validated in applied settings.

Personality and Individual Differences and Deception

The acceptance and likelihood of engaging in forms of deception may be based on exclusive or multiple personality traits (McLeod & Genereux, 2008). In a holistic approach to deception there is a need for understanding personality traits and disorders and individual differences as these affect how people lie, the situations they

lie in, and motives for lying (Gozna, Vrij & Bull, 2001) and how people detect deception.

Social skills impact on deception with socially skilled people more expressive verbally and non-verbally in their truth-telling and lying, more involved non-verbally regardless of whether they are lying or telling the truth (Burgoon et al., 1999) and are faster in their response time to open-ended questions than less socially skilled liars but are still slower than truth-tellers (Walczyk et al., 2005). Liars with greater skills in encoding their behaviour are able to maintain a greater control over their behaviour when they are lying, and they are able to adjust their conversational involvement to mimic their interactional partner (Burgoon et al., 1999).

There are disorders related to deception, pathological lying and instrumental gain that need to be considered by practitioners as potential explanations for suspects' motives and behaviour (Taylor & Gozna, 2011). Psychopathy (Cleckley, 1982: Hare, 1970), Narcissism (Raskin & Hall, 1979) and Machiavellianism (Christie & Geis, 1970) are three personality constructs that form what has been termed The Dark Triad (Paulhus & Williams, 2002). When interacting with psychopaths it is important to realise that underneath their charm they may be deceiving you (Taylor & Gozna, 2011). Although psychopaths may be identified by thin-slices of behaviour (Fowler, Lilienfeld & Patrick, 2009), in interpersonal interactions they employ countermeasures to circumvent these initial impressions (ten Brinke & Porter, 2011). Those individuals suffering from Narcissistic Personality Disorder (NPD - Raskin & Hall, 1979) are more likely to lie and exaggerate their status and importance as they are obsessed with a fantasy that they are trying to create in reality (Taylor & Gozna, 2011). Manipulativeness and Machiavellianism are associated with more frequent acts of deception often committed for self-gain (Kashy & DePaulo, 2008; McLeod & Genereux, 2010). In everyday and high-stakes deception environments, such personality traits are further associated with little guilt and mental effort (Gozna et al., 2001). Conduct disorders involve physical aggression towards people and animals, destruction of property, and serious violations of rules and people diagnosed with conduct disorders are more likely to engage in deceptive practices (Taylor & Gozna, 2011). People with borderline personality disorder (BPD) may potentially manipulate others around them (Navarro, 2011b), whilst people with histrionic personality disorder (HPD) will lie to further their aims and their recollections are often biased by their own representations of reality (Navarro, 2011c), therefore, there is a need to

understand personality and challenging behaviour to ensure a robust response to deception.

There are individual differences in deception detection abilities (Aamodt & Custer, 2006; Baker, ten Brinke & Porter, 2012; Porter, Campbell, Stapleton & Birt, 2002; Vrij & Baxter, 1999). Teachers, social workers, secret service agents, psychologists and judges are deemed better at detecting deception than students; however this requires confirmation in applied settings (Aamodt & Custer, 2006). People high in emotional intelligence have been found to be more accurate in detecting deception than those who are not suggesting that they are less susceptible to deceiver's impression management strategies (Baker et al., 2012). More socially anxious and shy participants are less confident in their ability to detect deception than extraverted people (Vrij & Baxter, 1999) although there is no link between the Big Five personality traits in judges and the ability to accurately detect deception (Porter et al., 2002).

Culture and Deception

The impact of cultural differences on ability to deceive and to detect deception is critical in the globalised world. Deception is an evolutionary trait found in varying forms in every culture in the world (Bond & Rao, 2004). Different cultures have different beliefs regarding deception; for example, amongst Arabic people deception is acceptable if an individual is seeking societal approval (Al-Simadi, 2000). When people are communicating in different languages their ability to detect deception will be affected by language and it is hard to analyse whether this will benefit the deceiver or the target (Bond & Rao, 2004; Cheng & Broadhurst, 2005).

Beliefs about and incidences of deception may have similarities and differences across cultures (Bond & Rao, 2004). For example, the belief that liars are more likely to avoid eye contact is reported globally (Global Deception Research Team, 2006). Individuals across cultures believe that liars are more likely to: make speech errors, including pauses and stuttering; show signs of nervousness; show signs of inconsistency in their verbalisations, verbal-non-verbal inconsistencies, and statement-evidence inconsistencies (Bond & Rao, 2004). Highlighting, that across different cultures people have both correct and incorrect beliefs about how to detect deception. Group membership and situational influences were not mentioned as cues

to deception (Bond & Rao, 2004), however these are part of the context under which acts of deception can arise.

Cognitive load approaches to deception detection have also sought to detect deception in those from other nations and cultures (Colwell et al., 2013; Hazlett & Morgan, 2009; Morgan, Mishara, Christian & Hazlett, 2008; Morgan, Rabinowitz, Kallivrousis & Hazlett, 2010). ACID has been found to detect deception in Arabic, Spanish and English from a range of cultures and has found similar impression management strategies in English and Chinese speakers (Colwell et al., 2013). Morgan et al. (2008) found that truthful and deceptive Arabic speakers could be successfully identified through focussing on unique word count and response length in automated analysis of translated statements. Forced-choice questioning has also led to accurate identification of truthful and deceptive Russian and Vietnamese speakers (Hazlett & Morgan, 2009; Morgan et al., 2010). The success of cognitive approaches to deception detection in individuals from other cultures suggests that DRE techniques examine a basic level of human memory and cognition (Colwell et al., 2013).

Holistic Approaches:

Previous approaches to deception detection are limited as they have focussed on weak and isolated cues to verbal, non-verbal and paralinguistic behaviours that may indicate deception but may also indicate other forms of emotional and cognitive arousal. Furthermore, research has focussed largely on the act of deception in experimental conditions and has neglected real-world motives and contexts (Van Koppen, 2012), background personality and individual differences (Boon & Gozna, 2009), and the impact of culture. People are potentially not good at detecting lies in experimental situations (Park et al., 2002) and genuine cues to deception in experimental situations are weak (Hartwig & Bond, 2011). In seeking to detect deception it may be more beneficial to examine clusters of cues to deception alongside a comparison of such behaviours to baseline behaviours and incongruities between verbal and nonverbal behaviours to ensure that a more holistic view of veracity is produced (Aamodt & Custer, 2006; Ekman, 2001, p. 147; Granhag & Strömwall, 2004; Porter & ten Brinke, 2010; Vrij, 2008).

Multiple-cue approaches to detecting deception have combined verbal, non-verbal and paralinguistic cues to more accurately assess deception in high-stakes (Porter & ten Brinke, 2010; ten Brinke & Porter, 2011a) and low-stakes (Vrij, Akehurst, Soukara & Bull, 2004a; Vrij, Edwards, Roberts & Bull, 2000) environments. High-stakes lies should be easier to discern than low-stakes through their greater effect on an individual's psyche and cognitive process (Porter & ten Brinke, 2010). However, accurate veracity assessment in forensic contexts are often limited and individuals like psychopaths are almost 2.5 times more likely to be granted parole than other offenders due to their ability to deceive and influence others (Porter & ten Brinke, 2010). Ten Brinke & Porter (2011a) found that through combining verbal, non-verbal, and facial expression cues, 92.3% of genuine and 88.5% of high-stakes deceptive pleaders could be accurately identified. Whilst combining CBCA, RM and non-verbal cues to deception has enabled lie-truth discrimination of 80-90% accuracy in low-stakes environments (Vrij et al., 2000; Vrij, Akehurst et al., 2004a). In examining the reliability of rapid judgements of veracity based upon verbal and nonverbal behaviours, Vrij, Evans, Akehurst & Mann (2004) found that the observer's overall accuracy rate was 74%, and that quantity of details was the strongest predictor of veracity in rapid judgements, however, reproduction of conversation, visual details, and cognitive operations were also predictors of veracity. Using multiple cues to detect deception has been examined across both high and low-stakes environments suggesting that this technique should be incorporated into a holistic approach. Although these findings may be context specific and base-rates of behaviour may vary across individuals, suggesting that research into this area needs to incorporate these factors in credibility assessment.

When seeking to detect deception or even to deceive others there are a wide range of factors that need to be incorporated to understand how deception can be interpreted and identified (Kaina, Ceruti, Liu, McGirr & Law, 2011). In detecting adversary deception there is a need for understanding background history, culture, personality, cognition, surrounding environment and organisational and operational factors (Helman, 2007; Kaina et al., 2011), although further research is needed to more intricately explore the effect that these factors have on deception. Furthermore, as veracity assessment may be adversely effected in cognitively challenging and group decision-making environments (Kaina et al., 2011) decision-support tools are required to enhance deception detection.

The CHAMELEON Approach

The CHAMELEON Approach to Interviewing (CAI - Boon & Gozna, 2009; Gozna & Boon, 2010; Taylor & Gozna, 2011 – See Appendix 2.3) is a personality led investigative interview approach that takes into account a far wider breadth of information than traditional investigative interview approaches. In dealing with individuals it is acknowledged that every offender/suspect has the potential to be different from each other, to be different at different times, to behave differently with different people, to behave differently across different actions committed, to behave differently across different interviews, and to be different within each interview (Boon & Gozna, 2009; Gozna & Boon, 2010). Each Chameleon Offender (CO) will have different backgrounds, life experiences, attitudes, beliefs, offences and modus operandi (MO); each CO has the potential to vary in their cognitive ability, their affect and their cooperativeness at different times; each CO will behave differently with different interactional partners due to personal dynamics including, age, gender and socio-economic status and previous experience with people and their objectives; each CO will be different in their offences as not all victims respond in the same way, and circumstances including location, opportunity and interruptions will be different; each CO will be different within and across interviews due to how penetrative and subtle questions are, and the degree of incriminations as the interview progresses. When dealing with COs it is important to let them speak fully and not leap onto small mistakes, the longer an offender is left unchallenged for, the more likely they will overestimate their own cognitive ability and make mistakes (Taylor & Gozna, 2011). Work by Gozna and Boon has identified seven distinct chameleons (See Appendix 2.4 for an overview of the CHAMELEONS). The principles behind the CAI can be integrated into a holistic approach to deception through providing an awareness of the strategies that people use in attempting to appear credible and influence conversational partners, and this will be applicable to both interpersonal and online environments.

Conclusion

Past research has focussed on seeking out weak and isolated verbal and non-verbal behavioural cues to deception with more current approaches seeking to

increase behavioural differences between liars and truth-tellers through cognitive load and strategic questioning (Vrij & Granhag, 2012a), and others have begun to utilise multiple cues to deception to produce a more accurate assessment of veracity whilst re-examining assumptions regarding deception (e.g. Porter & ten Brinke, 2010). DRE approaches suggest that through increasing behavioural differences between liars and truth-tellers more cues to deception will be uncovered (Colwell et al., 2013), at first appearance these approaches seem to be effective in assessing veracity, however, much of this research has been conducted in laboratory environments using low-stakes paradigms where undergraduate participants have been automatically assigned to truth-telling or lying conditions suggesting that individuals lack motive and context for their actions. Further research validating these approaches in real-life high-stakes environments is required to ensure ecological validity.

Multiple cue and holistic approaches to deception may produce a more accurate understanding of deception and the context in which it occurs. These approaches can be further developed with the incorporation of the CAI (Boon & Gozna, 2009; Gozna, 2011; Gozna & Boon, 2007, 2010) and examining clusters of verbal and non-verbal behaviour within the wider context that individuals have different motives for different behaviours, across different situations, with different people, that different personality traits and disorders, and different cultures and religions may also effect whether a person may be lying or telling the truth and how easy it is to assess veracity. Furthermore, a holistic approach to deception needs to incorporate an understanding of the potential communication channels across which deception may occur (Porter & ten Brinke, 2010). In conclusion, a new approach to deception is needed that incorporates a far wider range of factors and elements than current approaches incorporate, alongside a greater understanding of the requirements that are needed and the challenges that occur in accurately assessing veracity in high-stakes environments.

Chapter 3: Online Deception and Influence

Introduction:

In the online world there are threats from deception whether through interpersonal interaction via computer-mediated communication (CMC), social engineering techniques (Lewis & George, 2008) or adversary attempts at influence (Cornish, 2008; Thomas, 2003). Increasing growth in the Internet, social media and communication technologies has led to an increase in deception in individuals' and groups' online interactions (Zhou & Zhang, 2006), with vulnerability potentially reflecting online usage (Vishwanath, 2015) and engagement with features alongside incorrect strategies for assessing credibility (Vishwanath, Herath, Chen, Wang & Rao, 2011). Deception in mediated environments, particularly text-messaging, is considered as an everyday behaviour where some individuals are argued to be more prolific in their deception than others (Smith, Hancock, Reynolds & Birnholtz, 2014). Although individuals may prefer to deceive in some face-to-face contexts (George & Carlson, 2010; Whitty, Buchanan, Joinson & Meredith, 2012), it is still important to understand how deception occurs in online environments as deception may increase when communicating online (Zimbler & Feldman, 2011).

Past research into deception detection suggests that people detect deception at chance levels (Bond & DePaulo, 2006), which presents challenges in cyberspace where increased anonymity challenges veracity assessment across interactions, statements, and identities (Cornish, 2008; Grazioli, 2004; Hancock, 2009). Deception detection accuracy in online environments is debated with some researchers arguing that there is no difference in detection accuracy between face-to-face and CMC interactions (Hancock, Woodworth & Goorha, 2010) and others arguing that mediated environments increase detection accuracy compared to face-to-face (Dunbar et al., 2013; Van Swol, Braun & Kolb, 2013). It may be that differences in findings are attributable to context and strategies used to detect deception, for example, deception is argued to be harder to detect in high-complexity situations, potentially due to an increase in cognitive load and reduction in situational awareness (Giordano & George, 2013). In online deception detection there may be potential difficulties due to limited applicability of traditional detection methods. However, some approaches may still be useful depending on context, for example, verbal methods may be applied to synchronous and asynchronous CMC; and non-verbal and verbal deception detection

methodologies may still be useful in analysing audiovisual content (Vrij & Mann, 2004). The current chapter builds upon Chapter 2 through expanding the examination of deception outside of interpersonal, offline interactions towards how deception manifests in online environments.

Forms of online deception:

In cyberspace there are a wide range of possible deceptions and a wide range of communication channels in which deception can occur. People use multiple levels of cyberspace for communication from synchronous or asynchronous CMC on messaging platforms, to video sharing, blogs, forums, chat-rooms, bulletin boards, and more recent forms of social networking (Cornish, Hughes & Livingstone, 2009). Deception may be identity-based where individuals manipulate aspects of themselves or message-based where the content of the message is manipulative or they may be combinations of both.

The most vulnerable aspect of a system to deception is individuals susceptible to influence as this bypasses computer security systems (Henderson et al., 2007; Thomas, 2008). There are several forms of social engineering used across both on and offline environments: pretexting, phishing; phone phishing, Trojan horses, road apple, quid pro quo (Thomas, 2008), page-jacking (Grazioli, 2004), piggybacking (or tailgating), impersonation, shoulder surfing, and dumpster diving (Henderson et al., 2007). Terrorist groups also create false charity groups to attract financing through deception (Jacobson, 2010; Thomas, 2003). Social engineers are argued to employ multiple influence tactics to gain advantage (Henderson et al., 2007 – See Appendix 3.1). Influencing targets to reduce their levels of risk resilience in online environments enables deceivers to more easily exploit targets for gain (Grazioli & Jarvenpaa, 2000). All of these deceptions involve judging whether information is truthful or deceptive and all have consequences related to judgement accuracy. There may be limitations to traditional forms of deception detection in mediated environments and a more holistic approach to deception detection is required to understand the behavioural context from which deception occurs.

Motives for online deception:

Motives for online deception vary according to people's needs and aspirations (Caspi & Gorsky, 2006; Lu, 2008; Utz, 2005). Motives for online deception include self-serving and other-oriented lies (Whitty & Carville, 2008), concerns about privacy and safety (Caspi & Gorsky, 2006; Utz, 2005; Whitty, 2002), idealised self-presentation (Utz, 2005), play (Joinson & Dietz-Uhler, 2002; Utz, 2005), avoiding unwanted social interaction (Hancock et al., 2009; Reynolds, Smith, Birnholtz & Hancock, 2013) and harmful intent, including financial gain (Buchanan & Whitty, 2013; Utz, 2005). Frequent Internet users may deceive more than infrequent users potentially due to enhanced understanding of technology reducing mistakes indicating deceit (Caspi & Gorsky, 2006). Individuals may also prefer to deceive others through an avatar as this may reduce anxiety felt during text-based deception activities (Galanxhi & Nah, 2007). Although this may only be affective if the avatar is not reflective of their real-world identity (Hooi & Cho, 2012). There may be more high-stakes motives for online deception related to adversary aims which current research has not fully explored.

Online Communication Strategies:

To understand online deception an understanding of how communication is conducted online is required. Detecting deception relies upon identifying cues from an individual's behaviour, in CMC two characteristics that may influence the ability of the target to interpret these cues are media synchronicity and media richness (Carlson & George, 2004). Deception in CMC can be asynchronous or synchronous (Zhou & Zhang, 2006): Asynchronous CMC allows people to communicate at different times enabling rehearsability where people have time to plan and edit what they mean to say whilst reprocessability enables individuals to review previous messages aiding the process of constructing deception (Carlson & George, 2004; Zhou & Zhang, 2006). Ambiguities created in asynchronous communication can be further exploited to enhance plausibility and consistency of deception (Birnholtz, Guillory, Hancock & Bazarova, 2010). Rehearsability and reprocessability can also be used in face-to-face (f2f) interactions although it may be more difficult to perform these tasks under time constraints (Carlson & George, 2004).

In interactions synchronous CMC is more involving than asynchronous CMC and has greater perceived similarity, mutuality, higher identification and interaction coordination, greater cognitive, emotional and behavioural involvement, increased group feeling and identification than asynchronous CMC (Burgoon, Chen & Twitchell, 2010). Such increases in deceiver's cognitive load may enable identification of deception (Zhou & Zhang, 2006). Greater conversational coordination leads to greater interpersonal interaction (Burgoon et al., 2010). Deceivers may be just as effective as truth-tellers in achieving conversational interactivity in both synchronous and asynchronous CMC and may appear more sociable, dominant and composed when lying compared to telling the truth (Burgoon et al., 2010). Burgoon et al. (2010) found that motivated deceivers can create a credible image while communicating via text and can use their credibility to influence others to make decisions regardless of synchronicity. Synchronous CMC poses greater risk due to increased interactions between the deceived and the deceiver, increasing the potential for malign influence (Burgoon et al., 2010).

When conversing through CMC people have the advantage of editability, which is not present in f2f interactions (Hancock et al., 2010). Editability enables people to edit what they say before interaction increasing potential for deception. This is possible in synchronous and asynchronous CMC; asynchronous conditions increase time for message construction, although in synchronous CMC there is still a slight delay enabling more editability than f2f conditions (Hancock et al., 2010). CMC increases selective-self presentation, where people can more actively choose which aspects of themselves to present to the target compared to f2f communication (Hancock et al., 2010).

People's perception of richness in a communication channel may influence their choice of communication medium for committing deception (Carlson & George, 2004), whilst cognitive and affective-based trust in low richness environments may mediate deception (Rockmann & Northcraft, 2008). Media richness theory focuses on four areas of communication interaction: speed of interaction; cue multiplicity; language variety; and personal focus (Carlson & George, 2004; Carlson & Zmud, 1994). There is a greater richness in communicational interaction with higher levels of these areas (Carlson & George, 2004). Judgements made regarding another individual may be influenced by cues available in the level of richness that decision-making occurs in (Wall, Taylor, Dixon, Conchie & Ellis, 2013). Both deceiver and deceived

may prefer synchronous interactions as they feel more able to deceive and to detect deceit (Carlson & George, 2004). A receiver may feel more confidence in detecting deception in familiar media formats and in conditions of high media richness as this is perceived as exposing more cues to deception whilst increasing accuracy in judgement (Carlson & George, 2004; Zhou & Zhang, 2004; Zhou & Zhang, 2007). A receiver may be less certain of their ability to detect deception in asynchronous communication with an unfamiliar sender (Carlson & George, 2004). Deceivers generally prefer synchronous communication for when they are lying but are able to differentiate between the usefulness of communication mediums for different types of deception, and may prefer asynchronous media for low-stakes deceptions where there is minimal risk (Carlson & George, 2004).

Channel expansion theory expands upon media richness theory through examining an individual's experience and perception of media richness in a communication channel in order to understand their choice of communication preference (Carlson & Zmud, 1994; Carlson & Zmud, 1999). Four experiences identified as being particularly important are: experience with the channel; experience with the messaging topic; experience with the organisational context; and experience with communication co-participants. As people develop their knowledge in these areas they will participate in increasingly rich communication through that channel and will then perceive that channel as becoming increasingly rich in communication ability. Alternatively if people do not develop these skills, they will not have an experience of rich communication via that channel and will not perceive it as useful in conveying information.

The Internet can lead to perceived anonymity where there is a focus on the self and reduced concern of accountability to others (Hancock et al., 2007). This perceived anonymity may increase disinhibition and lead to more risky and extreme behaviour. Suggesting individuals may find it easier to participate in acts of deception online as they perceive themselves as anonymous and that they will not be held to account for their actions. Such disparities in online communication may pose little risk for the deceiver whilst posing a greater risk for the target, encouraging adversaries to conduct deception online.

Online Impression Formation:

Mediated environments reduce the amount of behaviour that can be analysed to ascertain whether a person is lying, the cues to behaviour are filtered out (Burgoon et al., 2010; Carlson & George, 2004; Caspi & Gorsky, 2006; Hancock, 2009; Hancock & Dunham, 2001; Zhou & Zhang, 2006) and this presents a challenge for researchers used to f2f interactions (Lu, 2008; Utz, 2005). Elements of cognitive and verbal cues may still be apparent in synchronous communication as the deceiver requires cognitive effort to construct a story, especially if the conversational group involves multiple individuals (Zhou & Zhang, 2006).

The Social Identity/Deindividuation (SIDE) model accepts the lack of cues in making judgements, but shifts focus towards how CMC is affected by social identity and cognitive processes used to make inferences and attributions from minimal information (Hancock & Dunham, 2001). The lack of individuating cues in interactions suggests that people using CMC become anonymous, with an increased reliance on social cues, including from communication style, in which impressions are formulated (Hancock & Dunham, 2001). Impressions generated from these cues may be more stereotyped and exaggerated representations of interactional partners (Hancock & Dunham, 2001).

The hyperpersonal model combines the SIDE model and social information-processing theory, to present a model where experiential, cognitive and behavioural aspects are considered together (Hancock & Dunham, 2001). In the hyperpersonal model interpersonal impressions in CMC are more intense, receivers make overattributions regarding their conversational partner's personality and senders in CMC may also selectively choose personality traits that are present in interaction (Hancock & Dunham, 2001). It may be harder to detect deception in a person in online interactions if we initially perceive that person favourably and then make further attributions based on this favourable impression, understanding how such impressions are made may mitigate reliance on using partially formed online impressions to make judgements of veracity.

Online Deception Detection Strategies:

Deception occurs in a wide range of mediated environments, meaning deception detection strategies must reflect context, for example, verbal strategies may

be applied to online text-based communication and to online audio content, and non-verbal strategies may be applied to online visual and audiovisual communication, however, there may be different cues and strategies used in deception detection for other forms of online deception.

Theory of Deception (Grazioli, 2004; Johnson, Grazioli, Jamal & Berryman, 2001) argues that individuals detect deception through noticing and interpreting anomalies in their environment through reference to the goals and aims ascribed to interactional partners. Theory of Deception has four processes: Firstly activation occurs where received information is paired to cues where there are discrepancies between what is observed and what is expected (Grazioli, 2004). Secondly, there is a deception hypothesis generation; where people attempt to develop an explanation for the differences between their observations and expectations. Thirdly, once a hypothesis has been generated it needs to be evaluated through comparison with related criteria. In the fourth stage there is a global assessment, where the hypothesis is combined with an overall assessment of deception of the area being questioned. Grazioli (2004) recruited MBA students who were deemed to be media and computer savvy through their presence on that course. In conjunction with a real website, a 'jacked' website was created where half of the participants were unknowingly directed to the 'jacked' site (Grazioli, 2004). The participants who identified the deceptive site used fewer, but more predictive cues to deception (Grazioli, 2004). Priming individuals to the possibilities of deception may have some impact on people's ability to detect deception in the context of page-jacking (Grazioli, 2004) and other contexts (George, Marret & Tilley, 2004). Individuals who accurately detected page-jacking used cues related to information assurance rather than trust, suggesting individuals could see through deceiver's strategies to appear credible (Grazioli, 2004). Such strategies may be used upon an individual's knowledge and use of a communication format alongside awareness of potential for deception online.

Further development of the Theory of Deception argues that the recipient's individual disposition and perceptions are also vital for detecting cues to deception (Wright, Chakraborty, Basoglu & Marett, 2010). Disposition to trust and Web experience are influences on detecting phishing, however computer self-efficacy, security knowledge, perceived risk, and suspicion of humanity may not be strong predictors of detecting phishing (Wright et al., 2010). In detecting phishing via email there are two points to detect deception: the first point is before the email is opened,

where email authentication cues are salient and second after the email is opened it becomes the only source of cues to deception (Wright et al., 2010). Once opened there is an initial authentication of the email and perceived cues to deception before suspicion is activated by the relationship between the cues, context and individual factors (Wright et al., 2010). Individual factors include sensitivity to the value of information, concern for privacy, obedience to authority and conscientiousness in judgement, whilst contextual factors were linked to knowledge of the institution. The third stage of deception detection involved individuals' confirmation of suspicion. The evaluation of the hypotheses was found to be related to two main categories: confirmation seeking of authenticity and individual investigation of authenticity (Wright et al., 2010).

Prominence-Interpretation Theory (PIT – Fogg, 2002) argues that individuals assess credibility of websites through noticing features, judging them and then assigning credibility. Fogg (2002) argues that prominence is affected by user involvement, website content, the user task, user experience and individual differences, whilst acknowledging the potential for other factors that may influence how people assign prominence. User assumptions, user skill/knowledge, context and user goals are argued to be linked to the interpretation of features (Fogg, 2002). PIT focusses on the content and interpretation of the user in assessing credibility of websites, however, it seems possible that individuals may assess credibility in this manner in other contexts including other forms of online content and has the potential for expansion to face-to-face situations.

People focus on website design features to inform their judgements of website credibility (Fogg et al., 2003 - see Appendix 3.2). Fogg et al. (2003) examined whether different techniques are used to assess credibility in different contexts. E-commerce sites are judged according to their reputation and recognition, and customer service; news sites were judged according to perceived bias of information; non-profit organisations were judged according to their identity, with fewer references to their information structure; opinion/review sites were judged according to their information bias and accuracy; travel sites were judged according to customer service; and search engines were judged according to information functionality and design and individuals also tested these sites to form their own opinions (Fogg et al., 2003). However, further work is required to examine whether individuals use these strategies for assessing credibility in other online environments.

In assessing credibility there is a trust bias towards information coming from perceived reliable sources (Metzger & Flanagin, 2013), and to website design, content and complexity features rather than familiarity with website sponsors (Flanagin & Metzger, 2007). However, online information may lack the indicators used to assess author identity or reputation and subsequently credibility (Metzger & Flanagin, 2013). When information regarding the source is unavailable, difficult to interpret, or missing there may be uncertainty over the veracity of the information (Metzger & Flanagin, 2013).

Cognitive heuristics are often employed to make decisions regarding the credibility of online information, to reduce cognitive load during decision-making (Metzger & Flanagin, 2013; Metzger, Flanagin & Medders, 2010). Metzger et al. (2010) identified five cognitive heuristics used to evaluate credibility online in a US sample: *reputation*, *endorsement*, *consistency*, *self-confirmation*, *expectancy violation*, and *persuasive intent*. Although there is difficulty in sorting heuristics into explicit categories as processes may occur simultaneously in decision-making, and contexts may generate multiple heuristics, alongside one heuristic activating another (Metzger et al., 2010). Cognitive heuristics used to assess credibility may further not be effective in distinguishing truth and deception, highlighting the need for understanding whether individuals use correct or incorrect strategies for assessing credibility online. If individuals from adversary nations use such incorrect heuristics for judging credibility then they may be exploited through deception operations.

In developing a framework of online credibility assessment, Hilligoss and Rieh (2008) propose that there are construct, heuristic and interaction credibility judgements, although these judgement strategies may work in conjunction with one another. The construct level identified by Hilligoss and Rieh (2008) examines how individuals construct credibility which in turn influences how they judge credibility. The heuristics level involves judgement strategies that are used across multiple contexts, whilst the interaction level focuses on judgements based upon source and content cues (Hilligoss & Rieh, 2008). These processes are argued to influenced by context (Hilligoss & Rieh, 2008), although the impact of personality and its effect upon decision-making is also required. The interaction level proposed by Hilligoss and Rieh (2008) focuses upon an individual's interactions with a website and neglects the online interactions that occur between individuals which require credibility judgements that will be influenced by interpersonal dynamics. Furthermore, the

framework proposed does not focus upon the accuracy of credibility judgements in identifying truth and deception.

In linguistic patterns in synchronous CMC, deceivers may use a greater number of words, sense-based words, and other-oriented pronouns and use less self-oriented words when lying than when telling the truth (Hancock et al., 2008). Motivated liars may use fewer causal terms when lying, unmotivated liars may increase their use of negative terms and motivated deceivers will be more successful in their deception (Hancock et al., 2008). The anonymity of cyberspace means that individuals may feel no connection to those they are deceiving and no need to feel guilty for deceiving them (Caspi & Gorsky, 2006) suggesting that they may not show emotional cues to deception associated with guilt. Biases occurring in f2f interactions may also occur in mediated interactions, for example, the truth bias is prominent in assessing deception in CMC increasing vulnerability to deception (Boyle, Kacmar & George, 2008; Hancock et al., 2010).

Language change in online communication has enabled the identification of cues to deceit (Hancock, Curry, Goorha & Woodworth, 2005; Toma & Hancock, 2012; Zhou, Burgoon, Nunamaker & Twitchell, 2004), including potential cues to deception related to insider threat (Taylor et al., 2013) and linguistic markers for radical violence (Cohen, Johansson, Kaati & Mork, 2014). Hancock et al. (2005) found that deceivers produced more words, used fewer first person but more third person words and more sense words than truth-tellers. Increasing the number of words may be used by deceivers to appear more credible or as a strategy of distracting the receiver from inconsistencies in narrative, whilst other tactics may involve the deceiver distancing themselves from their behaviour. In a simulation of an insider attack, Taylor et al. (2013) found that in email communication insiders became more self-focussed, had greater negative affect and engaged in more cognitive processing whilst their mimicking of team members language deteriorated over time, potentially due the cognitive load involved in appearing credible. Examining the language used to identify intent to harm others, how individuals discuss targets and identify with others may be a promising approach for detecting violent extremists before acts may occur (Cohen et al., 2014). Analysing behaviour indicative of deception and threat in online environments is a promising approach to deception detection and can be further augmented with the inclusion of individual differences and the social and affective context of the interaction (Thompson, 2009).

ACID has been applied to deception detection in synchronous CMC via IM (Werdin et al., under review). CMC allows users to track their information and avoid releasing sensitive information or making contradictions, and they can appear calmer, furthermore users are able to edit and review their messages before sending, and with the lack of f2f there is less behaviour to control (Colwell et al, 2013). Werdin et al (under review) required participants to tell the truth or lie about their gender and interaction with a same-sex best friend and found that honest statements were longer and more detailed at free recall but not during mnemonics, although overall these differences were not significant. However, this study was low stakes and used a student sample, suggesting it may have issues of real-world validity. Techniques involving mediated interviewing may also be more likely to uncover deception through deceiver's confessing their deceptive behaviour (Dunbar et al., 2013). Not all individuals may confess to deceptive behaviour and confessions still have a requirement for investigation to ensure they are legitimate.

Cross-cultural deception in computer-mediated communication:

Although there has been an increase in the amount of research examining deception detection in f2f and CMC there has been little research examining cultural differences in deception detection across either communication medium (Lewis & George, 2008). For issues of national security and intelligence assessment of communication from other cultures, understanding the impact of culture on deception is critical. Culture can be divided into four dimensions: 1) individualism/collectivism; 2) power distance; 3) uncertainty avoidance; and 4) masculinity/femininity (Hofstede, 1980, p.260). In a comparison of Koreans' and Americans' experience of deception, Lewis and George (2008) found that: Koreans are more collectivist, more likely to use deceptive behaviour and lie about different aspects of themselves than Americans; and deceptive behaviour is greater in f2f communication than CMC for Koreans and Americans; Americans and Koreans hold similar beliefs about deceptive behaviour in CMC, however, Koreans are more deceptive using f2f communication than Americans, potentially due to richness of communication channel (Carlson & George, 2004). Individuals holding stronger masculine cultural beliefs are more likely to be deceptive than those holding stronger feminine value beliefs (Lewis & George, 2008).

Overall, regardless of culture people may prefer to engage in deceptive behaviours through f2f rather than CMC (Lewis & George, 2008).

When exploring Taiwanese deception, Chen and Huang (2011) found that deceivers often select tactics which reflect their own and the target's characteristics. Chen and Huang (2011) identified deception tactics including masking, mimicking, relabelling and inventing which were used against individuals and business. Tactics used to deceive business were more likely to include relabelling and inventing (Chen & Huang, 2011). Deceivers purporting to be businesses were more likely to use masking tactics, whilst deceivers purporting to be individuals were more likely to use mimicking and inventing tactics (Chen & Huang, 2011). It is crucial to understand the tactics which individuals use in order to appear convincing to others and further research is required to examine this across cultures.

Online Adversary Deception and Influence:

A major issue involving cyberspace is increased potential for adversary influence where there is a need for accurate methods of veracity assessment in order to mitigate adversary influence. The digital domain has the potential to be exploited at multiple levels by a wide-ranging group of adversaries, from lone actors, to criminal organisations, to terrorist groups and state-sponsored actions, furthermore these areas do not have set boundaries (Cornish, 2009; Cornish et al., 2009; Cornish, Livingstone, Clemente & Yorke, 2010).

The Internet has made adversary influence and deception (Tan, 2003) far more accessible and interactive with its audience from posting videos on website for viewing (Weimann & Gorder, 2009), to interactive virtual communities where people can anonymously discuss issues and ideas and engage in influence (Cornish, 2009; Nacos, 2007; Ramsay, 2008; Thomas, 2003; Weimann & Gorder, 2009). The wide range of communication formats in cyberspace has enabled groups to organise their activities even when they are severely restricted and monitored (Weimann & Gorder, 2009). Furthermore, as misinformation proliferates online, a wider range of individuals, whether predisposed towards such material or not, may interact with such information presenting additional challenges in reducing vulnerability to misinformation (Mocanu, Rossi, Zhang, Karsai & Quattrociocchi, 2015).

Terrorist and insurgent groups began to utilise mediated technologies during the Russian-Chechen conflict during the 1990s and early 2000s, since then there has been an exponential rise in the number of groups using the Internet (Thomas, 2009). The rise of the Internet has enabled terrorists to self-publicise through their websites, and maintain a greater control of their own image and perception amongst their target audiences, whilst simultaneously manipulating the image and perceived perceptions of their adversaries (Weimann, 2004). The internet is useful to adversary groups due to: easy access; little or no regulation; increased reach; fast flow of information; inexpensive development and maintenance of a web presence; the ability to shape coverage in the traditional mass media, which increasingly use the Internet as a source for stories (Weimann, 2004) and the development of influence strategies to reflect their targets (Thomas, 2003; Thomas, 2006; Weimann & Gorder, 2009).

Conclusion:

Individuals commit acts of deception on the Internet for a variety of reasons from playing with aspects of identity to acts of phishing where they seek to gain access to confidential information. In the online environment the ability to detect deception is similar to that in interpersonal interactions in that it is similar to levels of chance. Aspects of traditional verbal and nonverbal deception detection methods may be applicable to the online environment as verbal deception detection methods may be useful in assessing veracity in CMC and in audiovisual material, and non-verbal deception detection methods may be suitable to analysing visual and audiovisual behaviours. However, they may not be enough to assess veracity by themselves and there needs to be an understanding of the personality and individual factors and how these impact on behaviour in the online world.

Adversary use of the Internet for deception and influence increases the need for a model of deception detection that can be employed across technologically converging domains to counter threat. Current research in this area is lacking, in particular the impact of personality and culture on deception across communication domains. The range of utilities open to adversaries on the Internet shows a need to develop a comprehensive model of deception detection to examine veracity at multiple levels from interpersonal deception across terrorist disinformation and the analysis of strategic threats.

Chapter 4: Military and Strategic Deception

Introduction:

Military deception differs from deception in everyday life, where the ability to deceive is considered a valuable skill rather than a character flaw (Glenney, 2009). Military deception encompasses interpersonal and online environments and detection methods are required to assess veracity of information across attributable and non-attributable sources. Research in military deception has focussed on developing strategies for deceiving others and the use of deception as a force multiplier (DCDC, 2007), whilst research into deception detection has been neglected. Adversary use of deception in asymmetric conflict should be anticipated as it is cost effective and enables increased flexibility against superior forces (Godson & Wirtz, 2002; McPherson, 2010; Whaley & Busby, 2002). Current challenges in military environments reflect the rise in social media and the increased reach, impact and speed in which the information environment may be shaped by adversaries (Collins, 2002; Dearth, 2000; D'Ovidio, 2007; Stein, 2000). Increasing the need for developing strategies to counter adversary deception. Whilst the majority of research into deception examined in Chapters 2 and 3 addresses deception from a forensic background there is a contingent need to examine military approaches to deception whether interpersonal or mediated to ensure robust responses are developed to potential threats. The current chapter outlines theories of military deception, target audience analysis, historical lessons learned, decision-making biases and approaches to counter-deception.

Theories of Military Deception:

Deception ranges across the strategic, operational and tactical (DCDC, 2007; Glenney, 2009). Strategic deception occurs in the misleading of an adversary of intended operations at the highest level, operational deception occurs in the misleading of an adversary in the Joint Operations Area (JOA) and is used to support strategic deception in the medium or short-term, whilst tactical deception incorporates all short-term measures intended to mislead the adversary (DCDC, 2007; Glenney, 2009). It is argued that strategic deception is often hardest to understand and identify, due to the complexity of operational environments, and the multiple features involved

in constructing deception increasing cognitive load in the target (Henderson & Lee, 2007; McPherson, 2010).

Taxonomies of Deception

Taxonomies of different forms of deception have been developed exploring the forms that deception is argued to take across a range of environments (Bell, 2003; Henderson et al., 2007; Henderson & Lee, 2007; Macdonald, 2007; Whaley, 1982; Whaley, 2007). Deception is proposed to comprise of simulation and dissimulation (Bell, 2003; Whaley, 1982). Simulation is considered to be showing false information to the target through mimicking, inventing and decoying strategies (Whaley, 1982). Mimicking tactics seek to deceive the target through imitating reality, inventing tactics create something new which is false, and decoying tactics deceive the target through diverting attention to another area (Bell, 2003; Henderson & Lee, 2007; Macdonald, 2007; Whaley, 1982). Dissimulation is argued to deceive the target through hiding information by masking, repackaging and dazzling tactics (Whaley, 1982). Masking aims to hide information by making it invisible to detection, repackaging hides reality through disguising and modifying appearance, and dazzling hides reality through presenting a range of options to blur reality in sense-making (Bell, 2003; Daniel & Herbig, 1982; Henderson & Lee, 2007; Macdonald, 2007; Whaley, 1982).

Deception tactics can be used to reinforce the target's existing beliefs enabling exploitation (Bell, 2003; Cali & Romanych, 2005; Henderson & Lee, 2007; Heuer, 1981, Macdonald, 2007). If the target is fully or partially aware of attempts to deceive them, the deceiver may deploy ambiguity increasing or decreasing tactics (Bell, 2003), which require resources, whether physical or cognitive to uncover the deception. Changes in ambiguity may also affect the target's decision-making abilities, particularly use of cognitive heuristics which may result in bias (Gerwehr, 2006; Heuer, 1981). Exploiting the target's emotions will provide another tactic for deceiving others (Dauber, 2009; Henderson, 2007). For example, Dauber (2009) reports that Iraqi insurgents posed as US soldiers injured during Gulf War II in online chatrooms and attempted to influence the domestic US audience against the war.

Deception is argued to mainly occur as a combination of both simulation and dissimulation tactics (Bell, 2003; Macdonald, 2007), as whilst simulating reality,

reality also needs to be concealed from the target to maintain consistency and plausibility of the deception. Macdonald (2007) includes disinformation as a deception tactic which incorporates both simulation and dissimulation as truthful information may be concealed whilst real information may be simulated through camouflage, decoys, dazzling and conditioning and such tactics may occur across a range of communication channels increasing the need for a holistic approach to deception detection.

The target may also be deceived through conditioning techniques where the deceiver creates a pattern of behaviour which can then be exploited later, for example as in the 1973 Yom Kippur War between Egypt and Israel (Macdonald, 2007). The Egyptian forces conditioned the Israeli forces through staging numerous canal-crossing exercises, and movement of large numbers of troops to the border before withdrawing them. This meant that when then the Egyptian troops were mobilised for the invasion the Israeli forces were not prepared as they thought the troops would be withdrawn again (Macdonald, 2007). Such conditioning may be conducted over a period of time so that the target then accepts behaviour as normal with no apparent threat shown (Macdonald, 2007). Another form of deceiving the target involves changing tactics or rules as the target may not have anticipated or prepared for eventualities that do not reflect perceptions of normal behaviour (Macdonald, 2007).

Recent approaches have sought to apply psychological principles to military deception to create greater understanding of the deception process and how to conduct deception (Henderson, 2007; Henderson et al., 2007). Henderson et al. (2007) conducted a review of deception research to identify generic principles of deception that occur across a range of contexts. A model of deception was proposed where deception is accomplished through presenting the target temporally-anchored perceptual cues sequences which through pattern recognition shape the target's cognition and behaviour (Henderson et al., 2007). Cues are argued to be physical and information based and can be combinations of both, whilst cognitive, affective, social and environmental factors may be manipulated to reduce or disrupt the target's pattern matching and expectancies (Henderson et al., 2007).

These principles are seeking to highlight how people can be deceived rather than how to detect deception, although knowledge may be reversed for detecting deception, for example, an understanding of how people can be influenced is beneficial to both senders seeking to deceive and receivers seeking to detect

deception, whilst target audience analysis of adversaries may generate an understanding of the potential deception strategies they will utilise.

Deception Planning

In order to successfully deceive others in strategic, operational and tactical environments deception must be carefully planned to ensure its effectiveness (Henderson, 2007). Deception should be expected in some operating environments where it presents an asymmetric advantage for weaker nations against stronger nations who rely on superior forces and technology (Godson & Wirtz, 2002; Macdonald, 2007). Various approaches have been developed for planning deception operations (Bell, 2003; Daniel & Herbig, 1982; Henderson, 2007; Latimer, 2001; Whaley, 1982). Deception plans have covered key areas of human behavior including identifying the actions and means required in targeting key adversaries to influence their cognition and behavior towards a desired state (Heuer, 1981; Johnson & Meyeraan, 2003; McPherson, 2010).

The deception planning process is argued by Whaley (1982) to consist of 10 stages. First the deception planner must know the strategic goal of the deception; second the planner must decide how they want the target to react for strategic advantage; third the planner must decide how they want the target to perceive events or information; fourth the planner is required to decide what is to be hidden and what is to be shown in place of reality; fifth the planner must analyse the pattern of reality which is being hidden to identify the characteristics that must be hidden or altered; sixth the planner then analyses the pattern of the false reality to ensure that it is plausible; seventh the planner has designed the desired effect and the method with which it is constructed and now the means for presenting this information to the target is required; eighth the effect and the means to convey the effect have been developed and now the deception begins; ninth the channels through which the deception is communicated are selected for links to the specific target audience; and tenth to ensure the success of the deception the target must believe the information they receive (Whaley, 1982). This process covers the deception planning process in depth, however, it does not consider how the adversary may respond to the deception and how such changes are measured and then responded to by the deceiver.

Bell (2003) proposes a similar deception planning process to Whaley (1982), however, the effectiveness of deception and further responses by the target and deceiver are also considered. Bell (2003) argues that the deception process covers 11 stages: first the deception is planned, where the goal is identified alongside the costs and benefits of the deception, and the selection of the form of deception and the channel to be used in the deception; second the ruse is constructed from a variety of tactics to ensure the context is reflected; third the channel for the deception is selected; fourth the deception is channeled to the target; fifth the target makes a decision regarding whether to accept the deceptive information as truthful or not; sixth the deception is accepted and the target adjusts their behavior to match the deception; seventh the target responds to the deception; eighth the deception planner analyses the target's response to the deception; ninth the deception planner decides whether to respond to target feedback; tenth the deception cycle is continued where the planner makes further adjustments to the deception or continues to measure the target response to the deception; or eleventh, where the deception cycle is closed whether through discovery by the target or achievement of the planner's goals (Bell, 2003). However, there is a further need for understanding how the target may counter such attempts at deception, whether through the tactics they use to uncover the deceit or how they may identify attempts at deception but then begin a deception cycle of their own.

Daniel and Herbig (1982) developed a model of deception focussing on: secrecy, organisation and coordination; plausibility and confirmation; adaptability; predispositions of the target; and factors in the strategic situation. Secrecy refers to protecting the deception with a cover story, and ensuring operational security (OPSEC) amongst own forces. To protect secrecy the deceptive act must be well organised with precision planning. Both the organisation and secrecy of a deception will be coordinated from a centralised point. The deceiver must think like the adversary, in order to ensure plausibility the deception must appear like a realistic proposal, and be confirmed from a number of credible sources (McPherson, 2010). The deception strategy should be flexible and able to adapt as the situation changes and as adversaries react to the deception (Martin, 2008). How an adversary reacts is based on their predispositions, they may believe that something is wrong but will still fall for a deception if the deception is credible to their biases (Martin, 2008).

UK deception is argued to have 4 main objectives: to provide a commander with a choice of actions to implement their mission, by manipulating the adversary as to his intentions and by diverting the adversary's focus away from the action being implemented, in order to achieve the allied aims; to mislead the adversary and persuade them to implement actions that are to their disadvantage and can be exploited; to gain surprise; and to reduce friendly causalities (Latimer, 2001). Latimer (2001) has seven principles for deception focussing on the decision maker's thinking; action to make them act in a specific manner; coordination and centralised control; preparation and timing which requires a logical planning process where timing is critical, and this links to the operational plan; security including OPSEC; credibility and confirmation where the adversary must believe the deception, through the provision of a credible plan; and flexibility where there is an ability to adapt to change (Latimer, 2001).

Success in deception has been typified by its integration into the operation plan, central control, minimal staff planners, maintenance of OPSEC, multi-layered and complementary deceptions which reinforced adversary sensemaking within the context of tactical norms (Henderson & Lee, 2007). When deception has been unsuccessful there has been less central coordination of the multi-layered approach potentially decreasing the plausibility of deception attempts and increasing detection by the adversary (Henderson & Lee, 2007). To increase the success of deception in depth knowledge of the target is required.

Target Audience Analysis:

An in-depth knowledge of the deception target is needed to increase chances of influencing key decision makers through deception strategies (DCDC, 2007) and to avoid mistakes associated with cultural and religious differences (Jajko, 2002; Wolfe & Arrow, 2013). Mackay and Tatham (2011, p. 95) argue that understanding audiences is central to communication and should be part of preparations for operations and this concept is readily transferable from influence operations to deception operations. In influencing a target audience the message needs to be contextually rational to the audience to actually change their behavior (Mackay & Tatham, 2011, p. 96), if the message is not rational or plausible to the target they may remain skeptical.

In deceiving and detecting deception in military domains incorporation of cultural intelligence is argued to improve the effectiveness of deception capabilities (Coles, 2006). Cultural intelligence considers information derived from cultural demographics, social, political, and economic information, enhancing understanding of a nation's people, history, psychology, beliefs, and attitudes and behaviours. Cultural intelligence will improve deception detection through understanding the wider picture of the reasons for, how and why a person from another culture may commit deception. Understanding the interactions between language, culture and cognition enables the detection of group biases and preferences which will aid analysts and those in operational environments to uncover potential threats (Ceruti, McGirr & Kaina, 2010).

Awareness of culture in conflict enables greater influence in shaping the information environment, and defending again adversary deception. Spencer and Balasevicius (2009) refer to the usage of cultural intelligence by Special Operation Forces in Operation Enduring Freedom, where awareness of cultural differences in Afghanistan enabled enlistment of adversaries of the Taliban to help take down their regime. However, cultural awareness may be limited to specific operations rather than strategically deployed. In Afghanistan one of the difficulties facing troops is the ability to separate friend from foe, through understanding cultural differences we may be able to accurately do this (Spencer & Balasevicius, 2009). Spencer and Balasevicius (2009) state that skilled interpreters are able to detect deception through cues in changes in behaviour, speech pauses, facial expressions and ambiguities, and that they rely on how something is said rather than what is said (Spencer & Balasevicius, 2009).

Historical lessons learned:

A key aspect of understanding the effectiveness of deception is to understand lessons learned from successes and failures in deception and deception detection operations (Wolfe & Arrow, 2013). Sellers (2009) examined Operation Mincemeat and the principles which made it a successful mission. Operation Mincemeat was a deliberate deception operation to conceal the location of the D-Day landings conducted by Allied forces during the Second World War (Sellers, 2009). This deception operation involved placing false information on a body, purporting to be

that of an Intelligence Officer whose plane had crashed into the sea, and this body would then float onto Spanish shores where the false information would be fed back to the German forces (Sellers, 2009). Through understanding the adversary the target could be focussed towards specific behaviour. There needs to be strict centralised control in order to ensure that the operation is properly controlled with no leak of information. Time needs to be considered into a deception operation, as you need to allow time for the adversary to receive, interpret, respond and then you receive feedback to any information they receive. Each deception must also be integrated to the overall operation that the deception is supporting (Sellers, 2009).

Exploring lessons learned from military influence campaigns in Iraq and Afghanistan enables the understanding of successful and unsuccessful influence tactics (Wolfe & Arrow, 2013). In cross-cultural influence, tactics involving respect, empathy, prior relationships and familiarity with the influence targets predicted success in influence (Wolfe & Arrow, 2013). Negative tactics were used more commonly in unsuccessful attempts at influence (Wolfe & Arrow, 2013). These findings highlight the importance of using positive influence campaigns as they may reduce casualties and fatalities in operational environments (Wolfe & Arrow, 2013). Alternatively, these findings highlight that individuals are also more influenced by positive information which when linked to deception may suggest that there is more potential vulnerability from adversary deception operations which appear credible and positive to the target.

Deception as a strategy was neglected during the conflict between the former Yugoslavia nations of Serbia and Montenegro and Kosovo supported by NATO and Albanian troops and also in the more recent Afghan conflicts (De Caro, 2002; Vego, 2002). Vego (2002) argues that the US viewed deception as unnecessary as it was not needed in conflicts where they had powerful physical strength, and that adversary deception would be ineffective. However, Serbian use of deception during the Kosovo conflict was widespread in its attempts to undermine NATO morale (De Caro, 2002).

During the 2006 war between Israel and Hezbollah, Hezbollah succeeded in using deception to combat Israel's military superiority (Acosta, 2008). Hezbollah controlled the information sphere before Israel confronted them over their repeated attacks and border skirmishes on the northern Israeli-Lebanon border (Acosta, 2008). This enabled Hezbollah to control the ways in which they presented themselves to appear more credible to their audience (Acosta, 2008). Hezbollah's denial operations

were successful through their Counter-intelligence (CI), OPSEC, and strict control of open-source information (OSINT) and intelligence. Meaning Israel was unable to gather information and intelligence about Hezbollah's military capabilities before they engaged in combat seriously undermining their operations. Hezbollah built fake bunkers that would be picked up by aerial drones, and built their real bunkers out of sight of Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR - Acosta, 2008). Hezbollah also conducted an electronic warfare bluff through allowing rumours to surface that they were using electronic warfare capabilities that were able to monitor Israeli radio communications, and then took information like troop casualties and broadcast it on TV to undermine Israeli morale (Acosta, 2008). Hezbollah retrieved this information through monitoring UN provided OSINT about Israeli troop movements and actions in Lebanon (Acosta, 2008). Hezbollah expanded their TV station so that they could now broadcast their beliefs and messages to a wider audience, and their news stories were broadcast further by other Arab TV stations, for example, Al Jazeera (Acosta, 2008). These other networks did not check the validity of Hezbollah's broadcasts, footage made its way onto websites without any form of veracity assessment and journalists were given strictly controlled tours of Israeli bomb damage by Hezbollah guides (Acosta, 2008). Hezbollah also attempted to hijack other websites to provide links to video footage from their TV channel; however, they were thwarted in their actions by other Internet users (Acosta, 2008).

Dauber (2009) examined the aftermath of Operation Valhalla (an engagement between US Special forces and a Jaish al-Mahdi squad). Dauber (2009) states that prior to this conflict they could expect an adversary propaganda response between 24 to 48 hours of the event, however, in this case there was an adversary response within 45 minutes where the bodies of 16 or 17 Jaish al-Mahdi insurgents had their weapons removed and were moved into a position of prayer, and then photos were taken of these bodies and uploaded to the Internet where they were portrayed as having been the victims of unprovoked aggression. Dauber (2009) states that the targeted audience of this adversary deception was the US public in an attempt to reduce morale.

Decision-Making Biases:

Decision-making biases in intelligence analysis and deception detection highlight areas of vulnerability which may enable adversary exploitation. Awareness

of these biases in judgement is required to increase resilience against adversary deception. To interpret the real world people create simplified mental models to reduce complexity, and it is within these simplified models that intelligence analysis occurs, even if this is not the most efficient way of interpreting the real world (Heuer, 1999). People construct their own versions of reality through the information which they perceive from their senses and this information is then interpreted according to experiences, needs, desires and cultures (Heuer, 1999). Analysts need to be aware of themselves to understand how they and others might interpret the same data (Heuer, 1999). Heuer (1999) states that information analysts use is from a variety of sources, and such information is often incomplete, unreliable, subject to deception and decision-making is often affected by time constraints.

Further biases may reflect distrust of real information due to the information source (Whaley, 1973), an overreliance on traditional forms of warfare and perceived technological superiority (Bell, 1982; Johnson & Meyeraan, 2003), and anchoring and availability biases may also affect how information is interpreted (Heuer, 1981). Vulnerabilities in decision-making may emerge through a target's greed (Bell, 1982) where they fail to accurately assess information due to the perceived benefits, and where information target's pre-existing beliefs meaning analysts may fail to accurately question the veracity of information (Bell, 2003). To counter such biases in decision-making analysts require an open mind, skepticism, resistance in jumping to conclusions, to pay attention to anomalies and adherence to intelligence procedures (DCDC, 2007).

Military Deception Detection:

To increase resilience against adversary deception, deception detection strategies are required. In detecting adversary deception we must assume that our adversaries are using varying forms of deception, for example, the Soviet Union incorporated '*Maskirovka'* (strategic masking, camouflaging and use of denial and deception) throughout their military operations (DCDC, 2007). To identify deception, there is a need for knowledge of the adversary alongside strong intelligence and analysis of adversary behavior and patterns (Cali & Romanych, 2005; DCDC, 2007). Deception detection may be passive and active (Bell, 2003). Passive deception detection is argued to consist of a continual examination of reality seeking false

patterns and hidden threats alongside evidence of adversary deception planning (Bell, 2003). Active deception detection is argued to consist of measures of identifying those who plan deception based upon their background history or perceived future intentions (Bell, 2003). Cali and Romanych (2005) state that counterpropaganda, including disinformation, is a neglected area of focus within operating environments and that current strategies are focused towards reactively identifying adversary propaganda and how they shape situational awareness rather than proactively identifying adversary counterpropaganda which may mitigate threats before they occur (Godson & Wirtz, 2002).

Incongruities in behaviour can lead to deception detection (Whaley & Busby, 2002). Information received also needs to be compared with past information and this should not be rushed otherwise intelligence failures may occur (Heuer, 1981). The plus-minus rule argues that deception detection occurs when an individual identifies what has been added or hidden to make information appear credible (Whaley & Busby, 2002), however, this process will be affected by complexity in human interactions. In uncertain contexts more evidence will be required to detect deception and assessing deception across multiple channels may improve this process when there is understanding of how such techniques affect communication (Whaley & Busby, 2002).

Deception may be detected through identifying elements of deception plans (Bell, 1982; Whaley & Busby, 2002). Identifying patterns involved in misdirection, identifying the key players involved in an operating environment, the intentions they may have, what the payoff or gain may be, where the events take place, adversary strength, adversary style and the information channel involved in communicating the deception (Bell, 1982; Whaley & Busby, 2002). All of these areas may highlight vulnerabilities in an adversary's deception operation and in turn may exploit the target if undetected. The current research will seek to expand this approach through the incorporation of culture, personality and individual differences and the use of multiple context-specific forms of deception detection.

Decision Support Tools

The most common decision support tool used in deception detection is the Analysis of Competing Hypotheses (ACH – Heuer, 1981) and variations of this

approach (Pope, Jøsang & McAnally, 2006; Stech & Elsässer, 2004). Stech and Elsässer (2004) examine military deception detection through ACH and argue that counter-deception is hard because people often do not consider alternative explanations for the information they receive, and misinterpret the information they do have. ACH (Heuer, 1981; Pope et al., 2006) utilises information received to generate several possible scenarios for what may happen with the most plausible option being selected, however, this may also increase ambiguity in decision-making and increase vulnerability to deception (Pope et al., 2006; Stech & Elsässer, 2004). Stech and Elsässer (2004) try to rectify this problem by developing a system they call Analysis of Competing Hypotheses - Counter-Deception (ACH-CD) for giving support to decision-making. Stech and Elsässer (2004) use statistical analysis to identify anomalies indicative of deception, however, this approach has to date not addressed interpersonal or online deception.

Analysis of Competing Hypotheses using Subjective Logic (ACH-SL) is an approach to veracity assessment in intelligence reports (Pope et al., 2006). Stech and Elsässer (2004) state that there are four types of analytical failure that may affect ability to accurately detect deception: Poor anomaly detection where there is a dismissal of anomalies as they do not appear significant or do not reflect other information; Misattribution where analysts generalise anomalies to processing errors or gaps in data collection rather than to deceptive behaviours; Failure to link deception tactics to deception hypotheses; and inadequate support for deception hypotheses, where analysts fail to link deception to an adversary's potential goals. If there are more methods employed to assess veracity then a better overall analysis should be produced. Those individuals providing information and intelligence may be reliable on some aspects of the information they provide, but not on others; they may provide a mixture of first and second-hand information; they may provide information on some areas, but not on areas that may adversely affect them (Pope et al, 2006). If there are multiple sources of information for an area of intelligence, the reliability of the information received should increase (Pope, 2006). However, it may still be prudent to analyse every source of information for veracity, as information received from multiple sources may still be part of an adversary deception campaign. There may be decay in the reliability of a source for information over a period of time, therefore complacency in assessing information should be avoided (Pope, 2006). On the other side, sources whose past information may have been suspect and potentially

deceptive may start to produce information that is reliable (Pope et al, 2006). Past information may need to be taken into account in this assessment, but there needs to be a balance to ensure that good information is not disregarded due to previous deceptive information being provided by an informant.

Humans are argued to have cognitive limitations across perception, attention and memory and to counter such limitations in operational environments decision support systems can be used (Smith, Johnston & Paris, 2004). One such tool that has been tested in detecting deceptive threats is Tactical Decision-Making Under Stress (TADMUS – Smith et al., 2004). TADMUS aims to augment the recognition of malign behaviour, manage the attention of the practitioner, and to improve memory functioning in the search for diagnostic information (Smith et al., 2004). Smith et al. (2004) found that when using the TADMUS for decision support analysts made fewer false alarms than a control group when assessing threats in a simulated environment, although both groups still missed threats. TADMUS was argued to reduce the cognitive load on operators enabling them to more accurately match patterns of deception with their pre-existing knowledge (Smith et al., 2004). Further research would be required to examine the effectiveness of transferring such automating techniques to other contexts in which deception occurs, and it is anticipated that this may prove difficult to perform.

The Deception Analysis Cognitive Process (DACP – McPherson, 2010) is used for counter-deception and has been used with success in strategic operations. The DACP is split into eight phases (McPherson, 2010). First there is recognition of what to look for in detecting deception; second there should be an evaluation of the deceiver, alongside an awareness of target vulnerabilities and biases; third there is emulation of identifying or recognising how the adversary conducts deception; fourth there is selection of the tools used to detect deception; fifth there is implementation of deception detection techniques; sixth there is collection of information including resolving ambiguities or gaps in knowledge; seventh there is the integration of information to begin the formulation of whether deception is occurring; and eighth there is the determination of whether or to what extent the adversary is conducting deception (McPherson, 2010). The DACP outlines a promising approach to deception detection in operational environments, however, this approach may be improved through further understanding of deception and in particular deception detection strategies.

The CAI (See Chapter 2 - Boon & Gozna, 2009; Gozna & Boon, 2010) may be utilised for deception detection in the military environment. The CAI states that there will be differences across offences that need to be taken into account, for example, that people may be different across different offences and they may be different across and within interviews. In conducting deception a comprehensive knowledge of an adversary is needed including knowledge of characteristics and historical background, knowledge of the deception target (including their own cognitions and biases), current ISTAR, adversary intentions, preconceptions, deployments, their communication and information systems infrastructure (DCDC, 2007). In deception detection this approach may be adapted to analyse the adversary conducting deception as knowledge and awareness of the adversary will enable a more holistic understanding in detecting adversary deception. In detecting adversary deception analysing information and intelligence from a holistic perspective covering verbal and non-verbal behaviour across converging technologies may enable a greater understanding of deception and its detection.

Conclusion:

The nature of military deception is protracted with deception possible in both interpersonal and online environments; therefore there is a need for accurate veracity assessment to prevent vulnerabilities from adversary deception. Traditional forms of deception detection may be employed across these areas, however, to ensure that a more comprehensive assessment of veracity is produced a more holistic approach to deception detection is needed. Using singular verbal or non-verbal cues to deception may not be constructive when we are analysing received information and intelligence it may be more prudent to analyse clusters of behaviour and combine verbal and non-verbal detection methods, furthermore individual differences and personality factors may have an effect on a person's motivations for providing us with information enabling us to produce a more accurate assessment of veracity. If we understand an adversary's cultural background we will also be able to anticipate how an adversary may think and hypothesise what strategies they may use in deception.

Chapter 5: Towards a holistic model of deception: Theoretical developments.

Introduction:

The protracted nature of deception across interpersonal, online and military environments highlights the range of areas where vulnerabilities may occur and the requirement for bespoke and proactive techniques that can assess veracity across these challenging domains. Although accuracy rates in experimental settings for lie-truth judgements are low (Bond & DePaulo, 2006), it is acknowledged that interactions involving low or high-stake deception will likely incorporate a mixture of truth and deception (Bond & Speller, 2009). The varying nature of information presented to deception targets can increase the challenge of assessing veracity with a contingent need to approach the deception identification task by incorporating multiple elements that can be utilized across domains. Chapter 5 draws together the contrasting approaches to deception detection outlined in previous chapters and proposes a model of deception detection where detection approaches are tailored to match the context of interactions and illustrates this approach to three scenarios involving deception.

Traditional Approaches

In developing methods to detect deception, the application of verbal, non-verbal, and paralinguistic techniques have largely focussed upon isolated cues (Vrij, 2008); whilst recent approaches have sought to increase behavioural differences between truth-tellers and deceivers (Colwell et al., 2013). However, these approaches are primarily focussed on detecting deception in interpersonal interactions and using evidence to challenge individuals, which suggests a potential limited application to environments without interpersonal interactions or evidence to challenge individuals' narrative.

Verbal Approaches

Verbal approaches examine differences between truth-tellers and deceivers in how they construct events through verbal content across communication channels. Techniques include SVA (Köhnken, 2004), RM (Sporer, 2004), and LIWC – (Pennebaker et al., 2007). SVA involves a review of relevant information, a semi-

structured interview, CBCA and a Validity Checklist to assess findings related to veracity (Akehurst et al., 2011; Brown, 2010; Vrij, 2008). In studies of CBCA some criteria are present more often and have more support in lie-truth discrimination. For example, 'unstructured production' and 'contextual embedding' appear in more than half of studies involving CBCA, whilst 'self-deprecation', 'related external associations' and 'pardoning the perpetrator' appear in only a handful (Porter & ten Brinke, 2010). Such differences in the CBCA literature may in part reflect the studies being variously conducted as field/in vivo or laboratory/in vitro research. Limitations to SVA and CBCA are outlined in Chapter 2.

RM proposes that recollections of real experiences are developed from our perceptual processes whereas false experiences developed from our imagination will be cognitive in nature enabling discrimination between truthful and deceptive accounts (Bond & Lee, 2005; Masip et al., 2005; Sporer, 2004; Vrij, 2008). RM has shown similar levels of deception detection accuracy and similar limitations to SVA (See Chapter 2). LIWC (Pennebaker et al., 2007 – See Chapter 2) is a technique for analysing conversations in order to understand people's underlying thoughts, motives and emotions (Newman et al., 2003). As an approach LIWC has the greatest potential for analysing verbal behaviour for deception across interpersonal and CMC interactions.

Differential Recall Enhancement Approaches

DRE (Colwell et al., 2013 – See Chapter 2) approaches focus on increasing behavioural differences between liars' and truth-tellers through the use of cognitive mnemonics, questioning strategy and use of evidence, for example, ACID (Colwell et al., 2013), SUE (Granhag & Hartwig, 2015), and cognitive approaches (Vrij, 2015b). DRE is considered to assist honest people in their recall and providing more detailed and verbose statements whilst deceptive people need to work harder to maintain credibility and over-rely on short, carefully constructed narratives (Colwell et al., 2013). These techniques may overcome the paucity of valid cues to deception identified by Hartwig and Bond (2011) although their interview specific context could result in difficulties in application to non-interactive contexts. Although validation in applied settings is required such techniques may be useful in uncovering verbal

deception in interaction whilst application to areas outside of conversational interaction and other communication channels is more difficult to assess.

Nonverbal Approaches

Nonverbal approaches to deception detection have considered behavioural cues including facial expressions and micro-expressions (Ekman, 2001), and finger, hand and arm movements (DePaulo et al., 2003) (See Chapter 2). The challenge is that non-verbal cues are potentially rare and do not guarantee the presence of deception. Furthermore, assigning such cues as being 'deceptive', as distinct from idiosyncratic behaviour or forms of arousal may bring a potential confound and major source of error. In developing a holistic approach to deception non-verbal cues should be judged according to context and used alongside other means of detecting deception to develop a greater understanding of behaviour.

Physical deception has been largely neglected as a research focus although occurs across a wide-range of areas including sports with athletes feigning movements to gain strategic advantage (Sebanz & Shiffrar, 2009) and physical deception in military campaigns such as the use of dummy tanks during World War 2. Such deception in this domain may be uncovered through experience and the knowledge of tactics and strategies used by a potential deceiver and contrasting them with known capabilities. The physical domain can also manifest in the online environment through the proliferation of imagery and video footage of particular events (e.g. fake footage of the 9/11 attacks) and as such requires more understanding to identify particular vulnerabilities. One emerging area of deception is magic and the techniques that are used in magic to misdirect individuals and groups (Gurney, Pine & Wiseman, 2013; Kuhn, Caffaratti, Teszka & Rensink, 2014; Kuhn & Martinez, 2012). Although an audience is aware that deception is occurring, knowledge of the strategies that magicians use to divert attention may increase ability to detect deception in areas where misdirection is common, for example, confidence tricks.

The Holistic Approach

To increase ability in veracity assessment across multiple domains and contexts a holistic approach to deception is required, with strategies tailored to match contextual requirements (See Chapter 2). Through integrating a multiple-cue approach (ten Brinke & Porter, 2011a), multiple sources of information, an understanding of the

CHAMELEON nature of deceivers (Gozna & Boon, 2010), personality and individual differences (e.g. Gozna et al., 2001), and culture (e.g. Bond & Rao, 2004) alongside a situationally applicable use of verbal, non-verbal and DRE approaches, a more accurate assessment of veracity may be possible. The interpretation and identification of deception requires practitioners to incorporate a wide range of factors (Kaina et al., 2011) including an understanding of background history, culture, personality, cognition, surrounding environment and organizational and operational factors (Helman, 2007). Further, an understanding of how deception manifests from motives, contexts and associated decision-making processes is critical to deception detection. This is, especially the case in high stake police, security and intelligence domains where a range of challenges are presented to those charged with assessing, identifying and responding to threats.

The multiple-cue approach combines clusters of verbal, paralinguistic and nonverbal cues and has the potential to enable greater accuracy in lie-truth discrimination in low- and high- stake environments (Porter & ten Brinke, 2010; ten Brinke & Porter, 2011a; Vrij, Akehurst et al., 2004a; Vrij et al., 2000). Using verbal cues including CBCA criteria, non-verbal cues and facial expressions to detect deception in low- and high- stake situations and where rapid judgements are required increases accuracy in lie-truth discrimination to the levels of approximately 80-90% (ten Brinke & Porter, 2011a; Vrij, Akehurst et al., 2004a; Vrij et al., 2000; Vrij, Evans, Akehurst & Mann, 2004). Although such findings may be context specific and base-rates of behaviour may differ, it is important to include a more robust assessment of behaviour rather than focussing upon isolated factors in veracity assessment.

Using multiple sources of information, including multiple narratives, is a requirement of any holistic approach to deception detection and employs the use of contemporary and traditional methods. Granhag, Strömwall and Jonsson (2003) examined pairs of liars and pairs of truth-tellers to uncover how statements may differ between multiple suspects in individual interviews across time. Deceivers were found to be more consistent in their narrative than truth-tellers (Granhag et al., 2003), suggesting that deceivers may overcompensate in maintaining consistency or rely upon a pre-ordained script whilst truth-tellers may recall different areas of an event.

The CAI (Boon & Gozna, 2009; Gozna & Boon, 2010; Taylor & Gozna, 2011 – See Chapter 2) is a personality led forensic interview approach incorporating a wider range of factors than traditional approaches. The breadth and depth of the

complexities involved in understanding the CHAMELEON nature of a deceiver requires knowledge of motive, personality and likely intent in addition to a talented deception detector (Gozna & Boon, 2010). Individual differences may also affect people's ability to detect deception with some individuals more accurate than others (Aamodt & Custer, 2006). Work by Ekman and colleagues (O'Sullivan & Ekman, 2004) have identified individuals who have a 'natural' talent for detecting deception in laboratory environments, and although these findings have emerged from artificial research, it is argued these individuals are best placed to detect deception across a range of contexts. The importance of appropriate skills in the detector of deception cannot be underestimated, particularly when the various domains and mediums of communication are considered. The challenge faced by many organizations is to detect deception across many 'fronts' and to ensure that those techniques used are tailored to the particular need.

Although there is a temptation to identify and respond to deception as it occurs when engaging in interpersonal interactions, the method that has been proven to yield greater results is to collate evidence. This can require individuals tasked with detecting deceit to experience frustration, however moving into an accusatory phase prematurely can result in increased denials. It might be that a denial is irrelevant but this will depend on the stakes and context of the deception being identified. The principles behind the CAI can be integrated into a holistic approach to deception through providing an awareness of the strategies that people use in attempting to appear credible and influence conversational partners and the range of variables that effect interactions and this will be applicable to both interpersonal and online environments.

Understanding personality traits and disorders, individual differences and gender differences (Gozna & Boon 2010; Kashy & DePaulo, 1996; Suckle-Nelson et al., 2010) is critical, particularly because of the effect on how people lie, the situations they lie in, their motives for lying (Gozna et al., 2001) and how people assess the veracity of information (Baker et al., 2012). Knowledge of a sender's personality can increase our ability to detect deception (Vrij & Graham, 1997) because it enables a level of prediction as to how an individual might behave or respond to certain situations or questioning. Individuals with high levels of Machiavellianism can be more motivated to deceive for self-gain and lack honesty (Kashy & DePaulo, 1996; McLeod & Genereux, 2008). Furthermore, manipulativeness and ability to act or role

play are associated with lower levels of guilt when engaging in deception (Gozna et al., 2001).

Liars with greater skills in encoding or monitoring their behaviour have greater control over their presentation when engaging in deception and can adjust their conversational involvement to the person they are interacting with (Burgoon et al., 1999). Such skills enable individuals to appear more comfortable and thus more credible whilst deceiving others including in their responses to questioning (Burgoon et al., 1999; Walczyk et al., 2005). Porter, ten Brinke, Baker and Wallace (2011) found that those participants with greater emotional intelligence (EI) were more effective at simulating false emotions, but not at concealing genuine felt emotions, highlighting the subtlety that individual difference induces when deceiving others. Furthermore, individuals high in EI are less susceptive to deceiver's impression management strategies, thus increasing their ability to detect deception (Baker et al., 2012). This suggests that some individuals will have the ability to feign a reaction to an event but only when their true emotional response does not override this.

In the literature from forensic and clinical mental health and more broadly aspects of occupational literature, certain personality characteristics are relevant to the consideration of deception (See Chapter 2). Specifically pathological lying and instrumental gain can influence motives and behaviour (Taylor & Gozna, 2011) and particular personality constructs and those disorders captured under the Diagnostic and Statistical Manual of Mental Disorders (DSM-IV-TR; APA, 1994). The dark personalities, known as the Dark Triad (Narcissism, Psychopathy and Machiavellianism; Paulhus & Williams, 2002) and most recently the Dark Tetrad which extends the Triad to include the construct of Sadism (Paulhus, 2013) contain aspects of deceitful motives and behaviours. Psychopathy (Cleckley, 1982: Hare, 1970), Narcissism (Raskin & Hall, 1979) and Machiavellianism (Christie & Geis, 1970) should be the focus of certain methods of deception detection with approaches tailored accordingly. It is important to understand the influence of personality generally and complex/disordered personality when evaluating information in high stake contexts and across multiple domains due to the negative impact this might have on the detector of lies.

Cultural differences, religious belief and ideology, and transcultural identity are all areas of important consideration when assessing the ability to deceive and detect deception. When people are communicating in different languages their ability

to detect deception will be affected by language difference leading to implications that may benefit the deceiver or the target (Bond & Rao, 2004; Cheng & Broadhurst, 2005). Further, communication via language interpreters leads to emphasis and meaning being literally 'lost in translation' or misconstrued and is an increasing challenge for those working in police, security and intelligence domains. Deception detection abilities across different cultures are similar to chance and comparable to accuracy rates from research conducted in Western cultures (Al-Simadi, 2000; Bond & Atoum, 2000). The asymmetry of cultural understanding from a Western perspective means that certain vulnerabilities are enhanced. For example, understanding the North Korean psyche will be more challenging for non-allied countries than for those viewing UK or US culture.

Model Development

A holistic approach to deception detection drawing from multiple fields and approaches in developing a unified framework will enable practitioners to access a wider array of tools to detect deception potentially improving ability to assess veracity (Whaley, 2006). An *in vivo* approach to deception detection covers the nuances and dynamic nature of the real world enabling the development of a theoretical ecologically valid approach to deception detection (Boon & Gozna, 2009). In developing a theoretical framework of deception and a framework of individual differences a review of traditional and non-traditional approaches was conducted (see Appendices 5.1 – 5.2). Each proposed element of the deception and individual differences frameworks was assessed by SMEs (N=3) with experience in deception detection (3 – 26 years; M=15.67; SD=11.53). Each SME conducting ratings on a 5 point Likert-type scale of the appropriateness of supporting evidence (Appendices 5.1 – 5.2), an assessment of utility to a holistic model, whether the element is considered universally applicable or context-specific, the elements application to the on- and offline domains, the interactivity of the element (the interpersonal dynamics of the element), and its application to three potential deception scenarios (see Appendix 5.3). Mean averages of rater agreement for the proposed elements and their assessment criteria are outlined below (displayed in Table 5.1).

Element	Appropriate Evidence	Utility	Contextual Specificity	Application Across Domains	Interactivity	Application to Police-Suspect Interviews	Application to Online Deception	Application to Parole Interview
Verbal	5	3.33	3.33	3	3.67	5	1	5
Physical	5	3	2.67	3	3.33	5	1.67	3.33
Social Engineering	5	3.33	3.33	3.33	3.33	4	3.67	3.33
Impression Management	5	3.33	3.33	3	3.33	5	5	5
Written	5	3.33	3.33	3.67	3.33	3.67	5	3.67
Audio	5	3.33	3	3	3.33	4.33	1	3.67
Physiological	5	2.67	2.67	2.67	3.33	4	1	1.33
Mico-Expressions	5	3.33	3	2.33	3.33	4.67	1	3.33
Non-Verbal	5	3	3	2.33	3	4.67	1.67	4
Identity	5	3	3	2.67	4	4.33	5	4.33
Plausibility of Communication	5	3.33	3.33	3.33	3	5	5	5
DRE Approaches	5	2.67	2.33	2	3.33	3.67	1	3.33
Interaction	5	2.67	2.67	3	3.33	5	5	5
Personality	5	2.67	3	2.67	2.67	4.67	3	5
Motivation	5	3	3.67	2.67	3	5	4.67	5
Stakes	5	3.33	3.67	3.67	3.33	5	4.67	5
Demographic	5	3.33	3.33	3.33	3	3.67	3	4
Culture	5	3.33	3.33	3.33	3	3	3	3.67
Religion	5	3	3	3	3	1.67	1.67	2.67
Motive/Intent	5	3.33	3.67	3.67	3.33	5	5	5
Politics & Allegiances	5	3	3	3.33	3	3	3.33	1.67

Table 5. 1: Holistic Element Assessment

Through reviewing relevant deception literature across verbal, non-verbal, DRE approaches and more recent holistic approaches a framework (displayed in Figure 5.1) for detecting deception has been developed, alongside an individual differences framework (displayed in Figure 5.2). Utilizing combinations of these techniques to match the requirements of specific contexts will enable a more accurate assessment of veracity to be developed.

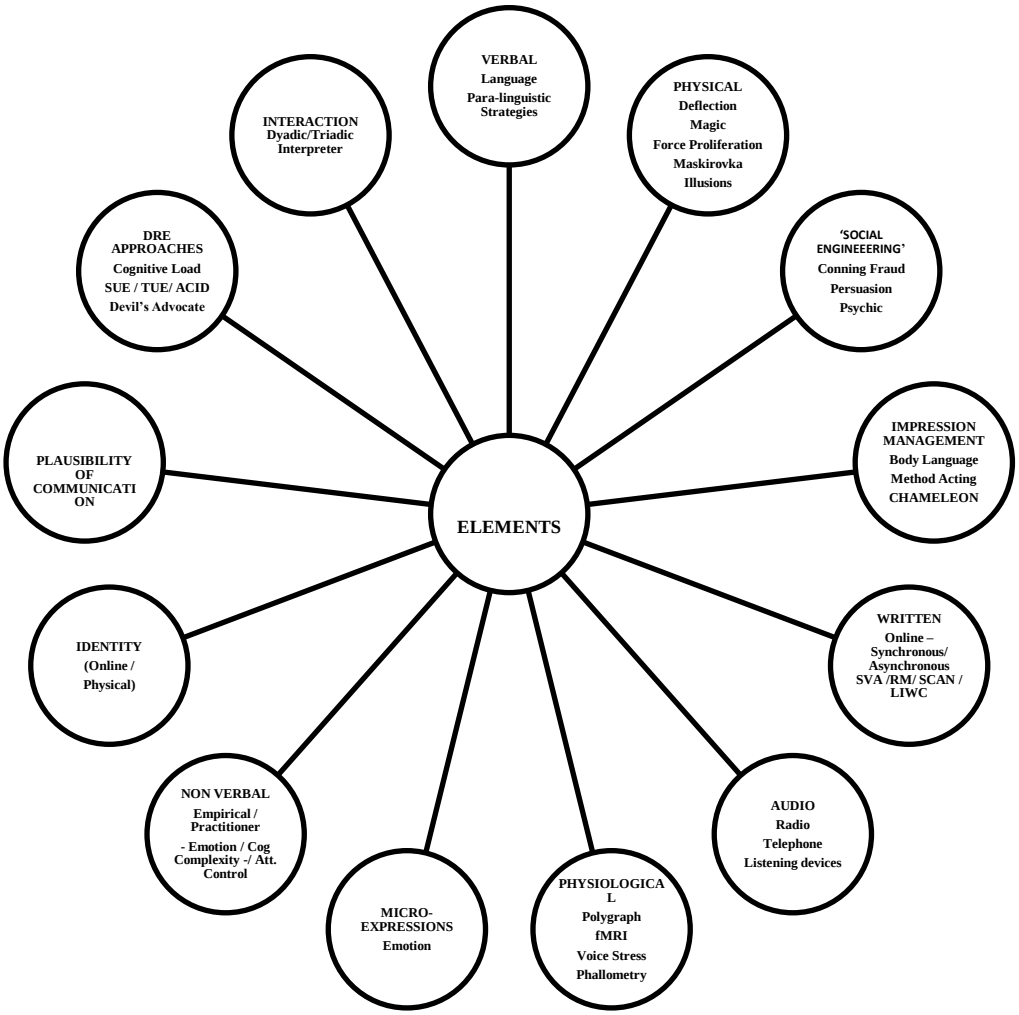

Figure 5. 1: Deception Framework

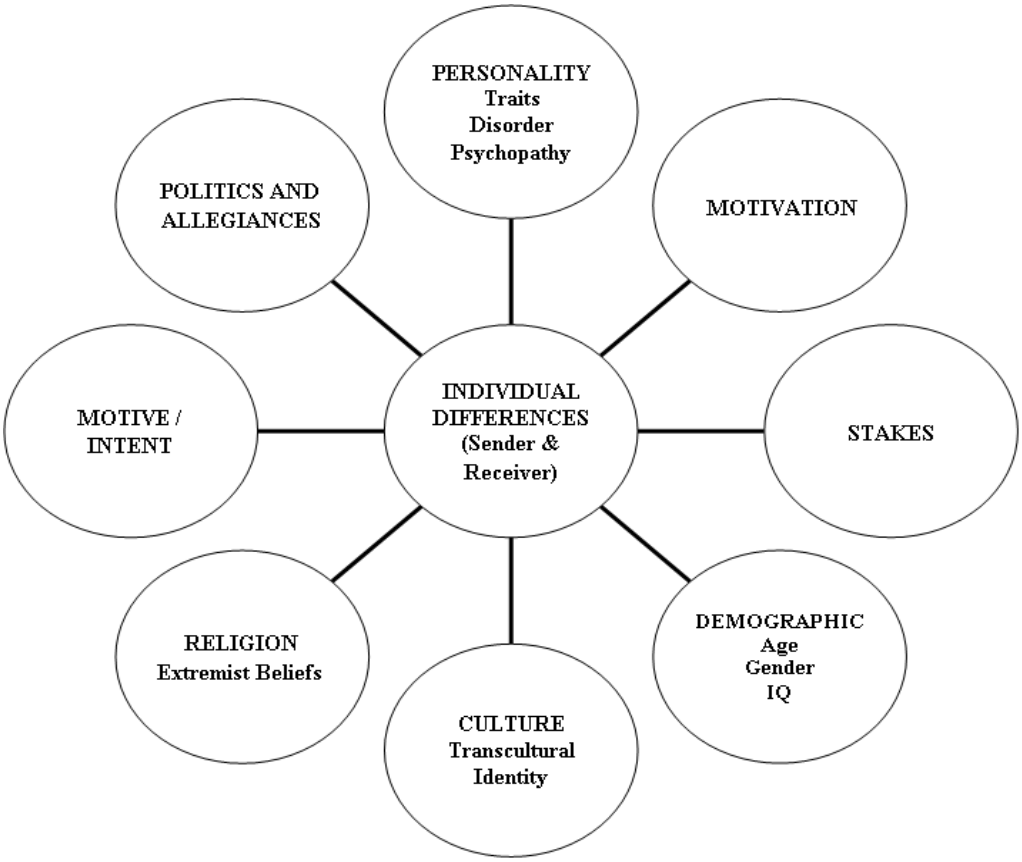

Figure 5. 2: Individual Differences Framework

The theoretical and individual differences frameworks developed from examining the research literature surrounding deception and related areas across interpersonal, online and military domains can further be considered as processes of interaction across time, that are reflective of changes in the environment rather than as singular elements influencing human behaviour. In an examination of forensic behaviour across violence in the night time economy, pathways to female terrorism and hostage negotiation as a sequence of behaviours rather than variables, Taylor et al. (2008) argue that a greater understanding of human behaviour may be developed. Adopting this perspective and that of the CAI (Boon & Gozna, 2009) towards a holistic and tailored approach to deception detection whilst acknowledging personality, individual differences, and culture as surrounding factors effecting behaviour of the deceiver and the target, deception may be considered as: i) occurring where there is a motive; ii) deceivers strategies will reflect type of interaction and communication medium; iii) deception will occur across different communication mediums; iv) deception may be detected through multiple approaches reflecting the type of interaction and medium; and v) deception detection approaches reflect context and availability.

Way Forward

Previous approaches to deception detection are limited as they have focussed on weak and isolated cues that may indicate deception but may also indicate other forms of emotional and cognitive arousal. Furthermore, research has focussed largely on the act of deception in experimental conditions and has neglected real-world motives and contexts (Van Koppen, 2012), background personality and individual differences (Boon & Gozna, 2009), and the impact of culture. People are potentially not good at detecting lies in experimental situations (Bond & DePaulo, 2006) and genuine cues to deception in experimental situations are weak (Hartwig & Bond, 2011) suggesting that in order to improve our deception detection abilities a more holistic approach is needed. An awareness of actuarial conditions involved in detecting deception is required as no approach has yet reached 100% accuracy and it may be considered doubtful that this may be achieved. However, it may be more beneficial to examine clusters of cues to deception coupled with a comparison of behaviours to baseline behaviours and incongruities between verbal and nonverbal behaviours to ensure that a more holistic view of veracity is produced (Aamodt & Custer, 2006; Ekman, 2001, p. 147; Granhag & Strömwall, 2004; Porter & ten Brinke, 2010; Vrij, 2008).

Future refinement and development of the deception and individual differences frameworks proposed should seek to examine a wider breadth of knowledge of deception from areas that have not been previously considered as this may increase our ability to detect deception (Whaley, 2006). Through incorporating academic and practitioner Subject Matter Expert (SME) knowledge across deception, security, and intelligence domains a greater understanding of deception and its detection may be generated. To enhance our abilities to detect future threats and to generate a proactive model of deception the importance of future planning cannot be underestimated. Development of future threat scenarios will enable the generation of robust, comprehensive responses to deception across interpersonal, online and physical domains. In developing a model of deception the operational and experiential needs of practitioners needs to be considered in development of a 'user-friendly' model for individuals with non-psychological expertise.

To ensure the validity and application of an *in vivo* holistic approach to deception, empirical examination of both individual and multiple elements across multiple contexts and domains is required in order to test the robustness, flexibility

and dynamism of the model proposed, and its utility in aiding the task of real-world deception detection. Such testing would ideally be conducted in empirically valid scenarios where individuals are motivated to tell the truth or deceive for instrumental gain. Furthermore, research should be conducted in applied settings, for example, police interviews, involving audio-visual recording, to assess the application of the model to these environments.

Chapter 6: Toward a holistic model of deception detection: SME validation

Introduction:

Traditional approaches to detecting deception have sought to assess veracity through analysing verbal, non-verbal and paralinguistic behaviours (Vrij, 2008). Recent approaches have attempted to increase behavioural differences between truth-tellers and deceivers through increasing cognitive load and tailoring interviewing strategies (Colwell et al., 2013). Reid, Gozna and Boon (2012) propose a theoretical holistic model of deception incorporating traditional and DRE (Colwell et al., 2013) approaches to veracity assessment alongside multiple-cue and multiple-sourcing approaches, and a consideration of the effects of culture, personality and individual differences, motive and mindset. In this chapter I discuss interpersonal, online, military and holistic approaches to deception detection and the further validation of a holistic approach to deception through discussions with SMEs including researchers and practitioners working in diverse fields of deception. The current chapter builds upon the initial model development and piloting outlined in Chapter 5 through incorporating the knowledge of a wide range of SMEs across interpersonal, online and military deception and related areas to develop a comprehensive model of deception detection.

Interpersonal Approaches

Established techniques for detecting deception in verbal communication include SVA (Köhnken, 2004), RM (Sporer, 2004), and LIWC (Pennebaker et al., 2007) (See Chapter 2). Although these techniques were developed for examining interpersonal communication there is potential application to mediated communication. For example, LIWC has been applied to examine linguistic differences between truth-tellers and deceivers in mediated communication (Hancock et al., 2005). However, SVA and RM will have limited application to mediated environments as they require in depth statements with which to analyse credibility and are further reliant on the voluntary provision of information, which, realistically, not all deceivers will be willing or able to provide.

Cognitive approaches challenge deceiver's narrative through increasing cues to deception related to cognitive load, whilst increasing truth-tellers ability to recall events in regard of more detail and accuracy (Vrij, 2015b) (See Chapter 2). Questioning approaches relate to strategic (Hartwig et al., 2006) and tactical (Dando & Bull, 2011) interviewing challenge the deceiver's prepared narratives through evidence-disclosure, resulting in sacrifice of statement consistency to maintain statement-evidence consistency. DRE techniques have the potential to be adapted to online contexts where there is an interactional element (Colwell et al., 2013), although it is anticipated that the effectiveness of these techniques will be mitigated by conversational involvement of the deceiver and the sophistication of the deception employed, including supporting collateral information. In the Reid et al. (2012) model, DRE approaches are identified as part of a holistic approach to deception where their primary use will be in specific contexts involving conversational interaction.

Non-verbal approaches to detecting deception focus largely on isolated cues to deception including facial expressions and micro-expressions (Ekman, 2001; ten Brinke et al., 2011; ten Brinke & Porter, 2011a; ten Brinke, Porter & Baker, 2012), and hand and finger movements (DePaulo et al., 2003; Vrij, 2008) (See Chapter 2). The nature of behaviour displayed in real-world situations is critical to understanding deception, and therefore it is important for the present model development to evaluate the application of research from laboratory settings for ecological validity. For example, although offenders may increase body movements when deceiving to enhance credibility or distract the observer from their verbal content (Porter, England, Juodis, ten Brinke & Wilson, 2008), the content of the discussion, the purpose of the interaction, the personality, motive and mindset all require incorporation into the interpretation of such behaviour from the 'baseline'. Understanding the context of an interaction in addition to baseline behaviour is critical to identify behavioural responses when particular questions are posed (Porter & ten Brinke, 2010) – for example, behaviour may change due to questioning around historical trauma rather than due to deceit. Through monitoring individuals' behaviour discrepancies may be noted and used to direct follow-up questioning (Porter & ten Brinke, 2010). This consideration has applicability across interpersonal and online environments utilising visual content.

Online Approaches

Deception detection in online contexts may be challenging (Giordano, George, Marett & Keane, 2011) and requires consideration of linguistic patterns (Hancock et al., 2005), the use of 'warrants' to confirm a sender's identity (Warkentin, Woodworth, Hancock & Cormier, 2010), 'digital footprints' and 'scent trails' to uncover malign intent (Sandham et al., 2011), and adaptations of computer-mediated investigative interviewing approaches (Colwell et al., 2013; George, Marett & Tilley, 2008; Jenkins & Dando, 2011) (See Chapter 3). In mediated communication deceivers may present as more verbose, have fewer self-oriented pronouns, greater other-oriented pronouns, and use more sensory descriptions than truth-tellers (Hancock et al., 2005). In regard of the influence of third party opinions, Ott, Choi, Cardie and Hancock (2011) examined the linguistic features of online reviews to identify truthful and deceptive opinions and found that truthful reviews contained more concrete and sensorial language and were more accurate about spatial information, whilst deceivers focussed upon elements not directly related to the subject they were reviewing and, in contrast to previous research (Hancock, Curry, Goorha & Woodworth, 2008; Newman et al., 2003), used more positive language. This has implications for understanding the content of opinions and speeches posted in online environments, especially in higher stake situations where such views can sway public belief and behaviour, for example, reviews may have a large impact on auction fraud, whilst deceptive opinions may affect support for on-going regional conflicts.

In the online environment the ability to alter true identity benefits those who engage in malign acts, regardless of the deceptive nature of the behaviour. Hence altering personal information to create a more genuine impression is considered acceptable in some contexts, for example, online dating. However the malign intent of a child sexual offender purporting to be a child while grooming a victim, or a sadistic stalker who presents in a chameleon manner provides a more concerning presentation of behaviour and intent. This becomes further problematic when offending behaviour is online and offline and individuals use aliases to reduce the likelihood of detection. The use of 'warrants' enable links to be examined between an individual's real-world and online identities (Warkentin et al., 2010) and deception may occur more routinely in online chat environments that enable greater anonymity, and less often in the use of email where warrants are visible but can be modified to

mislead. Although examining 'warrants' may be a useful strategy for assessing credibility in low-stakes online interactions, in high-stake interactions the levels of sophistication employed by groups and individuals to cover their identities and tracks are greater, as is the motivation, level of resources and ability to manipulate.

Uncovering hidden deception and malign intent across interpersonal and online environments can include the identification of 'digital footprints', 'digital exhaust' or 'scent trails' that can be coupled with collateral evidence such as surveillance footage (Forster, 2012; Sandham et al., 2011). Although rarely the focus of traditional deception approaches, examining patterns of behaviour, including email communications, online statements and online searches of information about potential targets (Forster, 2012) may enable the identification of concealed actions. In a holistic approach to deception, a proactive stance is required where potential adversaries are being monitored to ensure that information is collated and assessed for deceit. Furthermore, there is potential for collected evidence to be later used in investigative interviews with which to challenge suspect's narratives.

Military Approaches

Approaches to detecting deception in the military environment have focussed on ACH (Heuer, 1999; Stech & Elsässer, 2003; Stech & Elsässer, 2004), the Busby-Whaley Ombudsmen technique, and a more holistic approach to counter-deception advocated by Bennett and Waltz (2007) (See Chapter 4). ACH consists of a series of steps firstly involving the identification of possible hypotheses, secondly listing evidence and assumptions for and against each hypothesis, thirdly drawing tentative conclusions about the likelihood of each hypothesis, analysis of the sensitivity of the conclusion to significant evidence, and lastly the identification of future observations that would confirm or eliminate the hypotheses (Stech & Elsässer, 2003). ACH has been applied to historical incidents of deception including the D-Day landings (Stech & Elsässer, 2003) and the Battle of Midway (Stech & Elsässer, 2004). To counter confirmation biases and aid decision-making Heuer (2005) recommends that there should be an increased emphasis on seeking refutations for hypotheses rather than confirmations. ACH is a promising method of supporting decision-making processes involved in detecting deception, as there is the potential to incorporate a broader range

of factors including human behaviour, motivation, intent and mindset alongside evidence developed from HUMINT.

Whaley and Busby (2002) propose a theory of counter-deception based upon approaches applicable to multiple contexts. They identified nine categories of cues (pattern, players, intention, payoff, place, time, strength, style and channel) which are elements that the deceiver may conceal or reveal during deception (Whaley & Busby, 2002). The major principle of this approach is the 'plus-minus rule' where cues may indicate deception by their presence or absence and the 'congruity-incongruity rule' is suggested where deception may prove challenging to identify and requires further investigation (Whaley & Busby, 2002). Techniques argued to detect deception include: 'Locard's exchange principle' – where a deceiver may leave evidence at the scene and take some away; 'verification' – of the deception; 'the law of multiple sensors' – examination of multiple channels for deceit; 'passive and active detection' – the examination of current evidence and the search for further evidence; 'pre-detection' – where understanding an adversary's deception modus operandi, goals and capabilities may uncover potential deception; 'penetration and counterespionage' – uncovering an adversary's plans through espionage and neutralising adversary operatives to protect target infrastructure; 'the prepared mind and intuition' – where preparation for deception and the intuition to detect it enables counter-deception; and 'indirect thinking and the third option' – the ability to detect potential adversary options for deception is required for counter-deception. Whaley and Busby's (2002) final element is the 'Ombudsman Method' where irrelevances, discrepancies and misdirection are examined alongside indirect thinking and intuition (Bennett & Waltz, 2007). This approach to deception detection appears promising where elements may be adopted towards a holistic approach particularly in regard to using multiple sources of HUMINT, and active detection of deception alongside alternative ways of considering threats.

Holistic Approaches

Holistic approaches to deception have sought to use combinations of verbal and non-verbal cues (Porter & ten Brinke, 2010; ten Brinke & Porter, 2011a), and knowledge of background, personality, cognition, culture and environmental factors

(Kaina et al., 2011) to increase accuracy in detecting deception. Furthermore, as veracity assessment may be adversely affected in cognitively challenging and group decision-making environments (Kaina et al., 2011) there is a need to implement a bespoke holistic approach to deception detection which incorporates an understanding of decision-making to counter potential vulnerabilities.

Bennett and Waltz's (2007) counter-deception approach examines 'intelligence functions' including deception cues, deception detection and exposure, adversary discovery and penetration alongside 'operational functions' incorporating mitigation and exploitation of adversary deception. These functions are argued to be highly interdependent and present deception as a continuum of functions rather than individual elements (Bennett & Waltz, 2007). Human reasoning and self-assessment of our own beliefs and methods of intelligence gathering and intelligence-gathering channels will identify potential vulnerabilities potentially mitigating the effects of deception (Bennett & Waltz, 2007). Multiple channels of information should be used to ensure a greater range of HUMINT with which to assess credibility (Bennett & Waltz, 2007). Threat and situation assessments are required to understand the influences and circumstances in which deception may occur (Bennett & Waltz, 2007) and such approaches parallel more recent psychological approaches to understanding high-stakes future intent (Gozna & Lawday, 2015). Bennett and Waltz (2007) recommend incongruity testing and ACH as tools for detecting deception, and combined with psychological deception detection methods outlined by Reid et al. (2012) more accurate credibility assessment will occur.

In order to increase accuracy in the detection of deception in complex operating environments, Reid et al. (2012) propose using a combination of verbal, nonverbal and paralinguistic cues to deception alongside a consideration of personality and individual differences, motive, mindset and consideration of decision-making. Cues are argued to reflect context and may not be applicable across all instances of deception (Adams & Harpster, 2008; Harpster, Adams & Jarvis, 2009). The multiple cue approach to the detection of deception has to date incorporated consideration of low-stakes (Vrij, Akehurst et al., 2004a), high stakes (Porter & ten Brinke, 2010) and rapid judgement (Vrij, Evans et al., 2004) environments and hence such evidence supports a holistic, tailored approach. Reid et al. (2012) propose multiple-sourcing alongside multiple-cues whereby different sources of information can be examined for consistency increasing available knowledge for credibility

judgements. The incorporation of the CHAMLEON Approach (Gozna & Boon, 2010) into a holistic approach to deception by Reid et al. (2012) highlights that individual's behaviour and the strategies they use to present themselves change across contexts. The impact of culture, religiosity and belief system on deception is highly relevant to emerging global challenges and its incorporation into a holistic approach to deception is required (Reid et al., 2012).

A bespoke, tailored approach to deception creates individual assessments of veracity across situations and ultimately meets the requirements of practitioners. An *in vivo* approach to research proposed by Boon and Gozna (2009) outlines guidelines for conducting research whereby a theoretical model is first proposed and refined before validation and application to real-world environments. The current research seeks to refine and expand the theoretical holistic approach to deception developed by Reid et al. (2012) through interviews with SMEs in deception. In military environments there are limited opportunities for practitioners to develop skills necessary in countering adversary deception and in deceiving others; to overcome this limitation Whaley and Busby (2002) and Whaley (2007) propose an incorporation of knowledge from a wide range of areas to identify techniques used to uncover deception. Through adopting an *in vivo* approach to research and incorporating a wide range of SME knowledge a more robust approach to deception detection can be developed.

Method

Participants

An opportunity, snowballing sample enabled the recruitment of 19 SMEs in deception and influence. The sample comprised 14 (74%) males and 5 (26%) females, of which, 15 (79%) were European and 4 (21%) were North American. The average length of expertise within the SME cohort was 17.6 years (SD = 11.46) ranging from 5 to 42 years' experience. Participants had expertise in both singular and multiple areas of deception and influence. Overall participants had expertise in the following areas: interpersonal deception (N = 12), online deception (N = 6), military deception (N = 5), influence (N = 2) and personality (N = 4).

Materials

A series of parallel interview schedules were developed for the interpersonal, online and military domains of deception and credibility assessment (Appendix 6.1). Interview questions were designed to elicit SMEs knowledge of deception to validate and refine the holistic model of deception developed in Chapter 5. Interview questions were focussed around the environments in which deception occurs, strategies that deceivers use to convince others of their credibility, the potential impact of personality on deception, current strategies of deception detection and potential ways to improve them, parallels between the domains of deception, and the identification of potential future threats. For example, the interpersonal deception section contained questions including "*What strategies do you believe that liars use in their attempts to influence people that they are telling the truth? (Include strategies related to verbal and nonverbal impression management, the concealment of emotions etc.)*", whilst the military deception section contained questions including "*Which are the more concerning forms of deception in the military context – online or physical/behavioural?*".

A digital Dictaphone was used to record interviews which were stored securely on an Ironkey to ensure security and transcribed verbatim. Hardcopies were additionally stored in a secure environment.

Procedure

Participants were initially approached via email or face-to-face contact and followed up by an email inviting them to participate in research seeking to develop a holistic model of deception. Of the 41 individuals who were asked to participate in the research, 19 agreed. A general interview schedule was included as an email attachment to enable participants to examine the questions being asked of them, although interviews were further tailored to SMEs areas of expertise. Due to the nature of some of the work undertaken by SMEs approached, two different interview schedules were made available to participants, one interview schedule including interpersonal and online topics (Appendix 6.2) was provided to participants without appropriate clearances and another interview schedule including interpersonal, online and military topics (Appendix 6.1) was provided to those participants with appropriate

clearances. Once participants had read through the information sheet (Appendix 6.3) and agreed to participate in the research they were informed that their data would be anonymised and stored in a secure location, that they had a two-week window to withdraw their data if they so chose and that their data would be used as part of a PhD thesis and in further journal articles (See Appendix 6.4 for consent forms). Participants were then interviewed at a location of their choice and convenience. Following the interviews participants were debriefed about the aims of the research and thanked for their input (see Appendix 6.5). Ethical approval for this research was granted by the Ethics Committee of the School of Psychology of the University of Lincoln (see Appendix 6.6).

Data Analysis

Responses were transcribed verbatim and treated from a critical realist perspective (Braun & Clarke, 2006; Braun & Clarke, 2013) where responses were considered as reflecting reality whilst acknowledging they were generated as part of the interview procedure. An explanatory thematic analysis (Guest, MacQueen & Namey, 2012) at the semantic level was conducted according to the conventions outlined by Braun and Clarke (2006 - See Appendix 6.7). First, familiarisation with the data set occurred through transcription, and initial idea generation. Second, initial coding of relevant data was conducted. Third, codes were gathered together into themes. Fourth, themes were reviewed against coded extracts and the entire data set. Fifth, clear naming and defining of themes was conducted, followed by the sixth stage, construction of the report. The explanatory thematic analysis resulted in the generation of 5 meta-themes across the process of deception.

Analysis and Discussion

Findings

Analysis of SMEs responses led to the identification of 5 meta-themes related to the process of deception and its detection, including the meta-themes of ‘Deceiver’, ‘Intent’, ‘Deception Tactics’, ‘Interpretation’ and ‘Target’ (See Figure 6.1). These

themes put forward a comprehensive view of deception from the acts of the deceiver, to the intent to deceive, to the components of the deception itself, the processes of interpreting information, and the elements of the target itself, including a focus upon target vulnerabilities (See Appendix 6.8). These themes highlight a wide range of techniques for examining veracity and through adapting these techniques to match specific contexts then more accurate deception detection can occur.

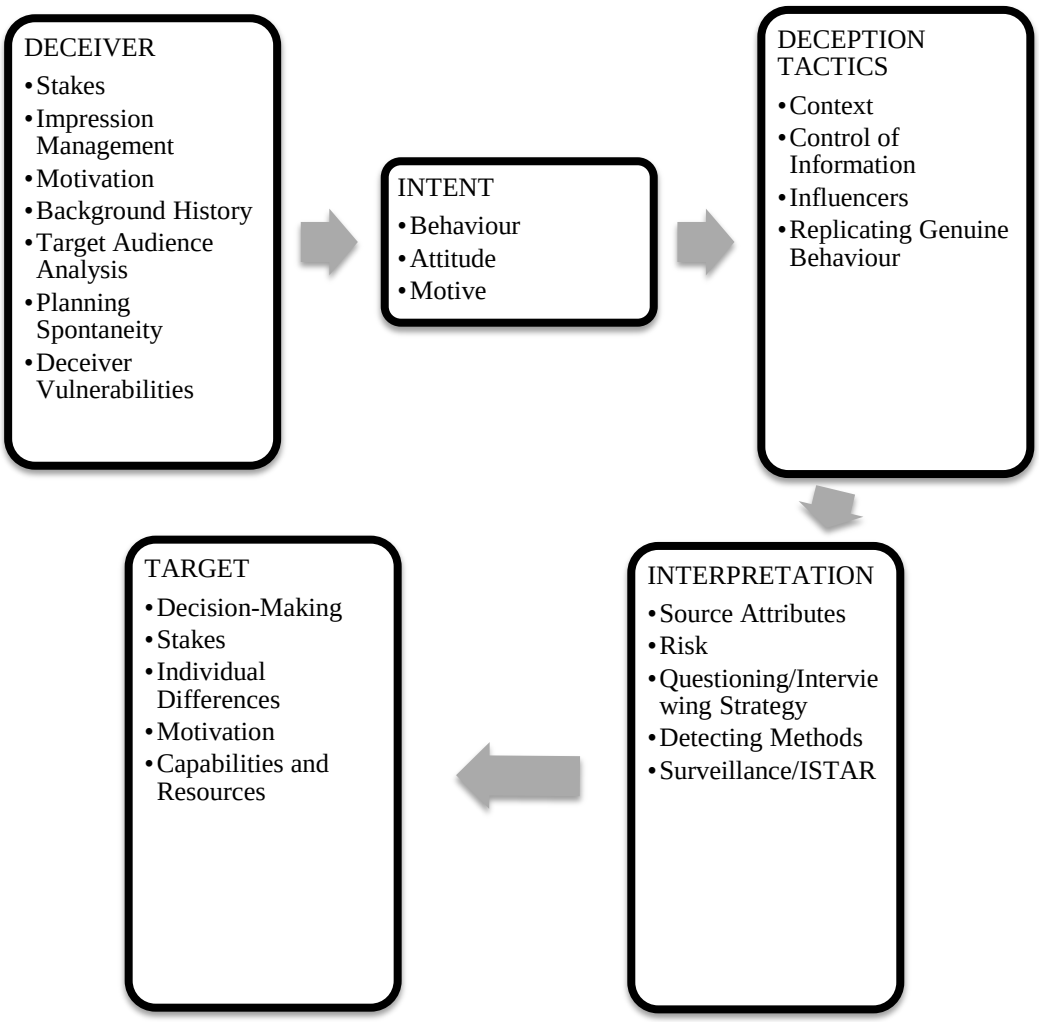

Figure 6. 1: Holistic Model of Deception

Deceiver

The first meta-theme identified from the dataset was *'Deceiver',* this meta-theme incorporates sub-themes related to *'Impression Management'*, *'Stakes'*, *'Motivation'*, *'Background History'*, *'Deceiver Vulnerabilities'*, *'Target Audience Analysis'*, and *'Planning Spontaneity'*. The themes examine factors influencing how the deceiver makes decisions regarding deception and their potential ability to appear

credible whilst deceiving. *'Impression Management'* examines the strategies which the deceiver uses to appear credible to others across different environments.

> *"I think it's about creating an impression in the other person of credibility erm and honesty and being able to attach to it so so to an extent the strategies can be within the lie erm that the information presented is such that someone believes it to be credible and plausible but you can also have additional peripheral elements that you present with your verbal deception that just allow an impression to be given that you are a credible person"* (Participant A: Lines 118-123)

Participant A highlights how '*Impression Management*' requires strategies in face-to-face encounters that are credible, plausible and create an impression to another that you are honest.

> *"so there's gonna be a a different form of impression management I suppose it's gonna be at least with a strictly you know linguistic communication you're not gonna be you're not gonna be as concerned about er what's going on your face or your body language you're gonna be mainly focussed on you know convincing the person of whatever it is you're trying to convince them through your er language"* (Participant C: Lines 817-821)

Participant C highlights the changes in forms of '*Impression Management*' that reflect the online environment, where communication can be primarily verbal and less emphasis is placed on non-verbal behaviour to convince another person.

> *"we know from research that when people say that when they lie or intend to lie they try to say as little as possible"* (Participant G: Lines 173-174)

Participant G shows how '*Impression* Management' can be very simple in how individual's attempt to adjust their behaviour to appear credible, highlighting the variety of strategies that individuals will use to appear credible in different contexts. Previous research has focussed upon how people manage their statements (e.g. Hartwig et al., 2010) and body language (e.g. Hines et al., 2010) and Gozna & Boon (2010) proposed a series of distinct personality-based behaviours which are used to influence and persuade others of their credibility. Online approaches to impression management have focussed upon the design features of websites and how people present themselves, for example, in online dating profiles (Toma, Hancock & Ellison, 2008). Incorporating *'Impression Management'* into a holistic model of deception will enable practitioners assessing veracity in security and intelligence settings to

understand the ways in which people and information are constructed to appear credible according to context.

The *'Stakes'* of a situation, what the deceiver has to gain or lose, will affect a deceiver's approach to deception in how they formulate deceptive content, how they may react across contexts and their success at deception.

> *"individual differences account for a lot in terms of what the stakes are to the deceiver whether they're high or not how they need to present it and also how they perceive the target of their lie to be in terms of the likelihood of them being found out"* (Participant A: Lines 106-109)

Participant A explains how the stakes of a committing an act of deception effect how the deceiver presents themselves and how they perceive the target of their deception. Participant B highlights how the stakes of a situation may also make it easier to detect deception as it increases behavioural cues to deception.

> *"so looking at high stakes situations not only are you more likely to be able to detect the lie erm because of like motivational impairment and er all kinds of other theories erm that accompany behavioural cues to deception when the stakes are high"* (Participant B: Lines 65-67)

High-stakes situations may prove more challenging to appear credible (e.g. ten Brinke et al., 2011) than in low-stakes situations where deceit may have little consequence and impact on cues to deception. High-stakes situations are argued to increase anxiety and cognitive load in some deceivers leading to the identification of cues to deceit (Porter & ten Brinke, 2010). However, in strategic environments deceivers may place more emphasis upon carefully designing deception plans to avoid highlighting cues to deceit. Hence the sophistication of the planning from the perspective of the deceiver should mirror the ability of the lie detector to identify the likely strategies and focus of the deceit.

The *'Motivation'* of the deceiver will have an impact on how they deceive others and the deceiver's motivation is closely linked to the *'Stakes'* of the situation:

> *"well erm I would say from the (noise) motivated to succeed (noise) will do more of the elaborate lies and erm that might then lead to your downfall because the wonderful thing is the more you tell people erm the more there is to follow up"* (Participant H: Lines 270-272)

> *"you know so if you're really motivate if it's very important to you that you succeed in the lie you are likely to feel more anxious about it erm which might produce some cues but also obviously anxiety can affect your frontal functioning so it might exacerbate the effects of cognitive load ... so you*

> *might also produce more cues related to cognitive load erm and also the more motivated you are the more you're going to try and control your behaviour um which will probably have the converse effect or the inverse effect that your behaviour becomes more inhibited or rigid"* (Participant R: Lines 563-571)

Participants H and R both highlight that the motivation to succeed in an act of deception has the potential to negatively effect the deceiver as they will create more elaborate acts of deception which may be later verified whilst also increasing potential cues to deception related to cognitive load and body language. Participant Q explore another important element of motivation, in the need to understand a deceiver's motivation for conducting deception.

> *"so surely you you cannot conduct interviews or understand deceit or anything unless you know the motivations behind why people commit you know you've got that that's the key isn't it I'd say one of the major keys to understanding or trying to at least understand"* (Participant Q: Lines 832-835)

In interpersonal deception, motivation has been found to impair deceiver's ability to deceive others (DePaulo, Kirkendol, Tang & O'Brien, 1988) as the deceiver's cognitive load and anxiety may increase leading to cues to deception appearing (Porter & ten Brinke, 2010). However, this may not occur in all circumstances as individual differences will have an effect on cognitive abilities during interviewing. In the online environment '*Motivation*' has an enhancing effect on deception where cues available to detect deception in the real world are lacking (Hancock et al., 2010). This would suggest that motivated deceivers will seek to influence others through online communication channels where there is an increased chance of success; however, this may be mediated by the deceiver's expertise in deception and the impact of communication channels. *'Motivation'* will affect how far the deceiver is willing to plan their deception and this may vary according to goals and the context in which to achieve these goals.

'Background History' of the deceiver, including their personality disposition, individual differences, their culture and language, and previous interactions with the target is required in a holistic model of deception as this will affect their interactions with the target and the strategies they use to deceive them. This includes their mindset at the commencement of the deceit.

> *"and then the really clever people think of lots of alternative ways of of achieving it but the expert deceivers got the the third option which is*

> *something so out the box so left field that it it can't even be classified in the alternative ways of thinking"* (Participant D: Lines 377-379)

Participant D highlights how a deceiver' expertise will enable them to develop more creative ways of conducting deception, whilst Participant F focuses on behaviours associated with explicit personality types which influence their interactions with others. Participant Q further expands on this through discussing a deceiver's background with criminality and interactions with law enforcement.

> *"is psychopathic erm they are certainly capable of lying but the objectives there are a combination of impulsiveness or can be a combination of compulsiveness and complete disregard for anybody else erm in relation to whatever their objective"* (Participant F: Lines 262-265)

> *"from the type of person they are the background whether they've had interaction with the police before what type of crime we think they might have committed"* (Participant Q: Lines 551-552).

Knowledge of an adversary's background history, culture, individual differences and mindset factors (Kaina et al., 2011; Porter, ten Brinke, Baker & Wallace, 2011) can increase our ability to accurately detect deception; the current research further incorporates knowledge of personality and its impact on deception, alongside knowledge of previous interactions with the adversary and what the outcomes were. Therefore the model considers the dynamic assessment of deception over protracted periods of time in addition to situations where an individual lies in a spontaneous manner. An individual's culture and language will present additional challenges to veracity assessors as this affects how they will view information presented by a deceiver from another culture (Gerwehr, 2006). In multicultural operating environments an awareness of the impact of culture is required to avoid decision-making errors. Gozna and Boon (2010) highlight that individual's background histories and previous experiences will affect how they will behave in future interactions, and these same principles can be applied to the holistic model of deception.

'Deceiver Vulnerabilities' will affect how the deceiver will appear credible to others and open up pathways of detecting deception. The impact of emotional arousal, cognitive load and decision-making biases will adversely affect the deceiver's ability to appear credible.

> *"more cognitive load it just increases all of those um you know theoretical er bases for cues to deception and so I think that its its huge in terms of increasing the amount of behavioural leakage"* (Participant B: Lines 296-298)

Participant B states that through increasing cognitive load there is a potential to increase behavioural leakage in the deceiver and which in turn increases theoretical cues to deception making the deceiver more vulnerable. Participant R identifies a potential deceiver vulnerability in the specific context of emotional appeals where deceiver's display fake emotions which may enable them to appear credible but actually help to detect their deception.

> *"when I'm looking at appeals um one of the things that I've noticed is that people who are making deceptive appeals they tend to put on these displays of fake emotions they pretend to cry quite often"* (Participant R: Lines 64-67)

The lack of emotions in some contexts adversely affects deceivers whereby they fail to present emotions that are expected and that truth-tellers often experience (ten Brinke & Porter, 2011a). Cognitive load adversely affects deceivers as it reduces capacity to present a credible argument (e.g. Vrij, Granhag, Mann & Leal, 2011a). These vulnerabilities in the deceiver can be exploited during the *'Interpretation'* phase of the model and cues to deceit identified.

When seeking to influence others, especially in strategic contexts, *'Target Audience Analysis'* is often conducted which will enable an influencer to develop an enhanced understanding of the audience and identify key individuals and organisations to target.

> *"I think a lot of the time we don't we think that there's a one size fits all approach to how people tell a lie but I think from the liars' perspective they have to tailor their deception to the target"* (Participant A: Lines 112-114)

Participant A states that there is a need to understand that deceiver's tailor their act of deception to the target and that not all deceivers use the same strategy. Participant K expands the concept of undertstanding the target further through incorporating specialist knowledge from cultural advisors and academics before developing further knowledge through interaction with potential targets. The approach stated by Participant K expands how understanding the target may be expanded from just one target to larger audiences where different influence approaches may be required.

> *"when you're doing a target audience analysis phase you should er especially with social media that's when you start so not only do you have you're cultural advisors not only do you have your you know you're academics coming to you and saying well this you know I've researched the history of this country and this is how it developed blah blah blah all that could be stuff that you need to know you should immediately have a team starting to talk to people in the area to see if if the er if academias er research balances with today's reality"* (Participant K: Lines 580-594)

> *"provide false information er but they they're able to provide that false information because their audience or the subject that that they're trying to convince wants to be convinced and because they are in at that time under those emotional conditions they are gullible"* (Participant M: Lines 380-383)

Participant M shows how understanding a target's emotions at different points of time may make the more vulbnerable to deception. An influencer's ability to successfully conduct *'Target Audience Analysis'* affects their ability to influence the target through whatever strategy has been selected for influence, and deceiver skill will play a role in how effective this is (Mackay & Tatham, 2011). Although *'Target Audience Analysis'* as a concept has emerged from strategic environments the idea of influencers carefully selecting and exploiting the target can be seen in both interpersonal and online environments.

The deceiver may carefully develop or spontaneously perform an act of deception to a specific target and *'Planning Spontaneity'* emerged as a sub-theme in the data.

> *"if you're looking at an interview somebody who had been arrested and has been suspected of commitment of an offence so we are kind of the inquisitor in changing them if I am trying to convince somebody that I am a wonderful person erm in interview for a job or be it er to join er I don't know a secret (noise) I have to actively do something more to convince somebody I have to more… that I am a genuine person so that's its its different levels and different levels of preparation"* (Participant H: Lines 227-234)

Participant H explains how different levels of preparation are required for different interviewing situations where there is a need to appear credible. Alternatively Participant J explains how there is often a lack of planning in some phishing emails as the deceiver is targeting people who are more vulnerable meaning they do not place as much emphasis on the presentation of the emails.

> *"you typically find all kinds of English grammatical and usage errors um rarely do you find er graphics or or email layouts that actually look professional um so I think people just don't people are are kind of going for*

> *the low hanging fruit anyway and I guess for for the low hanging fruit you don't really need to have that professional of a of a presentation"* (Participant J: Lines 222-226)

Participant N shows how individuals with specific personality types, for example, psychopaths, may not place much emphasis on planning and are more spontaneous in their behaviour.

> *"they actually they aren't what ive seen in c connection with cases is psychopaths aren't very good liars what they do is deny anything anything they did until er the the point in time that it's a er its its undeniable"* (Participant N: Lines 247-249)

The level of planning that the deceiver puts into their deception will affect their ability to convince others that they are credible (Strömwall & Willén, 2011). The current research highlights that poor planning can be identified or that deceiver's strategies may subsequently collapse from challenges to their narrative. However, in long-term strategic deception, planning will play far great emphasis highlighting adversaries should be monitored and assessed for threat.

Intent

A need to understand the '*Intent*' of the deceiver emerged from the data as a meta-theme, whereby understanding an individual's motive and intent for engaging in deception will enable preparation for adversary deception to prevent vulnerabilities (Gozna & Lawday, 2015). From the analysis it is apparent that SMEs believe that deception only occurs when there is intent:

> *"if you're interviewing somebody who you know has a sexual interest in children and you know that they want to be released from prison they will be highly motivated to present to you in a positive honest and credible fashion regardless of whether or not they have every intention on release from prison of abusing another child"* (Participant A: Lines 197-201)

Participant A shows how intent to be released from prison will guide the manner in which an offender will present themselves as credible and honest, whilst Participant F shows an individual being interviewed will have an intent to deceive to avoid incriminating themselves.

> *"and suddenly it all becomes very hazy at important bits charitable people might say that this is dissociation I'm saying it's because they don't want to*

> *go there and incriminate themselves further motive and personality once again"* (Participant F: Lines 51-53)

Participant M highlights intent for deception through the need to increase survivability in a combat situation.

> *"is making somebody believe I'm somewhere where I'm not if I'm in an aeroplane and I'm very much aviation based if I'm in an aeroplane and somebody is looking at me with a radar then er I want to destroy his perception I want to er effect his situational awareness even if its only slightly it can cau it can give me a greater survivability*' (Participant M: Lines 37-41)

These differning intents to deceive whether to avoid being incarcerated for an act of criminality or to increase survival chances in a combat situation show a strong need to understand that deception occurs which there is intent. Past research has sought to uncover malign intent through questioning strategies (Granhag & Knieps, 2011), however it may be more pertinent to understand intent as part of a holistic approach to deception where the intent to deceive is regulated by adversary aims and motives and how situational elements will affect the timing of when deception occurs. This presents implications for how research into deception detection is conducted where participants are often automatically assigned to deception or truth-telling conditions excluding an individual's intent to deceive in specific contexts.

Deception Tactics

The third meta-theme of *'Deception Tactics'* emerged from the dataset where the role of context is highlighted and different tactics for controlling information, influencing and deceiving the target are outlined. Sub-themes related to *'Deception Tactics'* include: *'Context'*, *'Control of Information'*, *'Influencers'*, and *'Replicating Genuine Behaviour'*.

'Context' plays a large role in which tactic the deceiver will employ against the target, and how the situation, including communication channel, may change the form of interaction. Online communication has changed elements of the deception context, where there is a greater, scale and reach of deceit and the potential for anonymity in interactions.

> *"at deception then erm exactly the same principles are employed now really er with regard to the military some of the contextual changes are obviously the rise of technology a proliferation of communications technologies extended*

> *range ability to deploy force at range for example use of drones"* (Participant D: Lines 54-57)

Participant D has extensive experience in military deception and agues that the same principles exist behind deception although there has been contextual changes with the development of communication technologies which have increased the range for deception.

> *"we're now doing amazon reviews where we look at the language of deception and um we find some really interesting things around (real) reviews fake reviews and they differ depending on erm what the context is and I think this is a really important point that the online world is making very clear to us and that is um when we look at language and deception we can't be thinking about universal cues erm if we ever should have been thinking about universal cues … something like Pinocchio's nose in language we need to think about what is the actual deception context and what are the psy psychological and psycholinguistic implications for that context"* (Participant P: Lines 187-197)

Participant P has been conducting research across a variety of online environments and his identified linguistic differences between different mediated environments. Participant P refers to the need for understanding cues to deception within context rather than seeking cues to deception that are the same across all contexts. Participant R describes context from a different perspective where individual's being interviewed for crimes will have different deception tactics reflecting their specific crime.

> *"these people being interviewed you know some of them are lying about erm burglary some of them are lying about murder some of them are lying about rape and I think it's likely that behaviours related to deception might also be context specific"* (Participant R: Lines 98-101)

Previous research into deception has generally ignored the context of deception and how this impacts upon interactions between individuals and whether cues to deception are actually generalizable across contexts. Research by Gozna and Boon (2010) highlights understanding that people will behave according to the context they are in, this can further be expanded to how groups and organisations may seek to influence and deceive others according to the situation. The holistic model of deception places a strong emphasis upon context and the situational factors that may lead to a deceiver choosing a specific tactic of deception.

'Control of Information' enables the deceiver to control what information is portrayed to the target. Through increasing the amount of information the target receives, the deceiver can increase target ambiguity and cognitive load as there will be more information to process reducing the target's ability to respond to a situation. Through decreasing the amount of information the target receives target ambiguity is also increased as the target will have less information with which to assess veracity.

> *"why is it that that individual erm suddenly became excessively fluent erm and it may be of significance but in psychoanalytic erm therapy erm blocking and fluidity erm excessive fluency are key signs when someone's trying to conceal something"* (Participant F: Lines 568-570)

Participant F refers to the deceiver controlling information through either reducing or increasing information as an attempt to conceal other information. This tactic is also shown by Participant H who describes a form of deception by concealing information completely.

> *"the main thing then if you do it about law enforcement context that's the key thing I don't have to tell you a lie I just say no comment"* (Participant H: Lines 131-132)

Participant R highlights a more extensive form of fluidity discussed by Participant F where deceivers may increase the amount of information they provide, potentially as a strategy to distract the target.

> *"pleaders displays of erm fake emotion er some of them go into very long involved detail about um their version of events that day"* (Participant R: Lines 247-249)

Deceivers often seek to control the way in which they present information whether verbal, non-verbal or physical to others and previous research has highlighted that deceivers may give shorter statements to their target to control their narrative and ensure consistency (Hartwig et al., 2007), but may also increase the number of individual details within their statement (Morgan et al., 2011), potentially as a way of distracting the target from the deceptive content. Understanding how the deceiver may control information and the way in which they choose to release this information is required in detecting deception as this affects the strategy used to detect that deception.

'Influencers' highlights the various strategies that individuals use to persuade the target of their credibility.

> *"so those th so those are the strategies actually you know so the gangmaster would say I'm ru I'm I'm doing this fraud to keep all these people er er you know from from starvation you know that's what I'm doing it for the greater will"* (Participant E: Lines 557-559)

Participant E refers to gangmasters who often hire groups of foreign workers to perform manual labour in agricultural and industrial employment. However, there is also fraud in such areas which the deceiver seeks to justify that they are actually performing a service through employing individuals.

> *"an image erm from um Syria of a father with his baby in his arms and a woman er reaching out to him er and behind er are are some really really badly destroyed buildings and it looks like this guy is running away with his child and his wife is in a state of panic actually what came out was the fact that erm the guy is walking down a street in Syria erm and his wife is just asking can you give me the baby … but it's been manipulated now why I use that situation is if people are involved in the Syrian mission area"* (Participant K: Lines 200-208)

Participant K outlines a case of deception from the on-going Syrian Civil War, where a powerful, emotionally arousing influencer is used through portraying vulnerable individuals as fleeing conflict when that is not the case. However, the image may manipulate the target's perception meaning they will be more likely to believe the image. Participant T describes another form of influence through the use of humour as this again effects decision-making in the target and they will be more likely to find such deceptions credible.

> *"just to pick up on any sort of rumour and as long as it's entertaining and interesting and fits with their world view then they'll repeat it you know"* (Participant T: Lines 430-432)

There are a large number of techniques that can be used to influence others in everyday interactions, whether deception is occurring or not. Research examining persuasion tactics has identified key areas for influencing others (Cialdini, 2007) which has been applied to real-world activities, for example, advertising strategies. However, examining the impact of influence tactics in deception has been relatively neglected and the proposed model seeks to incorporate these.

One technique of appearing credible to others is through *'Replicating Genuine Behaviour'*, whether the perception of genuine behaviour is based upon lay beliefs or

upon actual understanding of how to replicate behaviour an awareness of both will be required to understand how differing individuals and adversaries will behave.

> *"heh er I mean they were definitely trying to replicate emotions that you would expect to be present in the those er situation and which were present in the genuine pleaders so they were trying to replicate this expression of sadness"* (Participant B: Lines 180-182)

The ability to appear genuine is an important tactic for deceivers; Participant B describes how deceptive pleaders attempt to replicate emotons which genuine pleaders show. Participant D provides an example of physical deception from warfare where there reality was replicated through making equipment look like it had been destroyed.

> *"they also did um created a made it look like a er they'd been a fuel explosion and half the stuff was wrecked when it (wasn't)"* (Participant D: Lines 1450-1451)

Participant T refers to how phishing emails replicate genuine emails through offering plausible messages that the target may expect in their daily lives.

> *"erm you know a senior office gets er an email that says hi Fred its Mike erm I'm gonna be in London next week I'm going to this conference erm you might be interested in it you know just you are the links below and you say it well you know dear friend Mike's a good guy and he's in London next week I wonder what conference is about and you know you you click on it and then you're infected"* (Participant T: Lines 707-710)

Replicating genuine behaviour and appearance is a strategy that individuals seek to use in deceiving others (Hartwig et al., 2010), however, this strategy may not always be effective as certain behaviours are harder to replicate in some contexts (Porter & ten Brinke, 2010). To date psychological research into exploring how deceivers replicate genuine behaviour has mainly focussed upon examples of deception in low-stakes environments where individuals may not have time to develop a plan for deception that often occurs in the strategic environment. Further understanding of the strategies that people use in high-stakes environments to appear genuine to others is required.

Interpretation

The fourth meta-theme of *'Interpretation'* emerged from the dataset and lists the varying techniques and areas of focus which are used in the detection of deception across different communication mediums. Identified sub-themes for the *'Interpretation'* enable an analysis of information: *'Source Attributes'*, *'Questioning/Interviewing Strategy'*, *'Detection Methods'*, *'Surveillance and ISTAR'*, and *'Risk'*. The wide range of techniques uncovered for assessing veracity may also enable the development of bespoke strategies for detecting deception reflecting contexts in which deception occurs. '*Source Attributes'* examines factors (consistency, plausibility, credibility and prominence) that enable a source, whether the source is an individual in a face-to-face setting or information in an online domain, to appear credible.

> *"ways of detecting inconsistencies er erm sort of assessing um how congruous information is and (noise) indicators of detecting anything anomalous or that stands out"* (Participant D: Lines 719-721)

Participant D refers to examining information to look for inconsistencies or information that stands out with which to detect deception. Whilst Participant P refers to how the plausibility of online contexts helps to make judgements of credibility.

> *"simple as that to the look and feel of the er online space"* (Participant P: Line 519)

Participant E explains how looking at the consistency of information can help uncover deception through making sure that two sets of information matches each other.

> *"line a he ga he he he obviously you know to the officer yeh this is my name date of birth address line s line c so we we course lying and no such person exists okay line s line c cos well I I was coordinating the activities so I said well look this is an easy one here line a and line c will have two matching dates of birth"* (Participant E: Lines 1076-1080)

Through examining these factors of what makes the source itself credible a more considered judgement of the source may be made. Past research in interpersonal deception has examined these factors as separate elements (e.g. Vrij, Granhag, Mann & Leal, 2011b) rather than seeking to combine them enabling more accurate judgement about information. Research examining the credibility of websites has taken a more holistic approach to examining the source for credibility (e.g. Fogg et

al., 2003). However, offering clear guidance on factors that enable analysis of sources across different communication channels as outlined above is required.

When interacting with potentially deceptive individuals in dyadic or triadic conversation '*Questioning/Interview Strategy'* plays an important role in the generation of information to examine for deception or identify discrepancies for further examination, although as a factor it may not be applicable to all contexts.

> "*get them wound up then you go through you break it down as part of the cognitive interview break it down into their topics again ... you let them go through each you summarise it they agree to it even though you know half of its lies"* (Participant Q: Lines 664-668)

Participant Q, an expert in interviewing, outlines how the cognitive interview may be used for questioning deceivers through discussing their statements extensively before requiring the deceiver to agree to their statement even if this contrasts with external evidence. Participant E refers to another questioning strategy probing questions are used to generate information.

> *"don't know its re a really good questioning strategy to ah ask an open question followed by a series of probing questions ... and as the interview goes along and you you know really get that micro details of the story er then then then (just) the ratio of probing questions increases to the open question because you really are you're getting them to talk on one thing"* (Participant E: Lines 1278-1284)

Participant B refers to CBCA, a series of criteria assessments, as a strategy for detecting deception. To be effective Participant B states that CBCA requires a good interview highlighting the importance of the interviewing and questioning strategy in deception detection.

> *"we've got a pretty good idea in terms of CBCA which of course requires um requires a good interview if you've got a crappy interview then you can't do the CBCA properly erm so I think you need to marry the interviewing er with deception detection"* (Participant B: Lines 390-393)

Questioning and interviewing of individuals has often generated information for further analysis and also has the potential for usage in conjunction with some verbal methods of detecting deception. Its inclusion in a holistic model to deception is required for usage in when we are interacting with individuals in interpersonal environments, and modern approaches to detecting deception have been employing this (e.g Colwell et al., 2013; Vrij, Granhag, Mann & Leal, 2011a).

Established techniques for examining information and intelligence for veracity emerged from the data set and *'Detection Methods'* provide a range of techniques to detect deception from psychological and military backgrounds. Techniques to detect deception include: verbal, non-verbal, pictorial, neuropsychological, paralinguistic and techniques used by military and intelligence personnel.

> *"and I think that's why er again as you know one of the few nonverbal behaviours that in recent times has been found across a number of studies to significantly relate to lying is a a reduction in hang hand and finger movements"* (Participant G: Lines 309-312)

Participant G refers to one deception detection method examining hand and finger movements as these behaviours may reduce when an individual is engaged in deception. Participant C describes another detection method where individuals are required to maintain consistency to appear credible, if they do not maintain consistency then their deception may be detected.

> *"so identifying particularly particular kinds of linguistic patterns I think is is definitely the way to go there er the parallels you still have to keep your story straight"* (Participant C: Lines 822-824)

Participant D describes military and intelligence analysis approaches for detecting deception. Such approaches have been developed to detect deception in warfare.

> *"there are a number of formal military processes for conducting intelligence analysis er which are geared around detecting deception there's Heuer's analysis of competing hypotheses… er there's the er there are various signal detection methods er there's the Whaley Busby ombudsman technique"* (Participant D: Lines 104-109)

These techniques will be utilised as part of a toolbox approach where the techniques used will fit the requirements of the situation. Previous research has begun to explore the use of multiple techniques to detect deception (e.g. Bennett & Waltz, 2007) and has found higher accuracy levels in detecting deception (Porter & ten Brinke, 2010).

To uncover intelligence for assessment *'Surveillance and ISTAR'* will enable the generation of information through varying surveillance techniques depending on the availability of channels for retrieving information and evidence.

> *"is the question cos some would say well how do you know it's true why would anyone tell you and then you have to make some judgements and you have to look at other sources to see how they tie in you know if if somebody if you*

want to know about say erm a Chinese aircraft for example I mean there are there will be pictures of it on a on a web" (Participant G: Lines 101-105)

Participant G refers to one technique of generating information for detecting deception through checking different sources for information including searching online. Participant D describes how with technology the ability to search for more information to check facts has become wider and faster which will enable a greater ability to generate information for analysis.

"the technology erm which means things like ISTAR become more … wide ranging more real time er more forms of sensor erm computer technologies for supporting decisions support sense making situational awareness" (Participant D: Lines 60-63)

Participant K describes the potential of social media for identifying key influencers which will aid the detection of deception.

"that's what social media is all about monitoring erm output from a potential influencer" (Participant K: Lines 513-514)

Through adapting the use of ISTAR techniques to examining deception in interpersonal and online environments changes in the way in which deception is detected can be made. ISTAR techniques traditionally generate intelligence about an adversary which can then be used to inform decision-making, whilst in approaches to deception detection focus has been on identifying cues to deceit, though combining both approaches verbal and non-verbal behaviour can be analysed alongside other intelligence, which reflects how deception is often detected in real-life (Park et al., 2002).

In examining information for veracity there is always an element of *'Risk'* involved where incorrect decisions may have large consequences for organisations and an ability to examine risk is required.

"some techniques that are heavily statistical for example so you're numerical abilities may come into into play there erm the critiquing processes the ability to again juggle risk and probability" (Participant D: Lines 406-409)

Participant D refers to the difficulties the target may have in detecting deception through numerical techniques and how they assign risk. Participant P discusses how deception occur across multiple environments and the associated

challenges in responding to some deceivers who may use coded messages to communicate.

> *"touches on all aspects of human life in the same way that mainstream deception does so you see everything from terrorism concerns where erm terrorists use chatrooms to send coded messes messages to each other"* (Participant P: Lines 303-306)

Participant Q highlights that there is no universal way of detecting deception for every individual in every context, and that strategies need to be tailored to the environment. Such an approach will reduce the risk of reliance upon techniques that will be effective in some but not all contexts.

> *"but there's no in my opinion that exists full proof way of detecting deceit … that every time it will catch the right person in the right scenario the right situation"* (Participant Q: Lines 283-285)

The impact of *'Risk'* on deception has been generally neglected within the deception literature with techniques focussing upon percentage of accuracy. However, in real-life situations relying upon probability may prove problematic, through adopting multiple approaches to deception detection adverse risk can be reduced.

Target

The final meta-theme of *'Target'* emerged from the dataset which focuses upon the targets decision-making abilities and the factors that may affect the ability to accurately detect deception. Identified sub-themes that will affect the target are: *'Decision Making'*, *'Stakes'*, *'Individual Differences'*, *'Motivation'*, and *'Capabilities and Resources'. 'Decision Making'* and how we make sense of the world is key to effectively detecting deception and mitigating risk. However, decision-making biases and attribution errors that the deceiver exploits may adversely affect the ability to detect deception.

> *"better to allow them to have to work to assemble patterns of information to generate sense of what what's going on and that to be wrong but because they've invested the cognitive effort in forming that understanding that whole range of factors working for you there in terms of er investment"* (Participant D: Lines 221-224)

Participant D argues that the target's decision-making may be exploited if you present them with limited information and they then invest resources in an attempt to detect deception, meaning that they will be more biased in their decision-making.

Participant E discusses a further bias in decision-making where the target did not check for further information as the deceiver made the target feel like they had succeeded in their job, therefore they were more vulnerable to deception.

> *"that motivation to be a social worker actually ... the amount was congruent was was was was quite consistent with her story cos if this this story happened to be true ... then she'd been a success as a social worker"* (Participant E: Lines 836-841)

Participant J discusses the need to be suspicious about individuals you are interacting with, which may prove a useful strategy for detecting deception in some circumstances. However, it may also lead to incorrect judgements regarding credibility.

> *"that er you know you're never gonna know for sure who you're dealing with and you should probably be suspicious ... erm all the time of of the person you're talking to and and what they represent themselves as"* (Participant J: Lines 454-458)

Decision-making biases have partially explained the reasons for poor accuracy in detecting deceit (See Chapter 2), and an awareness of these biases and the decision-making process and their impact on the '*Interpretation*' process is recommended to reduce error in detecting deception.

The *'Stakes'* of a situation will affect the receiver and how they will judge a situation where potential deception may be occurring,

> *"looking at high stakes situations not only are you more likely to be able to detect the lie erm because of like motivational impairment and er all kinds of other theories erm that accompany behavioural cues to deception when the stakes are high er but I mean if you catch that lie it actually makes a difference"* (Participant B: Lines 65-68)

Participant B examines the impact of stakes on the deceiver as this will affect their ability to appear credible and enhance the target's ability to more accurately detect deception. Partipant G states that the stakes and consequences of deception affect both the deceiver and the target.

> *"I'd put that in obviously wed put in the the stakes the consequences er both for the the sender of the truth lies ... and for the receiver"* (Participant G: Lines 580-583)

Participant P outlines how the stakes are a high for the target across a range of areas where there is potential for deception.

> *"the stakes you know couldn't be higher when it comes to terrorism to fraud er say even somethings that seems as simple as hiring people (you know there's) fraud there erm can huge costs for a company erm"* (Participant P: Lines 309-312)

In everyday acts of deception the lies are often of little consequence and are used to maintain social harmony (Bond & DePaulo, 2006) therefore the target of that deceit may be less likely to question a situation, however, in cases where deception of strategic interests then stakes and the consequences of a decision will have a larger impact on the target and how risk is assessed.

A wide range of *'Individual Differences'* affect our ability to accurately judge others including the detection of deception:

> *"I've looked at you know aspects of the judge so are people who are high in emotional intelligence better at judging another person's personality"* (Participant S: Lines 19-21)

Participant S describes how individuals with specific personality traits are better able to judge others personality, suggesting that individuals with such traits will best be placed to detect deception. Participant G also argues for the selection of individuals best placed to conduct interviews through their past performance.

> *"in the broader context of if you were selecting people who already within an organisation of an ef (noise) fective nature … to be the hopefully be their best interviewers… interrogators … what things would you be looking for and of course the most reliable guide is their past performance"* (Participant G: Lines 550-558)

Participant Q provides an example of someone with the ability to effectively provide support for interviewing.

> *"I have the profiler knowledge but also have the interview knowledge so I work on cases a lot I'm working on about seven cases at the moment giving advice on the interview"* (Participant Q: Lines 145-148)

Through understanding receiver individual differences (e.g. Aamodt & Custer, 2006) awareness of potential vulnerabilities and advantages emerges, and through understanding these vulnerabilities the risk of deception can be mitigated. There are

also implications in the selection of interviewers and deception detectors based upon their personality and individual difference factors.

The target's *'Motivation'* to detect deception will affect their ability to accurately detect deceit.

> *"got that motivational impairment effect I mean if we know that something is really on the line then you're trying much harder you're feeling more emotion"* (Participant B: Lines 292-294)

Previous research has identified that motivated individuals are often less accurate in detecting deception (Porter et al., 2007), and this may occur where individuals rely upon lay strategies for detecting deception rather than cues identified by research. However, where individuals are motivated and have expertise in identifying genuine cues to deceit, motivation may have a reduced impact on decision-making errors.

The target's *'Capabilities and Resources'* will affect their ability to detect deception. Through understanding what *'Capabilities and Resources'* are available the target will be able to ensure that they can recover information across varying communication channels and they will have sources of expertise with which to analyse received information.

> *"say oh I was so drunk I can't remember anything right and people say that a lot in terms of strategies oh I can't remember which is brilliant because then if they say ooh but we've got evidence of you doing this there's CCTV footage of you"* (Participant H: Lines 172-175)

Participant H provides an example of how target resources may be used in the aid of an investigation as they can provide evidence that an individual is deceiving. Participant O states that we can use resources including experts to provide advise on a deceiver's claims which can help in the judgement of credibility.

> *"you know this is much talked about you say and he says well gosh how could they have done that you know when we would be struggling if we tried to do the same thing you see so this is why you need technical experts to say can they actually enrich u uranium"* (Participant O: Lines 167-170)

Participant P refers to the benefits of mediated communication as a resource in detecting deception where deceptive messages or communications will stay there forever meaning that such information can be verified against other available evidence.

> *"recordability er the traces that all of our conversations leave is we can now take (there's that) email message I can now go compare that to other peoples er sense of the events or actual physical evidence"* (Participant P: Lines 259-261)

The resources that are open to the target will enable a greater understanding of a situation whereby drawing information across differing communication channels together with expertise in the area deception may be occurring in will enable more informed judgements of credibility.

Implications

The Holistic Model of Deception (HMD) integrates IDT (Buller & Burgoon, 1996) and features-based models of credibility (Fogg, 2002; Johnson, Grazioli, Jamal & Zualkernan, 1992; Hilligoss & Rieh, 2008; Metzger & Flanagin, 2013; Whitty et al., 2012). The HMD proposes that the context will affect the form of interaction used, how the deceiver will behave in that interaction and the techniques that will be deployed to detect deception. Multiple interpretation techniques, where applicable, can be used simultaneously to detect deception building upon recommendations by Porter and ten Brinke (2010) that multiple-cues to deception are used, multiple sources will also be used alongside an awareness of personality, individual differences, mindset and background history.

Reid et al. (2012) proposed a model of deception which focussed upon the elements of deception and provided a framework of individual differences that will affect the deceiver and the target. The HMD has built upon this model through the examination of diverse deception elements and individual differences across the deceiver, their intent, their strategy, ways of interpreting information and the target. Understanding the process of deception requires an iterative process where the HMD will be revised in future to reflect new developments in understanding of the deceiver, their intent, deception tactics, strategies of interpreting information and assessing credibility and understandings of the target's decision-making processes.

Limitations

The current research sought to validate and refine the holistic model of deception detection proposed by Reid et al. (2012) by incorporating SME knowledge from a range of research and practitioner backgrounds. Volunteer bias suggests that this sample may not be representative of all SMEs in the field of deception and related areas and the specificity of the sample is acknowledged. Difficulties were encountered in accessing participants from security and intelligence backgrounds due to security reasons; therefore it is acknowledged that there may be other techniques for detecting deception in military environments that the research has not incorporated into the holistic approach to deception. Further research may seek to address this issue through securing access to an SME sample with military and intelligence backgrounds.

Future directions

The current research validates and refines the model of deception proposed by Reid et al. (2012); however, although strategies used to detect deception proposed by this model are outlined by SMEs there is a requirement for empirical validation. Future research should seek to examine the applicability of the model to real-world deception challenges, with a specific focus towards the online environment as an emerging area of risk. 'Red teaming' presents an option for large scale strategic deception where rigorous analyses of the HMD can occur in a simulated real-world environment (DCDC, 2013).

The *'Deceiver'* meta-theme proposed by the current research states a strong requirement for cultural knowledge to understand an adversary and what may affect their attempts at deception and its detection. In addition the focus on the mindset of individuals at any particular time when there is the need to identify future intent and incorporate an understanding of risk requires broader perspectives to be taken. Developing knowledge of these strategies may mitigate risk of deception. However, there is a current lack of research into cultural variations in how people deceive and seek to deceive others, specifically in the online environment, which presents additional challenges in an increasingly globalised world where individuals from differing cultural background interact on a daily basis, therefore future research should seek to address these concerns.

In assessing credibility there is always an element of risk involved in making decisions, especially in high-stakes environments where there may be large consequences for incorrect decisions. The current research has identified as sub-theme of *'Risk'* in interpreting information that future research should examine in depth to acknowledge the element of risk involved in detecting deception and produce guidelines for reducing risk in high-stakes deceit.

Conclusion

In seeking to develop a holistic model of deception, the model proposed by Reid et al. (2012) has been partially validated and refined through a series of interviews conducted with SMEs across the field of deception and influence. The current findings expand upon previous research into deception through formulating deception as a process whereby the deceiver conducts deception to achieve an aim motivated by their goals and affected by their culture, personality and mindset. The deceiver's choice of tactics and strategies with which to deceive will be reflective of context, communication channels and resources available to them, whilst the target has a large number of techniques with which to interpret information and assess credibility, and the target in turn will be affected by individual differences, available resources and decision-making ability. In conclusion, it is argued that taking a more holistic perspective to viewing deception is required to mitigate risk.

Chapter 7: Cultural similarities and differences in credibility assessment strategies in interpersonal and online domains.

Introduction:

In a historically infamous lack of understanding of culture, mindset and ideology, following a meeting between the then UK Prime Minister Neville Chamberlain and the German Chancellor Adolf Hitler a paper was signed declaring that Hitler would not start a war leading to Chamberlain to declare on 30th September 1938 "*peace for our time*", however war was declared less than a year later. This lack of understanding had massive implications upon the rest of the 20th Century and in shaping modernity, indeed Bond and Rao (2004) argue that in all cultures there are those who seek to exploit others, highlighting the need to understand culture to increase resilience against risks posed by deception. With the rise of the Information Age, globalisation and CMC, there is an even greater need for understanding the impact of culture, mindset, religiosity and ideology on assessing information related to forensic and security interests. The current research defines culture as "*the set of cognitions and practices that identify a specific social group and distinguish it from others. In essence, 'culture' is the expression of group norms at the national, racial and ethnic level*" (Hogg & Vaughan, 2005, p.616). The current chapter aims to build upon the cross-cultural research discussed in Chapters 2 and 3 and the need for understanding how individuals assess credibility across differing communication mediums, which with increasing technological usage is required to increase resilience against deception. In this chapter interpersonal and mediated approaches to credibility assessment and the impact of culture on credibility assessment are examined before presenting broad strategies used by individuals from Western and Eastern cultures to assess credibility across these domains.

Psychological research into credibility assessment has primarily focussed on behavioural cues to deception which individuals from Western cultures use in attempts to accurately assess veracity, whilst neglecting behavioural cues to the truth, and differences in strategies used by other cultures to assess credibility. More recent research has begun to focus on the strategies people use to assess credibility in online environments. The impact of immigration means that there are now large émigré populations globally, increasing the requirement to understand the relationship

between culture and decision-making regarding credibility – for example distinguishing between true and false asylum applications and the identification of illegal immigrants.

Interpersonal Credibility Assessment

Individuals from Western cultures hold a variety of beliefs regarding cues to credibility in interpersonal encounters, with a particular emphasis on eye gaze aversion and grooming behaviours (Vrij, 2004). These beliefs are held by a wide range of individuals from lay and law enforcement backgrounds (Vrij, 2004) and are argued to be linked to beliefs regarding deception as an emotionally taxing behaviour (Ekman, 2001). In particular cues associated with nervous behaviour (Lakhani & Taylor, 2003; Taylor & Hick, 2007) and incongruent emotional displays (Kaufmann, Drevland, Wessel, Overskeid & Magnussen, 2003) are believed to indicate deception across situations and such cues to deception are believed to increase in high-stakes contexts (Lakhani & Taylor, 2003; Taylor & Hick, 2007). Further, Taylor and Hick (2007) found that some individuals believe eye contact to increase in more serious deception, potentially as tactic to appear more credible in response to the belief that deceiver's avoid eye contact. Cues related to plausibility, consistency and greater length of verbal response are further related to perceived credibility and truthfulness rather than deception (Lakhani & Taylor, 2003).

In a meta-analysis examining the relationship between perceived cues to deception and actual cues to deception, Hartwig and Bond (2011) found that a potential explanation for why people are bad at detecting deception in interpersonal contexts is due to a lack of strong cues to deception rather than people using incorrect cues when detecting deception. Hartwig and Bond's (2011) findings suggest that people may actually be more discerning in their strategies used to detect deception than previous research suggests (e.g. Global Deception Research Team, 2006[1]).

[1] Toivo Aavik (University of Tartu, Estonia), Maher Abu-Hilal (United Arabs Emirates [UAE] University), Farrukh Z. Ahmad (Institute of Professional Psychology, Pakistan), Ramadan A. Ahmed (Kuwait University, Kuwait), Barbara Alarco (University of Lima, Peru), Benjamin Amponsah (University of Ghana, Ghana), Adnan Atoum (Yarmouk University, Jordan), Hadi Bahrami (Tehran University, Iran), Peter Banton (University of Aix-Marseille, France), Veronica Barca (State University of Moldova, Moldova), M. Basualdo (University Columbia of the Paraguay), Corina Benjet (National Institute of Psychiatry, Mexico), Uma Bhowon (University of Mauritius, Mauritius), Charles F. Bond, Jr. (Texas Christian University), Trevor I. Case (Macquarie University, Australia), Letizia Caso (University of Rome, Italy), Derek Chadee (University of West Indies, Trinidad and Tobago), Robert Churney (College of

However, these findings apply explicitly to the interpersonal environment and may not be transferrable to mediated conditions where deception cues and detection may differ due to the relatively recent rise of mediated communication in overall human evolution (Hancock, 2015). Furthermore, Hartwig and Bond (2011) do not specify whether their meta-analysis incorporated research examining the perceived cues to deception of those from other cultures rather than Western ones, it is argued to be

---

Micronesia, Micronesia), Marjorie Courtoy (Université Catholique de Louvain, at Louvain-la-Neuve, Belgium), Hrach Datevyan (Yerevan State Linguistic University, Armenia), Dahourou Donatien (University of Ouagadougou, Burkina Faso), Cecilia Gastardo-Conaco (University of Philippines, Phillippines), Guido Gendolla (University of Geneva, Switzerland), M. Arif Ghayur (Slippery Rock State University, Slippery Rock, PA), Vijai N. Giri (Indian Institute of Technology, Kharagpur, India), Raja Gunawardhane (University of Colombo, Sri Lanka), Hyuseog Han (Chonnam National University, Korea), Maria Hartwig (Goteborg University, Sweden), Nida Ul Hasanat (Gadjah Mada University, Indonesia), Dora Herrera (University of Lima, Peru), Angelika Hofhansl (University of Vienna Medical School, Austria), Roberta Holland (University of Malta, Malta), John Horgan (University College of Cork, Ireland), Shih-Tseng Tina Huang (NCCU, Taiwan), Rosnah Ismail (Universiti Malaysia Sabah, Malaysia), Tina Javahishvili (Academy of Sciences, Georgia), Lucy Johnston (University of Canterbury, New Zealand), Andreas Kapardis (University of Cyprus, Cyprus), Mujde Ker-Dincer (Ege University, Turkey), Maria Kerslake (National University of Samoa, Samoa), Anna Khaltourina (Academy of Sciences, Russia), Darya Khaltourina (Academy of Sciences, Russia), Jennifer Ah Kion (University of Mauritius, Mauritius), Guenter Koehnken (University of Kiel, Germany), Flora Kokkinaki (Athens University of Economics and Business, Greece), Mladen Koljatic (Pontifica Catholic University of Chile, Chile), Aleksandra Kostik (University of Nis, Serbia and Montenegro), Jenny Kurman (University of Haifa, Israel), Kang Lee (University of California San Diego, San Diego, California), Elena Levintsa (State University of Moldova, Moldova), Ladislas Lovas (University of P.J. Safarik, Slovakia), Jaume Masip (University of Salamanca, Spain), Carlos Ruiz Matuk (University of Santo Domingo, Dominican Republic), Annika Melinder (University of Oslo, Norway), Harald Merckelbach (University of Maastricht, Netherlands), Rachi Messili (University of Algiers, Algeria), Lynden Miles (University of Canterbury, New Zealand), Patricia Thuli Mngadi (University of Swaziland, Swaziland), Margaret M. Munyae (University of Botswana, Botswana), Jasmina Nedeljkovic (University of Nis, Serbia and Montenegro), Felix Neto (University of Porto, Portugal), Marika Niemi (Institute of Occupational Health, Finland), Shanta Niraula (Padma Kanya Multiple Campus, Tribhuwan University, Nepal), George Nizharadze (Academy of Sciences, Georgia), Takashi Oka (University of Tokyo, Japan), D. E. M. O'Sullivan (University College of Cork, Ireland), Boguslaw Pawlowski (University of Wroclaw, Poland), Marcos E. Pereira (Federal University of Bahia, Brazil), Carolina Platon (State University of Moldova, Moldova), Sandhya Rao (Texas Christian University), Shawn Reynolds (Institute of Behavioral Research), Bernard Rime (Université Catholique de Louvain, at Louvain-la-Neuve, Belgium), Olga Rodriguez (National University of Colombia, Colombia), Ruthie Rono (U.S. International University, Kenya), Incze Roxana (Babes-Bolyai University, Romania), Velko S. Rus (University of Ljubljana, Slovenia), Marion Schulmeyer (University Privada de Santa Cruz, Bolivia), Li Shu (Institute of Science, China), Monica Silva (Pontifica Catholic University of Chile, Chile), Roma Simulioniene (Klaipeda University, Lithuania), Iva Stuchlikova (University of South Bohemia, Czech Republic), Iva Sverko (Institute of Social Sciences, Croatia), Victoria Talwar (McGill University, Canada), Therese M. Tchombe (University of Yaounde, Cameroon), Sonia Tifner (National University of San Luis, Argentina), Colin Tredoux (University of Capetown, South Africa), Martin Voracek (University of Vienna, Austria), Aldert Vrij (Portsmouth University, UK), Kip Williams (Macquarie University, Australia), Rex Wright (University of Alabama), and Yuching Zhang (Institute of Science, China).

crucial that an understanding of the strategies that people from other cultures use to assess credibility is required.

When seeking to assess credibility of others the primary focus of research has been on the detection of deception rather than that of truth (Adams & Jarvis, 2004). SVA (Köhnken, 2004) was initially developed to distinguish between truthful and deceptive accounts of children's accounts of sexual abuse in Sweden and Germany and has since been applied to assess credibility across other areas of deception and deception in other cultures. When applied to the context for which is was developed SVA and its CBCA component has achieved high accuracy in use by experts in distinguishing between truthful and deceptive narratives of child sexual abuse (Akehurst, Menton & Quandte, 2011). However, these techniques have to date not been applied to CMC and will be affected by people's experience of CMC alongside the interactional context.

In an examination of the everyday strategies that people use to detect deception, Park et al. (2002) asked participants to recall information, including how they discovered the lie, from a previous deceptive interaction. Participants relied on information provided by third parties and on physical collateral evidence with deception being detected over a period of time ranging from days to months (Park et al., 2002). These findings highlight further methods of credibility assessment beyond eye gaze aversion (Global Deception Research Team, 2006). As Park et al. (2002) did not rely on immediate judgements of credibility and enabled participants to report strategies other than observing verbal and/or nonverbal behaviour their findings are argued to more accurately reflect how individuals detect deceit in the real world. It is likely that general strategies of assessing credibility will be transferrable across cultures; however, understanding the subtle differences in how individuals from other cultures present themselves in turn reflects judgements of credibility formed by those from other cultures (Vrij, 2004).

Computer-Mediated Credibility Assessment

Credibility assessment is required across the digital domain where issues reflect a continuum of detecting deception in mediated interactions to assessing credibility of websites or phishing emails. Increasingly society is reliant on information that is only available online furthering the need for understanding online

credibility assessment strategies (Metzger & Flanagin, 2013). There is evidence that people feel more confident in detecting deception online when there is more familiarity or predictability – any alteration from this indicating deception (Boyle et al., 2008); however, the reliance on the familiar can generate biases which could impede the reliability of such strategies (Boyle et al., 2008; Carlson & George, 2004; Carlson & Zmud, 1999).

People may use source credibility (Briggs, Burford, De Angeli & Lynch, 2002), reputation (Metzger & Flanagin, 2013) and trust (Blanchard, Welbourne & Boughton, 2011), website design (Flanagin & Metzger, 2007; Fogg et al., 2003) visual and textual information (Toma, 2010), warrants (Blanchard et al., 2011; Thompson, 2009; Warkentin et al., 2010) and reviews (Ott, Cardie & Hancock, 2012; Ott et al., 2011; Thompson, 2009) to assess credibility of information with strategies varying across source and context (Flanagin & Metzger, 2007) (See Chapter 3). Some of these strategies are anticipated to be universal whilst others will be more affected by cultural differences in which features are used to assess credibility. Generally, strategies used to assess credibility in interpersonal environments will be employed in CMC reflecting the relatively recent advent of recorded conversation (Hancock, 2015).

Research examining trust in online advice has found that people rely upon cues including good website design, source credibility, predictability and personalisation (Briggs et al., 2002). Trust is increased by adhering to group norms and online group identity (Blanchard et al., 2011). Perhaps unsurprisingly therefore, individuals who adhere and belong to the same online community may be perceived as more credible than outsiders. Individuals who present greater links to their real-life identity when communicating online are more likely to be perceived as trustworthy (Blanchard et al., 2011; Warkentin et al., 2010). Trust, however, is context dependent, with Toma (2010) arguing that in online dating greater trust is associated with textual than visual information due to the potential for manipulation. It is further likely that individuals will seek further information from other sources to ascertain credibility and trustworthiness (Park et al., 2002).

Credibility Assessment across Cultures

Deception is argued to be an evolutionary trait found in varying forms in cultures throughout the world (Bond & Rao, 2004). Individuals are argued to make sense of the world through their prior experience which is shaped by their culture and ideology and this will affect socially determined decision-making processes (Furner & George, 2012; Gerwehr, 2006). Culture has been broadly conceptualised as reflecting behavioural differences between individualistic and collectivist cultures (Hofstede, 1983), which are argued to inform how we interact others and whether emphasis is placed upon the individual self or the collective self (Bond & Rao, 2004). Culture may further be conceptualised as impacting on an individual's cognition, mindset and behaviour whether that be within a social identity, an occupational identity to a larger national or supra-national identity. In particular religiosity has a strong impact on mindset and behaviour as evidenced by groups such as the IRA and the Islamic State (IS) and understanding how this impacts behaviour is crucial in high-stakes interactions (Campbell, 2006; Stempel, 2013).

In interpersonal environments people from different cultures rely on a number of strategies to detect deception focussed around an examination of primarily non-verbal behaviour, for example, eye gaze aversion and inconsistent behaviour, and these strategies are argued to be consistent across cultures (Global Deception Research Team, 2006). These stereotypical cues to deception have been found to be unrelated to actual cues to deception suggesting a potential explanation as to why people are not accurate in detecting deception. Cues to deception in Chinese online groups show that deceivers communicate less, have lower complexity and higher diversity in their messages than truth-tellers (Zhou & Sung, 2008).

Although research has explored cues to deception in interpersonal environments across cultures and has further explored judgements based upon website features and presentation, little research has sought to explore whether individuals employ similar strategies to assess credibility across both interpersonal and mediated environments and the extent to which culture effects such judgements. The current research seeks to examine the strategies that people use to assess credibility, including cues to deception and truth, in interpersonal and online contexts. To detect deception and potentially deceive others across cultures there is a requirement to understand their preconceptions, beliefs, intentions and capabilities to ensure resilience against deception and to more effectively plan deception (Gerwehr, 2006).

Method:

Participants

An opportunity, snowballing technique enabled the recruitment of 38 participants aged 19 to 63 (M = 24.67, SD = 10.34) from Eastern (9 Chinese, 7 Indian) and Western (21 British, 1 Australian) cultures. The sample comprised of 22 Western participants (14 female, 8 male) and 16 Eastern participants (7 female, 9 male) from a community and student background. The participants from Eastern backgrounds were all foreign born but now UK residents, therefore the participants all have experience of Western cultures which will affect the way they interpret information, compared to individuals from Eastern backgrounds with no direct experience of living in a Western culture. Volunteer bias and the location of recruitment in a city in the East of England suggest that this sample may not be representative of all UK national and Eastern cultures, and the specificity of this sample is acknowledged.

Materials

An interview schedule was developed based upon previous research into the strategies that people use to assess credibility in interpersonal and online environments (See Appendix 7.1). Interview questions were focussed around interpersonal and online situations participants have been deceived in, strategies individuals use to detect deception and truth, and strategies individuals may use to deceive others online whilst appearing credible. A sample question about strategies used to assess credibility in interpersonal situations is "*Are you able to tell when someone is lying to you? How? Are there any particular things that people do or say when they lie that help you to detect deception?*", whilst a sample question about strategies used to assess credibility online is "*Have you ever needed to assess the credibility of sites when you are online? How have you gone about doing this? What do you think are the characteristics of a site when you might be a little suspicious?*".

An electronic Dictaphone was used to record interviews with participants, and the interviews were then stored on an Ironkey to ensure security.

Procedure

Participants were initially approached via face-to-face interactions inviting them to participate in an interview study where they will be asked a series of questions regarding the strategies they use to assess credibility in interpersonal and online situations. Those participants who agreed to participate in the research were interviewed in a location of their choice and comfort, where they were informed of their ethical rights and that the interview would be electronically recorded for later analysis (See Appendix 7.2 for the Consent Form).

Data Analysis

Responses were transcribed to ensure a verbatim account of the interview was recorded. Participant responses were treated from a critical realist perspective (Braun & Clarke, 2006), where responses are treated as reflecting reality whilst acknowledging that responses are generated as part of the interview procedure. Separate explanatory thematic analyses, combining deductive and inductive approaches (Guest, MacQueen & Namey, 2012), at the semantic level were conducted for Western and Eastern participants following guidelines outlined by Braun and Clarke (2006) and Braun & Clarke (2013 – See Appendix 6.3). The first stage of analysis involved transcribing the data to ensure a verbatim account of the interviews. The second stage of analysis involved familiarisation and noting items of interest across the dataset. The third stage of the analysis consisted of coding the whole dataset. The fourth stage of the analysis involved searching for themes across the codes. The fifth stage of analysis consisted of reviewing the themes to explore the relationships within and between them. The sixth stage of analysis involved defining and naming the themes, and the final stage of analysis consisted of writing the report and linking the themes to research. Following the completion of separate explanatory thematic analyses for the UK national and Eastern participants a qualitative comparison of the separate themes (Guest et al., 2012) was conducted to enable the identification of potential similarities and differences in the strategies used by participants in assessing credibility in interpersonal and online contexts.

Analysis and Discussion:

Findings

An explanatory thematic analysis (Guest et al., 2012) examining both inductive and deductive themes from a critical realist perspective focussing on the semantic content of responses lead to the identification of 93 codes and 13 themes in Western participants and 62 codes and 12 themes in Eastern participants (See Appendices 7.3 – 7.4). These themes uncovered strategies that individuals across cultures use to assess credibility in their daily encounters with in-real-life and online interactions and strong similarities were found across cultures in the strategies used.

Cross-Cultural Themes

'*Behavioural Baseline*' emerged as a theme from the dataset where individuals from Western and Eastern cultures assessed credibility on the basis of familiarity and knowledge of what a person's normal behaviour is perceived to be allowing them to identify behavioural changes which they perceived as indicating deception.

> "*I think people who you know better and spend a lot of time with will be easier to detect deception or not through whether their behaviour is like out of character or whether they're acting differently but if you don't really know the person well (pause) I think it would be harder to identify whether they're lying or not*" (W3: 7-11)

Participant W3 describes how they believe that can detect deception through familiarity with an individual and monitoring for changes in behaviour, however, if you do not have prior knowledge of that individual it may be hard to identify whether such changes are indicative of deception. Participant E9 also argued that if you have prior knowledge of an individual then you will be able to see a behavioural chance when deception is occurring.

> "*If you know someone before then it is easier to see if there is a behaviour change before and after a lie is told*" (E9: 5-6)

Such an approach to assessing credibility relies heavily upon previous experience with the interactional partner, suggesting that as a strategy its effectiveness may be limited to specific contexts. An examination of behavioural baselines has been recommended as a tool for detecting deception (Ewens, Vrij, Jang & Jo, 2014; Navarro, 2003), although Ewens et al. (2014) recommends small talk is not used to establish such baselines rather baselines should be developed from comparable behaviour. As a strategy of assessing credibility changes in baseline behaviour will need to be examined to see whether they actually indicate cues to deception or are a

reaction to another factor. Some forms of deception also seek to condition the target over an extended period of time where subtle changes in baseline behaviour may be hard to detect requiring other forms of credibility assessment (Macdonald, 2007).

'*Verbal Behaviour*' emerged as a theme in participants' responses where there was a focus on the verbal content of statements and associated paralinguistic behaviour which enabled participants to form credibility assessments of others.

> "*plus their story is very detailed*" (E5: 16)

Participant E5 stated that they were more likely to believe an individual if they had a detailed story. Another examination of verbal behaviour was identified by Participant W7 who argued that if an individual did not provide information then they were less likely to be seen as credible.

> "*I think it was mostly sort of reluctance to give away more information than they needed to, sentences were short, they didn't elaborate on anything, like conversation didn't flow naturally*" (W7: 21-22)

Respondent from both Western and Eastern cultures focussed on areas of verbal content including sentence length, how detailed a story was, and more paralinguistic areas such as whether a conversation flowed naturally as opposed to delayed responses by their interactional partner. Such examinations of verbal behaviour have been found to differentiate between truth-tellers and deceivers (e.g. Porter & ten Brinke, 2010).

'*Non-Verbal Behaviour*' as a theme explores the credibility assessment strategies associated with body language, facial expressions, nervous behaviour and eye contact which are believed to indicate that deception is occurring.

> "*nervousness, like twiddling with your fingers or playing with your hair or looking off at funny angles*" (W1: 7-8)

Participant W1 identifies several non-verbal behaviours which they believe are indicative of deception, for example, finger movements and gaze directions. In contrast Participant E5 focusses on a more general element of body language arguins that negative body language was indicative of deception.

> "*probably their body language, was very negative so I picked up on that*" (E5: 9)

Participants' focus on these cues reflects stereotypes of cues to deception (Global Deception Research Team, 2006) some of which have no link to deception, for

example, eye contact (Wiseman, Watt, ten Brinke, Porter, Couper & Rankin, 2012), although blushing may occur during some deceptive interactions (Yue, Harmer, Guo, Adams & Hunter, 2014). These findings highlight the continued need to educate individuals about genuine cues to deception, which they need to focus their credibility assessment efforts towards. The focus on non-verbal behaviour for assessing credibility in face-to-face interactions has the potential for transfer to interactive online environments and further research should explore the impact of non-verbal behaviour on credibility judgements in these environments.

Credibility assessments can focus on examining "*Consistency*" across content, behaviour and time to uncover truth or deception, and this strategy has application across in-real-life and online interactions.

> "*more dramatasism put on it in like later, like later, like tellings of the story. So first of all, something tiny happened, and then the next time you hear the story it was more than that*" (W1: 19-21)

Participant W1 examines the consistency of a story and argues that such narrative may not be credible if the story does not remain consistent. Consistency was also identified by Participant E10 as a way to examine credibility where an individual may change their story, but also make different statements to different people suggesting that the individual was not credible.

> "*Their story was conflicting, erm, they kept going back on what they were saying and they were different things to different people as well*" (E10: 11-12)

Examining consistency has been used to increase behavioural differences between truth-tellers and deceivers in strategic and tactical interviews (e.g. Hartwig, Granhag, Strömwall, Wolf, Vrij & Roos af Hjelmsäter, 2011) and is argued to be a useful tool in detecting deception. However, the use of consistency by participants has not been towards improving questioning strategies to detect deception but as a more passive approach examining another individual's behaviour. The use of consistency to assess credibility by individuals from Western and Eastern cultures highlights the flexibility of techniques that individuals use to assess credibility based upon available information, which has previously not been identified as a lay technique of credibility assessment. The assessment of consistency over a period of time reflects findings from Park et al. (2002) that individuals often detect deception at a later date.

However, this may leave individuals open to exploitation by the deceiver, particularly in dynamic environments where there are often time constraints on decision-making.

The theme of '*Plausibility*' emerged from both Western and Eastern cultural datasets and was used as a strategy for assessing credibility in both in-real-life and online interactions.

> "*just like what they said was just very over the top. Erm the story wasn't very realistic in a way*" (W5: 12-13)

Participant W5 argues that if a statement is not plausible then it is not credible, whilst Participant E1 states that when purchasing a product online if the situation is not plausible then deception may be occurring.

> "*general knowledge how can you get a mobile for just 10 pounds or 20 pounds (pause) you know something like that*" (E1: 63-65)

Individuals have been argued to make judgements of credibility based upon plausibility in interpersonal interactions (Hartwig & Bond, 2011; Magnussen & Wessel, 2010) and the current findings suggest that individuals from Eastern cultures may also use plausibility as a cue to deception. The use of plausibility in assessing credibility in online environments also highlights its potential as a cue to deception across contexts, although in high-stakes environments plausibility may not be so effective in detecting deception by experienced deception practitioners.

Respondents from both Western and Eastern cultures used techniques for credibility assessment associated with the '*Verification*' of information through checking facts, examining links between online and in-real-life identities and examining information across multiple sources.

> "*obviously on Amazon; a user rating, you know, their rating. So I'll have a look at how many things they've sold, you know, err if they've been on the website a lot, so I'll just check their rating, as far as shopping goes*" (W2: 148-150)

Participant W2 describes the verification of information in online environments through checking across different sources to examine the credibility of information. Participant E4 also describes the verification of information in online environment across several sources as this is perceived as being more credible.

> "*I look at whose written it basically, and how many people have written it. If it's just one person then it's likely not to be credible, but if there's several of them it's a bit more trustworthy*" (E4: 34-38)

'*Verification*' is an emerging technique for assessing credibility across contexts which focuses on the amount of verifiable details used by truth-tellers and deceivers (Nahari, Vrij & Fisher, 2012; Nahari, Vrij & Fisher, 2013) and use of this approach by lay individuals as a credibility assessment technique shows that people do use techniques which have empirical validation. However, some methods, particularly use of reviews, for verifying information suggested by participants require caution as they may also be deceptive and part of a larger deception operation (Ott et al., 2012; Ott et al., 2011). Furthermore, as warrants present suggested links to in-real-life identities (Warkentin et al., 2010) and enhance credibility adversaries may use false warrants as a method to enhance their deception and appear credible to their target.

'*Judgements and Biases*' emerged as a theme in credibility assessment where individuals from Western and Eastern cultures referred to intuitive judgements and judgements based upon experience, whilst biases were also identified in how people assessed credibility across in-real-life and online environments.

> "*I think basically because I think I'm a person who tend to who tend to believe believe others*" (E2: 57-58)

Participant E2 identifies a vulnerability in their own decision-making as they state they are likely to believe other people, whilst Participant W4 states that such judgements of credibility are instinctive.

> "*it's instinctive it's you like or you dislike them*" (W4: 137)

The accuracy of judgement in deception detection may be affected by a range of biases including the truth bias (Bond & DePaulo, 2006; Granhag & Strömwall, 2000) of which some individuals were aware and on the basis of which people are argued to operate in interactions (Levine, 2014). As both Western and Eastern participants had similar biases regarding judgement errors in detecting deception this lends further support to Bond and Rao (2004) in their argument that beliefs regarding deception are to some extent universal. Intuitive judgements also emerged as a form of credibility assessment and such judgements were often guided by first impressions. This strategy may have potential for errors as first impressions may actually impede accurate credibility assessment (Porter & ten Brinke, 2009). Although intuition and unconscious assessments of credibility may prove more accurate than direct measures in some environments (ten Brinke, Stimson & Carney, 2014). Reduced accuracy in

credibility assessment may be linked to difficulties in accessing such unconscious judgements and the effects of explicit cognitive judgements (ten Brinke et al., 2014).

'*Aversion of Risk*' emerged from the dataset of both Western and Eastern respondents where individuals may seek to increase their resilience against deception by avoiding or treating with caution situations in which they may be deceived. This theme was particularly applicable to online environments and may be due to respondents' heightened awareness of deception in such environments.

> "*If he if he was to ask ask my personal information and uh you know something like my mobile phone number my email address my even my y'know credit card account y'know I wi- you know try to avoid it s- you know to stay away from them perhaps*" (E2: 240-242)

Participant E2 states that they would seek to avoid risk if an individual was trying to gain access to personal information. Participant W4 highlights the range of areas where risk may occur in online environments, suggesting the need to be cautious of online interactions.

> "*um you know there's thousand people out there on the Internet not just in terms of um the you know the sexual um predators but also uh financial um predators uh organised crime etcetera etcetera there are lots of websites that aren't real websites that are there just to um extract your financial details*" (W4: 177-181)

As strategies of avoiding risk and increasing resilience against deception they may be particularly effective in environments in which deception rather than truth is anticipated, where individuals have been warned about deception (George et al., 2008; Modic & Anderson, 2014) and where people may have previous experience of deception (Wright et al., 2010). Although these strategies may be deemed effective in reducing harm from deception, further research is required to see how effective people may be in instigating such techniques in their daily activities.

'*Impression Management*' emerged as a theme across both in-real-life and online environments where respondents from Western and Eastern cultures were more likely to judge sources as credible if they were well presented or reflected perceived genuine behaviour.

> "*by the way they talk and the way they try to come across to people that they're talking to, they might come across as trustworthy even though you know you might not necessarily see them in person*" (W6: 87-89)

Participant W6 focuses upon the way in which an individual interacts with others and by the way they talk. Participant E6 focuses upon how attentive an individual is as a sign of credibility, with that further reinforced through not sharing confidential information with others.

> "*when you actually stand and talk to them and you realise that they are listening, and then next day not everybody knows what you talked about , they kinda kept it to themselves, and they remember what you say*" (E6: 47-49)

This theme reflected the ways in which an interactional partner's presentation and behaviour enhances their credibility towards the target. Individual's focus on how others appear as a source of judging credibility increases the target's risk of being deceived as deceivers often engage in impression management strategies to appear more credible (e.g. Hartwig et al., 2010). To increase resilience against impression management practitioners should be informed of the ways in which deceivers may seek to appear credible towards the target.

There were a variety of tactics occurring within the theme of '*Social Influence*' in in-real-life and online environments and across cultures which are influential in how people form judgements of credibility.

> "*you have to build trust with someone and offer them to trust you back*" (W2: 228)

Participant W2 refers to what has been termed as reciprocity (Cialdini, 2007) where individuals are more likely to judge credibility and be influenced by those with whom behaviour is reciprocated. Participant E2 identifies being shown respect as a sign of credibility and trustworthiness, highlighting the different ways in which trust may be developed.

> "*I think if they show respect show respect to me and err they err I mean they easier to to be approached and uh you know this kind of person*" (E2: 123-124)

However, even though such behaviour is oft perceived as credible and influential, this does not mean that the source is actually credible. These findings suggest that individuals from both Western and Eastern cultures may be deceived by information sources they perceive as credible. To counter this individuals must focus attention and credibility assessment strategies towards areas of behaviour that are either verifiable or more accurately differentiate between truth-tellers and deceivers.

'*Website Presentation*' as a theme plays an important role in how respondents from Western and Eastern cultures were likely to judge credibility of online information.

> "*but if I think that a site looks quite unprofessional or a bit dodgy then I'd be more inclined to stay away from it*" (W5: 76-77)

Participant W5 deems a website to not be credible if its appearance is not professional, and a similar strategy is used as well by Participant E3 where there is a focus on text and font as to whether a website may be seen as credible.

> "*I didn't check before when I…online…But I think if the website is fake there is very similar to the real…so just depends on the err…text and the…err…font, something like that*" (E3: 57-59)

Sites were argued to be credible if they were well presented, had a clear layout and appeared professional to the respondents from both Eastern and Western cultures. This reflects findings by Fogg (2002) and Flangin and Metzger (2007) in how individuals assess credibility of websites based upon their features and content. At first glance such a strategy will be useful in filtering out websites of spurious content, however, some deceptive websites can appear highly credible even if they are not and further techniques may be required to assess content for veracity.

Western and Eastern respondents' '*Experience of Internet*' affected how they were able to assess credibility in online interactions, with perceived anonymity, a perceived lack of cues to deception and difficulties associated with lack of face-to-face interaction proving challenging to respondents.

> "*Erm… probably being anonymous like that's the biggest thing, like making sure that people can't track where the information's come from*" (E10: 80-81)

Participant E10 highlights anonymity as an area of concern in online interactions. Anonymity was also identified by Participant W12 who distinguished between being able to monitor someone face-to-face but it proved challenging to assess credibility by text alone.

> "*I am if it's someone, if its face to face, so you can see what their saying but I'm not very good at it by like text or something*" (W12: 15-16)

Respondents lacked knowledge regarding how people interact in online environments with anonymity perceived as a large threat, and respondents sought to use strategies to assess credibility in online environments which they used in real life. Focussing on

verbal content in online environments will enable credibility assessment methods based on verbal and linguistic analysis (e.g. Colwell et al., 2013) to be used where a focus on the non-verbal behaviour, which is filtered out in online environments, is not required for analysis.

Culturally-Specific Themes

One major culturally-specific theme of '*Response to Questioning*' emerged from the Western culture dataset. This theme explored an approach used by Western individuals to assess credibility in others by examining their interactional partner's responses to questioning, including how and whether they responded.

> "*be prepared to talk to me if they erm erm run away from me or erm you know don't want to have an- avoid me in the street then I wouldn't be inclined to trust them with anything or talk to them about anything*" (W4: 133-136)

Participant W4 identified an individual's response to further interactions as effecting their judgements of credibility as individuals who avoided further interactions were deemed not trustworthy. Participant W11 states that further questioning of an individual may be used to examine an individual's narrative further and their subsequent response helps to judge credibility.

> "*even if they say something a little bit differently and then by questioning further it will probably start to unravel a bit*" (W11: 12-13)

This approach highlights that individuals engage in active strategies for assessing credibility which reflects techniques of strategic and tactical questioning (Dando & Bull, 2011; Hartwig et al., 2006; Levine, Shaw & Shulman, 2010) to detect deception in others. Such an approach to credibility assessment is also transferrable to online interactions (Colwell et al., 2013; George et al., 2008). This strategy indicates that Western individuals may have explicit awareness of how to increase accuracy in assessing credibility in others; however, further research is required to examine how people actively engage in such techniques during interaction. '*Responses to Questioning*' may have emerged as a culturally-specific theme for Western individuals due to cultural differences related to power distance, the individualism of Western cultures and differences between holistic and analytic cognition (Nisbett, Peng, Choi & Norenzayan, 2001; Norenzayan, & Nisbett, 2000). Individualistic cultures may be more willing to question others, whilst collectivist cultures may seek

to maintain social harmony and may not be willing to challenge perceived authority (Colwell et al., 2013). Eastern cultures are argued to be field dependent where they focus on an individual's relationship with their environment to form judgements, whilst Western cultures are argued to be more analytic and focus upon the individual in making judgements (Nibett et al., 2001; Norenzayan & Nisbett, 2000). Such a difference in causal cognition may explain why Western cultures may seek to further question individuals regarding their credibility whilst, Eastern cultures may rely upon the surrounding context with which to form judgements of credibility. Further research may seek to explore whether individuals from collectivist cultures are willing to question others' credibility.

Potential similarities in strategies used to assess credibility by Western and Eastern cultures may be explained through cultural evolution where individuals experience in Western culture has affected how they interpret information (Gerwehr, 2006). As the individuals from Eastern cultures interviewed in the current research have had more interaction with Western cultures and will affect how they make sense of their environment.

Building upon both the Global Deception Research Team (2006) and Park et al. (2002) the current research has identified a range of techniques which individuals use to assess credibility in interpersonal and online environments, with participants using some strategies for both domains. Although some of the strategies used were incorrect for accurately detecting deception (e.g. eye contact and gaze direction), a large number have the potential for useful credibility assessment strategies (e.g. verification, consistency and plausibility) and further research should seek to educate individuals in accessing and selecting the most effective strategies for credibility assessment to increase resilience against threat, particularly in online communication. For those strategies which are incorrect in detecting deception and may be used by adversaries, deception planners may seek to exploit these through following deception planning guidelines (Gerwehr, 2006).

Similarly to Park et al. (2002) the strategies used to assess credibility by the participants are not claimed to be representative of all strategies which people use, nor will the strategies be useful for every context in which credibility assessment is required. The participants were not asked to develop strategies for specific contexts; instead the strategies which emerged from the dataset may be treated as general

strategies which individuals may select according to context and their previous experience in credibility assessment.

Limitations

Self-reports of strategies used to assess credibility may not be representative of all strategies that individuals use to assess credibility as people may have limited insight into their own decision-making processes (Strömwall, Granhag & Hartwig, 2004). However, individuals offered a range of strategies to assess credibility some of which reflect techniques currently being used to assess credibility in psychological research (e.g. plausibility, consistency, use of warrants). Strategies were also offered for credibility assessment which experimental paradigms may not enable individuals to use (Park et al., 2002) and have thus not been identified by previous research. Whether or not these individuals use these strategies effectively to detect deception requires further research.

Current research provides awareness of the strategies which individuals from different cultures state they use in credibility assessment, it may be that other strategies have not been identified by the current research. Although there is an awareness of multiple perceived strategies of credibility assessment not all of these strategies are correct, and it is yet to be seen how individuals may employ strategies when assessing credibility. Gerwehr (2006) states that field dependence will affect how cultures interpret information related to the surrounding context. Suggesting that individuals from collectivist cultures may be more likely to interpret information according to surrounding context, whilst individuals from individualistic cultures may not use surrounding context to interpret information (Gerwehr, 2006).

The culturally-specific theme of '*Responses to Questioning*' as a strategy used by Western participants to assess credibility may only be limited as it was only identified by a small number of Western participants. This would suggest that the current findings need to be taken with caution as it may not be representative of all Western individuals and requires further exploration to ensure reliability of this theme.

Future Directions

The current chapter has outlined similarities and differences between the strategies used in credibility assessment across interpersonal and online environments by respondents from Western and Eastern cultures. With deception occurring across a wide range of cultures it is particularly important to understand such strategies of credibility assessment, and an exploration of further cultures is required (Gerwehr, 2006), including cultures which reflect areas other than national identity, and how cultural fluidity may affect credibility assessment.

An awareness of the risks posed in assessing credibility was highlighted by respondents who sought to use caution in engaging with elements of online behaviour. Research has recently sought to warn individuals about the potential for deception in online environments (e.g. Modic & Anderson, 2014) and new approaches are required for increasing resilience against deception. In interactional contexts resilience may be increased through the adaptation of DRE approaches to online environments (Colwell et al., 2013). In non-interactional online environments resilience may be increased through education regarding online deception followed by testing to ensure that lessons have been learned.

Identifying credibility assessment strategies used by other cultures should also focus on identifying the credibility assessment strategies used by adversaries from a different cultural background. To persuade and influence others it is essential to understand their culture and background history to develop targeted strategies (Mackay & Tatham, 2011). Such a concept is equally applicable to conducting deception operations where understanding the target and how they may be influenced to achieve the objective is part of the deception planning process (Gerwehr, 2006). Through understanding an adversaries credibility assessment strategies it may be possible to conduct more effective deception and influence campaigns to achieve objectives, and further research is required to explore this area.

Conclusion:

The current chapter has focussed upon exploring the similarities and major differences between credibility assessment strategies used by individuals from Western and Eastern backgrounds use to assess credibility in interpersonal and mediated environments. A large number of similarities were found across both cultural backgrounds in how credibility is assessed reflecting past research (e.g. Fogg, 2002; Global Deception Research Team, 2006; Park et al., 2002). The major

difference between cultural groups was that respondents from Western backgrounds were more likely to seek to challenge their interactional partners to uncover deceit. General strategies for assessing credibility were found to reflect current and emerging research into deception detection, suggesting that individuals may perceive beneficial strategies of credibility assessment and future research should seek to increase individuals' awareness of such strategies and how they can be used to assess credibility particularly in mediated environments.

Chapter 8: Risk Assessment in Deception: Presenting DARN and DRAT

Introduction:

In regard of deception and the assessment of future threats, it is critical to consider the concept of risk as underpinning practitioner decision-making. The detection of deception and risk assessment have historically been intertwined when considered in the context of decisions in forensic and legal domains, however the application of structured risk assessment methods to security and military domains has to date been neglected. Chapter 8 builds extensively upon Chapter 6 through developing a new approach towards detecting deception based upon examining the risks posed through an in-depth understanding of the deceiver's and target's capabilities and the cues to deception identified from the interviews with SMEs. This chapter will discuss the challenges of risk assessment (actuarial and clinical judgements) within the forensic domain and present the development of two structured tools which are relevant for the detection of deception in computer mediated and interpersonal environments.

Risk is defined by Skeem and Monahan (2011, p. 38) as "*a correlate that precedes the outcome in time, with no implication that the risk factor and outcome are causally related"*. Adapting Hart's (1998, p. 122) definition of violence risk assessment "*as the process of evaluating individuals to (1) characterize the likelihood they will commit acts of violence and (2) develop interventions to manage or reduce that likelihood*", deception risk assessment can be defined as "*the process of evaluating individuals, groups and organisations, whether state or non-state, to (1) characterise the likelihood they will commit acts of deception and (2) develop interventions to manage or reduce that likelihood"*. Although perfect prediction is an unattainable goal (Ericson 2006), through conducting risk assessments UK vulnerability to threats may be reduced (Aven & Renn, 2009), whilst providing an audit trail of how decisions were made (Goble & Bier, 2013). Risk assessments are argued to inform relevant decision-makers and stakeholders about potential threats that may need immediate action, whilst providing options for risk prevention or mitigation (Aven & Renn, 2009). The deception risk assessments outlined in the

current chapter will consist of a continuing assessment procedure, predictions of future deception and suggestions for mitigating or preventing acts of deception.

Actuarial Approaches

Actuarial approaches to risk assessment and management seek to quantify risk and produce an outcome focussing on the probability of risk occurring in a given situation. Actuarial approaches have focussed upon a number of behaviours, including future risk of violence (Grann, Belfrage & Tengström, 2000; Helmus, Babchishin & Hanson, 2013) and sexual offender recidivism (Hanson, Lunetta, Phenix, Neeley & Epperson, 2014; Hanson, Sheahan & VanZuylen, 2013; Helmus et al., 2013). Actuarial approaches to risk assessment have risk factors and items developed from empirical research, for example, the Risk Matrix-2000 (Thornton et al., 2003), which are based upon collating the characteristics of individuals who are re-convicted following release from prison. Although considered a relatively reliable starting point to determine likely future risk of harm, the actuarial methods do not incorporate consideration of attrition within the legal system – that is, the likelihood of a case being 'dropped' between the allegation of the offence being made and the case being heard in court. Generally though, such approaches have found comparable assessments of risk across different risk assessments in predicting violent behaviour, with no assessment outperforming another (Grann et al., 2000; Helmus et al., 2013; Ho, Thomson & Darjee, 2009). In some circumstances actuarial approaches to risk assessment have utility (Hanson et al., 2014), when combined with consideration of dynamic factors in regard of risk. In the consideration of high-stake deception risk assessment the combination of static and dynamic risk factors are required.

Actuarial risk assessments can be categorised into unmodified and modified approaches (Monahan, 2012). Unmodified actuarial risk assessments identify, measure and combine the scores of risk factors and argue that the process is then complete (Monahan, 2012). Modified actuarial risk assessments, however use the same approach of the identification, measurement and combination of a score of risk but produce a probabilistic outcome rather than a definitive decision (Monahan, 2012). It is acknowledged that the presence of rare factors can affect outcomes of risk, and due to the idiosyncratic nature of risk, they may not appear as a static factor on actuarial assessments (Aven & Renn, 2009). To counter this assessment weakness,

clinical reviews of actuarial risk assessments are required and an allowance for flexibility in the approach is critical.

The reliance on static factors in some measurement tools fails to allow a more considered judgement to be made in regard of risk (Blacker, Beech, Wilcox & Boer, 2011), despite the refinement over time with the inclusion of updated empirical evidence (Hanson et al., 2014). As deception is argued to be context dependent and individual's strategies will change according to their strategic aims, actuarial risk assessments in isolation are likely to fail in capturing the broad range of issues to be considered. When applied to the challenges of detecting deception, it is critical to have the capacity to draw from a range of sources in order to ensure judgements can be underpinned by an evidence-based approach.

Structured Professional Judgement Approaches

The '*structured professional judgement'* (SPJ) model of risk assessment considers elements of clinical decision-making with a focus on an individual's characteristics and strategies of intervention and management to reduce risk (Boer, Tough & Haaven, 2004; Cook, Murray, Amat & Hart, 2014; Douglas & Reeves, 2010; Kebbell & Porter, 2012; Kropp, Hart, Lyon & Storey, 2011). SPJ risk approaches are argued to provide more accurate assessments of risk by combining actuarial and clinical judgement approaches (Blacker et al., 2011; Doyle & Dolan, 2006). The basis for such assessment of future risk emphasises the interpersonal interaction with the individual concerned in addition to broad collateral information to inform judgements (Kebbell & Porter, 2012). Hence although there is a structure to the particular risk assessment task (e.g., violence, stalking or arson), the assessor can use discretion in regard to the level of emphasis placed on different pieces of evidence and the associated confidence with which evidence informs judgements (Kropp et al., 2011). It is argued that SPJ assessments have an advantage over actuarial approaches through the incorporation of risk management strategies which are developed in response to the assessed level of risk posed. Similarly in the detection of deceit (cf. risk), the ability to make a judgement in regard of a particular threat has to occur on a continuum of likelihood. This is comparable to the national security ratings which are underpinned by evidence in regard of the level of severity and imminence of a threat to the UK. SPJ risk assessments support practitioner decision-making through the

application of assessments which reflect up-to-date scientific knowledge and clinical practice (Kropp et al., 2011), enabling a focus on a number of factors which are identified as being of high relevance and are useful in practice (Cook et al., 2014; Gozna & Lawday, 2015). Items on SPJ risk assessments may be scored to assess the risk that each factor may pose so that a profile of risk can be identified and tailored to an individual. For example, the Historical-Clinical-Risk Management V³ (HCR-20: Webster, Douglas, Eaves & Hart, 1997) scores risk factors as to whether they are absent (0), possible or limited presence (1), and definitely present (2) and further incorporates the use of collateral evidence to inform these decisions and in turn this is transferred into scenario planning of future risk. This enables practitioners using the assessment to clearly establish the factors that are particularly pertinent to the judgement of risk. When applying this process to deception detection and the assessment of future threats, practitioners will be required to make judgements about the deceiver's characteristics regarding factors identified in the HMD (See Chapter 6) and design the strategies of management and intervention according to risk factors developed from empirical research.

The basis for structured risk assessment tools (e.g., HCR-20: Douglas & Reeves, 2010 and Stalking Assessment and Management: Kropp et al., 2011) is the concentration on historical and current behaviours whilst anticipating future behaviours, principles which are transferable to the assessment and management of high-stake deception. Recent research has sought to expand the use of SPJ risk assessments from the assessment of violence and other criminal acts and focus on issues of national security (Beardsley & Beech, 2013; Kebbell & Porter, 2012; Monahan, 2012; Roberts & Horgan, 2008). SPJ approaches to terrorism have been developed to examine risk of terrorism (Kebbell & Porter, 2012; Monahan, 2012), whether a detained individual may be likely to reengage with terrorism and whether employees hold beliefs supportive of terrorism (Monahan, 2012).

Static Risk, Dynamic Risk and Warning Behaviours

Static risk factors are argued to not change, or change very little or very slowly over the course of time, for example, gender of victim and age of first offence (Douglas & Skeem, 2005; Meloy, Hoffmann, Guldimann & James, 2012; Wilson, Desmarais, Nicholls, Hart & Brink, 2013). Static risk factors may be used to

determine the level of deception risk posed over the course of time, but they will not determine all risk and behaviour will change according to an individual or groups' current aims and motives. In contrast, dynamic risk factors fluctuate in nature and severity over the course of time and these are linked to changes in overall risk (Douglas & Skeem, 2005; Wilson et al., 2013).

Dynamic stable risk factors are enduring changeable characteristics which in the current context, link to deceptive behaviour, whilst dynamic acute risk factors are rapidly changeable characteristics that may indicate behaviour will occur within a short period of time. Dynamic factors are argued to provide a target for intervention or treatment in the case of violence risk assessment (Meloy et al., 2012; Wilson et al., 2013), and in the case of deception dynamic risk factors can be identified and risk management strategies activated. An awareness that behaviour changes over the course of time rather than remaining indefinite is required for assessing risk (Douglas & Skeem, 2005) and this is applicable to deceptive behaviour.

Warning behaviours are argued to be acts which provide evidence for accelerating or increasing risk (Meloy et al, 2012; Meloy, Hoffmann, Roshdi & Guldimann, 2014). These behaviours are acute and dynamic changes of pattern in behaviour which may aid in structuring a practitioner's judgement of risk from the actor and require risk management strategies to be enabled (Meloy et al., 2012). Previous research into warning behaviours has focussed on areas of violence risk assessment including murder, assassinations and terrorism (Meloy et al., 2012). Identifying key warning behaviours of future threats enables a consideration of deception and can therefore produce more tailored, comprehensive risk assessments and management strategies.

Security and Terrorism Risk Approaches

The increased focus on the assessment of risk in national security environments has been largely in response to global acts of terrorism which have resulted in mass civilian casualties (e.g., September 11th and July 7th attacks). Risk assessment in security environments have involved assessment of state and non-state actors, with these assessments often built around adversary capabilities and intentions (Bennett & Waltz, 2007; Garrick et al., 2004; Koblentz, 2011; Nguyen, 2002; Willis, Morral, Kelly & Medby, 2005; Yang, Wang, Bonsall & Fang, 2009), although some

incorporate target vulnerabilities (Koblentz, 2011; Piegorsch, Cutter & Hardisty, 2007; Willis et al., 2005; Yang et al., 2009), how adversaries may identify targets (Strandberg, 2013) and consequences of attacks (Willis et al., 2005; Yang et al., 2009). These approaches tend to consider actuarial and probability approaches which have potential flaws (Aven & Renn, 2009; Brown & Cox, 2011; Garrick et al., 2004). Particularly as different terrorist and extremist groups have very different motives for engaging in terrorism (Jacques & Taylor, 2008), organisational structures and targeting strategies where casualties may or may not be intended (Wilson & Lemanski, 2013) and this reflects the type of weapons used (Wilson, Scholes & Brocklehurst, 2010), requiring a more contextual and dynamic understanding of how risks posed by terrorism emerge. A key challenge in seeking to assess the risk of deception by adversaries is to move beyond actuarial risk assessments assessing probability of risk, but instead to adopt SPJ approaches which provide evidence-based decision-making guidance across interpersonal and mediated environments and outline risk management strategies.

Rationale for deception risk assessment tools

Deception research recommends that approaches consider the cognitive complexity of conducting deception leading to less detailed and consistent accounts and more controlled behaviour and appearance than truth-tellers (Vrij, 2004, 2008). However, as much as the academic approach to deception has attempted to ground research outcomes in the real-world (Vrij, 2004); there remains a dearth of work adopting a scientist-practitioner model for the understanding of high-stake threat. The HMD argues that further consideration is required to target vulnerabilities, culture, and individual differences and personality factors (See Chapter 6). The purpose of developing dynamic and iterative risk assessment tools has been to provide a standardised, systematic and practical framework for gathering, considering and managing information in high stake decision-making.

The Deception Assessment Real-time Nexus©2015 (DARN) and Deception Risk Assessment Technique©2015 (DRAT) risk tools are intended for individuals and teams in security environments making decisions regarding deception and associated threats across real-world and computer-mediated domains with the intention of eradicating or

diminishing adversary threats. The DARN tool focuses on identifying 'warning behaviours' suggestive of possible deception and as such is a screening tool that can be adopted for use in isolation, or preceding the use of DRAT. The DRAT tool provides a full-scale risk assessment of deceptive behaviour including future scenario development and associated risk management strategies and this can be employed for longer term threat assessment as a standalone, or following the use of the screening tool DARN.

Deception Assessment Real-Time Nexus©2015

Figure 8.1 presents the DARN model and the stages of analysis, whilst Appendix 8.1 illustrates the DARN screening tool. The DARN screening tool provides practitioners with stages of analysis and enables a description of the context, the monitoring of any changes in adversary behaviour before identifying relevant evidence and assessing information for risk of deception.

Methodology – Tool Development

In order to adopt a standardized approach to the development of the DARN tool, the methodology adopted in the development of the Comprehensive Assessment of Psychopathic Personality (CAPP – Cooke, Hart, Logan & Michie, 2012) was used. This was considered to provide a systematic method for the development of a practitioner tool. The content of the items presented in the DARN tool were identified from a comprehensive review of psychological and military research and practice, alongside SME input (see Chapter 6) to construct a conceptual decision-making model focussing on the collection and analysis of information. This precedes any recommendations for counter-deception and risk management strategies outlined by the DRAT to respond to adversary deception operations.

Following the methodology outlined by Cooke et al. (2013) the first stage of the DARN development consisted of an extensive literature review covering a wide range of areas related to deception and its detection across interpersonal, online and military environments (e.g. verbal and non-verbal behaviour, personality, decision-support tools), however this review did not consider physiological approaches towards deception detection due to their limited potential in operational environments (see Chapters 2-4). Reliance on a top-down approach to formulating deception should be avoided as such approaches focus on only one area of research and ignore greater

complexities. As such a bottom-up approach to the literature reviewed in model development has been conducted as this enables identification of strengths and weaknesses in current approaches and established whether a new model is required, and the result of such work is presented as a theoretical holistic approach to deception detection (see Chapter 5).

The second stage of designing DARN reflected input from SMEs (see Chapter 6) and the manner in which they conceptualised deception. Following interviews with open-ended questions, SME responses were examined and led to the development of the HMD (see Chapter 6). The HMD outlines how deception occurs from the deceiver to the target, and identified further areas of deception that had not previously been considered during the literature review. These findings have been used to inform the development of the DARN.

The final phase of development refined the large number of identified items into a screening-tool version of a full scale SPJ risk assessment for detecting deception. This process involved arranging similar items together, for example, the DARN groups together the different forms of HUMINT that can be used to inform judgement of credibility (See Figure 8.1) and strategies of credibility assessment included were identified from research and SME responses (see Chapter 2 – 6). The DARN process is highlighted in Figure 8.1, whilst the descriptions of the DARN components are outlined below.

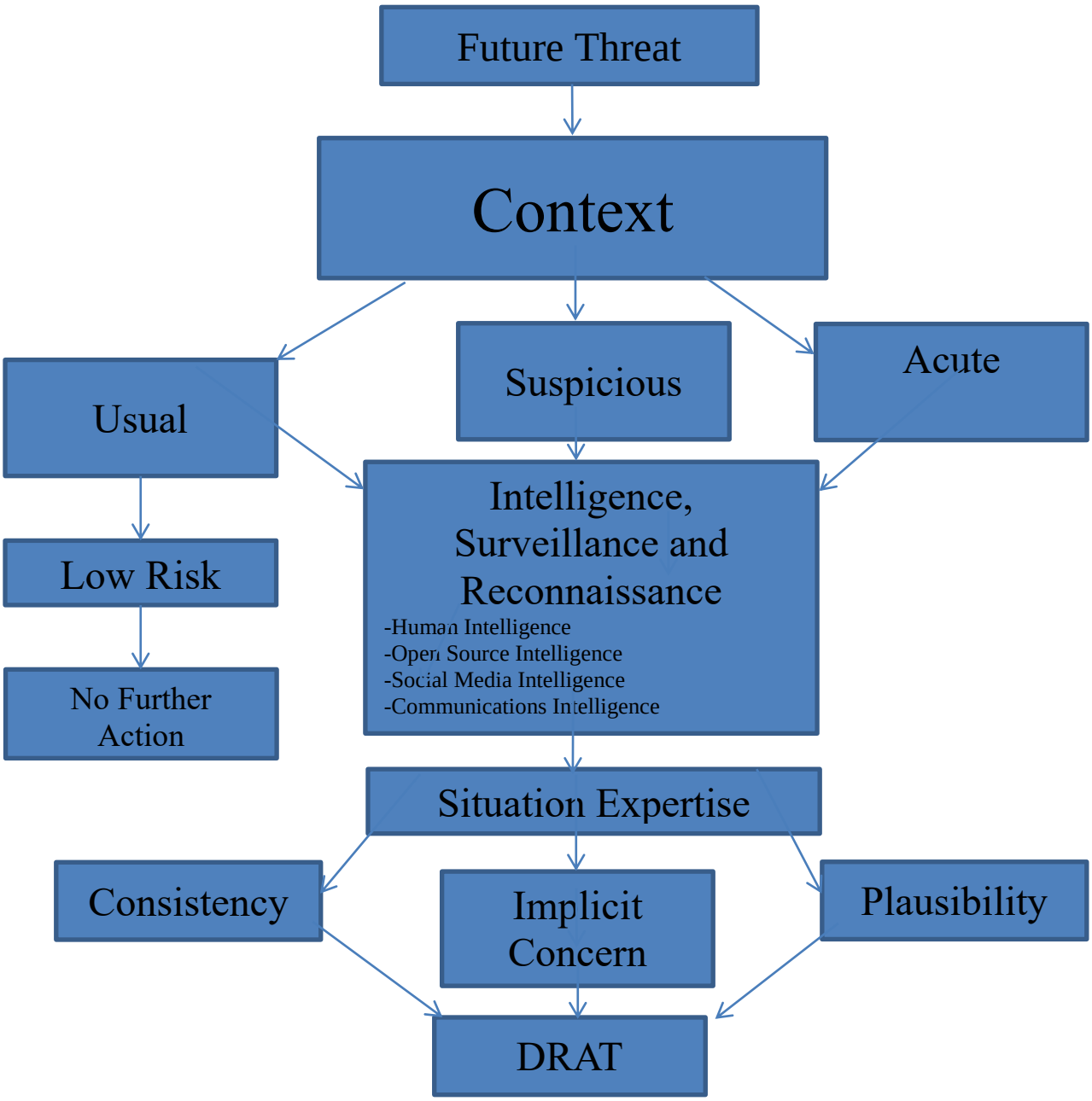

Figure 8. 1: The Deception Assessment Real-Time Nexus Process©2015

Deception Assessment Real-time Nexus©2015 Components

Future Threat Scenario Development

As presented in Chapter 9, the importance of specific and generic future threat scenarios are critical for the focus of the screening and full risk assessments. This can incorporate scenarios which are considered to be a higher likelihood in terms of threats to the UK, i.e., an IS motivated threat, whether a lone wolf or co-ordinated attack or alternatively threats that might be considered of lower imminence but high severity were they to occur. In regard of the risks associated with such threats, it is important to consider a holistic approach while incorporating critical involvement of the human aspect of all individuals involved at all levels.

Context

Intelligence, Surveillance and Reconnaissance (ISR) is used by security and intelligence organisations as a technique for collecting intelligence about adversaries through which a behavioural pattern can be developed and then used to inform operations (DCDC, 2011; Henderson & Pascual, 2008 – see Appendix 8.2). ISR is defined as "*activities that synchronise and integrate the planning and operation of collection capabilities, including the processing and dissemination of the resulting product*" (DCDC, 2011, p 1-9). The technique focuses intelligence collection broadly across human, electronic and geophysical information (DCDC, 2011). However for the purpose of the present risk assessment tools, it is the emphasis on the human element of information communication and behaviour that is considered to be of primary importance and ultimately the main source of evidence for the assessment of risk. HUMINT focuses on intelligence derived from information collected or provided by human sources including information recovered from debriefings and investigative interviewing (DCDC, 2011). Further information relevant to understanding and detecting human deception can be developed from OSINT (where information is publically available and recoverable for analysis), social media intelligence (SOCMINT – any information retrievable from social media technologies, e.g. Facebook and Twitter), and communications intelligence (COMINT – where information is developed from electronic communications, e.g. emails). Through ISR techniques an understanding of context and usual adversary behaviour may be developed.

Once intelligence has been gathered and assessed for credibility according to the range of techniques advocated by the HMD (see Chapter 6) a baseline of usual adversary behaviour can be developed, from which changes in baseline behaviour

may indicate deception. Furthermore, if the adversary behaviour is usually deceptive than there is a high risk of deception occurring and a full-scale risk assessment will be required. In deception research, changes in behavioural baseline have been examined and are argued to indicate that deception may be occurring (Ewens et al., 2014; Navarro, 2003; Vrij & Mann, 2001 – See Chapter 6, Appendix 6), although any change in behaviour will need to be confirmed as deception.

Suspicious Behaviour: This relates to alterations from normative behaviours which might be indicative of actions warranting increased focus and attention. In regard of suspicious behaviour, it is important that practitioners have flexibility to identify alterations that they (from their own expertise and experience) are against the norm or an expectation. A change in usual adversary behaviour, for example, there may be conflicting information from human sources compared to news channels compared to previous synthesis, might indicate a cause for concern although the context in which this occurs needs to be assessed more broadly with a breadth of factors.

Acute Behavioural Change: In risk assessments, an acute change in usual behaviour, for example, multiple sources may all start reporting the same information regarding adversary intentions, and/or the identification of key warning behaviours will be identified as a cause for concern and will require a full risk assessment (Meloy et al., 2012) and this principle will be applied to assessing risk of deception by adversaries.

Situation Expertise

Situation expertise will be required for analysing different sources of intelligence generated from ISR, for example, expertise in detecting deception will be required for areas including HUMINT, OSINT, SOCMINT and COMINT to analyse intelligence. Further, some experts have been found to have greater accuracy in detecting deception than others (Ekman & O'Sullivan, 1991; Wright-Whelan, Wagstaff & Wheatcroft, 2015) and such experts should be identified for deployment in intelligence-gathering processes.

Consistency

Once evidence has been developed through ISR capabilities checks for consistency of this evidence are required. Consistency can be examined across multiple areas, for example, between past and current behaviour, between current behaviour and adversary policies and aims, between current behaviour and known

capabilities, and between multiple sources of evidence. Examining consistency of evidence and statements has been used within investigative interviews and is a promising technique for detecting deception (e.g. Dando & Bull, 2011; Hartwig et al., 2006).

Plausibility

Once evidence has been recovered checks for plausibility are required. Research into deception detection has focussed upon using plausibility to discern between truth-tellers and deceivers verbal statements (e.g. Leins, Fisher, Vrij, Leal & Mann, 2011; Vrij, Leal, Mann & Fisher, 2011). Plausibility can be further used to assess other areas of credibility.

Concern of Targeting – Implicit belief

There may be an implicit belief, suspicion or scepticism that the adversary is engaging in targeting or deception operations, which would suggest that follow up assessment is required to assess these beliefs. People may have an implicit belief that deception is occurring based on their observations (Evanoff, Porter & Black, 2014; ten Brinke et al., 2014), increasing the need for a follow-up examination to substantiate such beliefs. Scepticism towards information has the potential to increase accuracy in identifying deception (Forgas & East, 2008; Kim & Levine, 2011), although it may reduce accuracy in detecting truth (Kim & Levine, 2011). Suspicion that something out of the ordinary is occurring and might indicate deception means that a full risk assessment is required to confirm or refute these suspicions (Bobko, Barelka & Hirshfield, 2014; Bobko, Barelka, Hirshfield & Lyons, 2014)

Activating the DRAT

Once intelligence about the adversary has been analysed for consistency, plausibility and judgements made regarding suspicious behaviour levels of risk regarding adversary behaviour can be developed. Levels of threat can be constructed from the intelligence available from multiple factors or from key critical factors which indicate acute risk and the level of risk will reflect the context. Practitioners will prioritise risk as follows:

- High Risk – Prioritise and Activate DRAT
- Medium Concern – Activate DRAT
- Low Concern – Do not activate DRAT but continue to monitor

Risk levels will be reviewed and revised on a regular basis in operational circumstances through deploying ISR capabilities (DCDC, 2007, 2011).

Deception Risk Assessment Technique©2015

To meet the challenge of managing deception risks the *'Deception Risk Assessment Technique'* ©2015 (DRAT- See Appendix 8.3) has been developed for use following the DARN or for use as a standalone risk assessment tool.

Methodology

In developing the DRAT, the work of Skeem and Monahan (2011) in assessing risk through SPJ approaches is drawn upon. SPJ approaches are argued to have two components to how risk is constructed: (a) identifying valid risk factors and, (b) determining a method for scoring each of these factors. Consistent with Webster et al. (1997) the presence of risk can be identified from both a single critical item or from a combination of items, therefore, presenting a combined risk score for overall level of risk is not required.

(A) Identifying Valid Risk Factors

In developing the DRAT risk factors a logical item selection method outlined by Cooke et al. (2012), Douglas and Skeem (2005), Douglas and Reeves (2010), Kebbell and Porter (2012) and Kropp et al. (2011) was selected, whereby a thorough review of the deception related literature was conducted, alongside the incorporation of the findings and themes developed from interviews with SMEs where risk factors with empirical and practitioner support across multiple samples and contexts were selected to form a conceptual model of deception risk. Following identification, items were separated on a rational basis into risk factors (Cooke et al., 2012). Appendix 9.4 provides a list of the risk factors and examples of research which supports their inclusion in the DRAT. This list is not exhaustive and will be subject to change with the incorporation of further research as required, or items dropped from the model if irrelevant in applied settings (Cooke et al., 2012).

(B) Scoring Risk Factors

In scoring risk factors, the situation identified by the analyst is described and then the item is coded following SPJ guidelines (Douglas, 2014) for low, medium or high

risk, for example, the analyst identifies the presence of sadism in the deceiver, therefore the risk factor is scored for high risk. Some items may actually decrease risk posed by adversaries, for example, if an adversary lacks capabilities they will have a low risk score. The presence of critical items and/or the identification of risk across multiple items will lead to the activation of deception detection and risk management strategies. Consistent with other SPJ approaches no assumption is made that all items will be applicable for all individuals (Douglas, 2014).

Deception Risk Assessment Technique©2015 Components:

Following the identification of risk factors from psychological and military research (Appendix 8.4), the elements of the DRAT are presented in Table 8.1 whilst the sections the factors fall under are described in detail below: The '*Context of Deception'* section of risk factors refers to the situation and context in which deception occurs. Risk items in this section include: the situation, the actors, current threats, communication medium, online communication characteristics, and in-real-life communication characteristics. Together these factors enable an understanding of how deception may occur, which in turn will affect the strategies used to detect deception and manage associated risks.

The '*History*' section of risk factors seeks to understand and develop a profile of the adversary through examining previous non-deceptive adversary behaviour to develop a baseline of 'normal' behaviour. Development of a behavioural baseline will enable UK capabilities to monitor for changes in adversary behaviour that may indicate deception is occurring. Further understanding of past acts of deception by the deceiver towards the UK and others will enhance knowledge of adversary deception strategies, although it is anticipated that these strategies may vary depending on context (Gozna & Boon, 2010).

The '*Nature of Deception'* section of risk factors considers the different strategies used to deceive others, and provides indicators of potential forms of deception within each risk factor, which may or may not be rated for presence depending on practitioner requirements (Douglas, 2014). Deceivers can create and identify vulnerability in the target which they then aim to exploit through a variety of techniques, for example, through ruses (Hansen, 2008) and through exploitation of target hopes (LeMire, 2002). Deceivers can condition the target into expecting a

certain pattern of behaviour, which the deceiver is then able to exploit, for example, the Soviet-Czechoslovakia Campaign 1968 (Whaley, 2007). Deceivers actively engage in impression management through controlling their verbal and non-verbal

Table 8. 1 The Deception Risk Assessment Technique©2015

Risk Factor	**Elements**
Context of Deception	Situation Actors Current Threats Communication Medium Online Communication Characteristics In-Real-Life Communication Characteristics
History	Previous Behaviour – Non-Deceptive Previous Deceiver Interactions – UK Previous Deceiver Interactions – Others
Nature of Deception	Create and Identify Vulnerability and Exploit Conditioning the Target Impression Management Control of Information Credibility Enhancers Social Influencers
Deceiver Risk Factors	Deception Doctrine Gains Vs Losses Motivation Capabilities, Resources and Experience Deception Spontaneity → Planned Cognitive Performance Language Personality and Individual Differences Belief System
Target Vulnerability Factors	Who is the Target? Stakes Motivation Target Characteristics Mindset – Cognition Mindset – Affect Capabilities – Information, Surveillance, Target Acquisition and Reconnaissance (ISTAR)
Risk Scenarios	**Elements**
	Nature Severity Imminence Frequency/Duration Likelihood
Risk Management Strategies	**Elements**

	Monitoring Supervision Target Inoculation Planning Other Considerations

behaviour in order to appear credible to others (Hartwig et al., 2010; Hines et al., 2010). Such behaviours may be difficult to identify without knowledge of impression management strategies. Deceivers' use further strategies of control of information, including increasing and decreasing the amount of information available to the target, in order to create ambiguity and/or increase noise and cognitive load in the target reducing their decision-making abilities (Macdonald, 2007). There are credibility enhancers which are used as strategies for the deceiver or information presented by the deceiver to appear more credible to the target, for example, website appearance (Flanagin & Metzger, 2007) and appearing objective (Ott et al., 2011). Tactics of social influence may also be used by adversaries to influence and deceive others through a variety of means (Cialdini, 2007; Henderson, 2007).

The '*Deceiver Risk Factors'* section provides risk factors which affect the deceiver's ability to conduct deception. The adversary may have deception doctrine, which governs the circumstances in which deception operations are allowed, however, this may not be applicable to non-state actors, or adversaries who are not limited by ethical and legal considerations. Adversary deception may be effected by the perceived gains and losses of deception, with lower risk for the target associated with high losses and low gains for the adversary. Adversary motivation may also pose risk to the deceiver as it may affect how much effort is placed into constructing the deception, and deception has the potential to be enhanced online (Woodworth, Hancock, & Goorha, 2005). Adversary capabilities, resources and experience will affect their ability to research, plan and conduct deception operations (Mackay & Tatham, 2011), and if these capabilities are lacking their ability to deceive will be reduced. Adversary deception may be spontaneous, planned or along a continuum of both, and this will affect how the adversary and the information they present are perceived by others (Strömwall &Willén, 2011). The adversary's cognitive performance will affect the risk they pose to the target, as deception is argued to be a cognitively demanding task (Vrj, Granhag, Mann & Leal, 2011a), those adversaries with greater cognitive abilities will pose an increased risk to the target. Language will also affect the level of risk posed by the deceiver to the target, whether this is through

the deceiver being able to construct deception to appear credible to the target, or to the target's ability to accurately assess information or conduct investigative interviews in a different language (Colwell et al., 2013). Personality and individual differences factors will affect how the adversary conducts deception and the way in which they portray themselves to the target (Taylor & Gozna, 2011). Dark personalities will add additional challenges and risks to the target (Paulhus & Williams, 2002). The adversary's belief system, their identity, culture, religion, politics and allegiances will affect how they interpret the world and influence their interactions with others which will shape the motive and context from which deception occurs. Understanding the adversaries belief system will help to reduce risk involved from deception.

The '*Target Vulnerability Factors'* section links to risk factors which may affect the target's ability to accurately detect deception and enable adversary exploitation of vulnerabilities. Identifying who the specific target is required in order to assess risk posed, for example, if the target is a key-decision maker then risk may be increased as deception may have greater consequences. The target stakes in assessing individuals or information for deception may pose risk as high-stakes may increase cognitive and/or emotional arousal reducing the deceiver's ability to assess credibility (Roets & Van Hiel, 2011). Target motivation to detect deception potentially increases risk due to the motivational impairment effect (DePaulo & Kirkendol, 1988), where assessment ability is reduced by increased motivation. Target characteristics in how information is perceived and assessed can present risk as some characteristics can negatively affect ability to detect deception (Baker et al., 2012). The target's mindset with focus on cognition will affect how information is analysed by groups and individuals, however, adversary deception may seek to exploit this area and decrease target cognitive performance through a variety of tactics (Henderson, 2007). The target's mindset will affect how information is processed and is again an area that adversary deception will seek to exploit (Henderson, 2007). Target capabilities, in particular ISR capabilities, are linked to risk, as if these capabilities are reduced or unable to effectively monitor adversary behaviour then risk may be increased (Henderson & Pascual, 2008).

Guidance on Risk Assessment Use:

Following the completion of the DRAT and the identification of items which indicate risk from adversary deception operations, future scenario generation,

deception detection and risk management strategies can be implemented to reduce the impact of adversary deception.

Case Formulation

Upon completion of the risk assessment formulation of deception risk is required (Douglas, 2014; Hart & Logan, 2011). Case formulations seek to combine information from the risk assessment into an easy to understand narrative of why the adversary has behaved in this manner (Logan, 2014), which will then enable predictions of their future behaviour and the design of risk management to address specific adversary risk factors and reduce risk to target capabilities (Douglas, 2014; Vess, Ward & Collie, 2008).

Future Scenarios

Following the DRAT, and identification of risk factors showing the increased likelihood of deception the generation of future deception scenarios can occur. Future scenarios are generated in SPJ approaches as part of the process of mitigating and managing risk (Douglas, 2014; Hart & Logan, 2011). The current research develops risk scenarios from the SPJ approach where scenarios are developed from available evidence and practitioner judgement rather than upon probabilities. Hart and Logan (2011) recommend the generation of multiple scenarios, based on research, theory, and experience and case evidence. This will enable the generation of best case, worse case, linear (adversary behaviour remains the same) and twist (target or nature of deception may change) scenarios (Douglas, 2014; Hart & Logan, 2011). Future scenarios of adversary behaviour can be developed to focus on: The nature of who is being targeted, what type of deception is likely to be committed, the strategy employed to influence the target, deceiver motivation; the severity of harm, including physical harm, to the target and whether deception will occur across multiple communication channels; the imminence of the threat and identification of warning signs of increased imminence; the frequency and duration of the deception; and how likely it is for this deception to occur (Appendix 8.3). Through generating a future scenario of deception, risk management strategies may be developed as part of a proactive approach towards deception detection and risk mitigation (See Chapter 9).

Risk Management

Following the identification of potential adversary deception operations and the generation of risk scenarios where it is anticipated the adversary will target, risk management strategies can be developed reflecting the intensity of the risk posed (Douglas, 2014). Risk management strategies have been applied in previous SPJ approaches, for example, the HCR-20 uses risk management strategies to reduce risk of future violence by offenders (Douglas, 2014). The DRAT proposes risk management strategies focussing on: monitoring the adversary through context specific techniques and identifying circumstances under which risk should be reassessed, for example, through ISR capabilities (DCDC, 2007, 2011); supervision of the adversary should focus upon identifying surveillance strategies to manage risk and any forms of possible restriction of the adversary to reduce risk, for example, through Counter-ISTAR measures (Henderson & Pascual, 2008); and target inoculation planning should focus on enhancing the protection of targets, and identifying vulnerabilities which may be guarded against, for example, deployment of OPSEC capabilities (DCDC, 2007) and Defensive Counter-Psychological Operations (PSYOPS) capabilities (DCDC, 2007). Other considerations in risk management should also be examined to identify circumstances in which risk might increase or decrease and if there are any other techniques for reducing risk available to the target, for example, drawing attention to demonstrably false claims by the adversary through Offensive Counter-PSYOPS (DCDC, 2007). Once management strategies have been implemented ISR should be used to monitor change in adversary behaviour (Davies, Black, Bentley & Nagi, 2013; DCDC, 2007).

Communication of Deception Risk

Once practitioners have scored items for risk they will be able to inform key stakeholders of which items are or are not indicative of risk, the level of risk they are deemed to be, the risk management strategies that are required and the reasons for their judgements (Heilbrun et al., 2004). In complex decision-making environments there is debate as to whether risk should be communicated via probabilities or ratios of risk (Bachishin, Hanson & Helmus, 2012; Hanson, Babchishin, Helmus & Thornton, 2012) or through describing individual items and the risk that they may pose based on their behaviour (Scurich & John, 2012). These approaches may reflect

differences between contexts and audiences (Babchishin et al., 2012; Hanson et al., 2012; Scurich & John, 2012). The current approach will communicate risk based upon individual items of risk, the behaviour that led to the risk and risk management strategies which can be deployed; such an approach will reflect the multiple pathways to deception.

Decision-Making Biases in Assessing Risk

Individuals and organisations are argued to struggle in assessing risk due to heuristic biases, which can lead to over and underestimation of risk and may also influence how risk assessments are modified over the course of time (Koblentz, 2011 - See Chapter 2). Biases linked to underestimation of risk include: '*hindsight bias*' where focus on previous failures leads to future false alarms; and the availability heuristic where people judge the frequency of an event by how easy it is to imagine and ignore challenging risks (Koblentz, 2011). Biases linked to the overestimation of risk include: '*salience bias*' where distinctive stimuli are more likely to attract attention and disproportionately affect judgement, and the affect heuristic where individual perceptions of '*goodness*' and '*badness*' influence our perception of risk (Koblentz, 2011). Further, '*confirmation*' and '*disconfirmation*' biases can have a strong effect on how risk is assessed as analysts may seek information which supports their pre-existing beliefs, for example, CIA analysts selected intelligence to support their informant's assertions about Iraqi CBRN capabilities (Koblentz, 2011). Awareness of these biases is required when assessing risk, and practitioners should be encouraged to discuss their analysis with others to overcome such biases.

Validation and Future Directions:

The DARN and DRAT models outlined above are in construction phase and require further validation and amending through case study, and empirical approaches, before testing in applied settings. It is anticipated that not all items of risk will be seen in all adversaries and that items of risk may present in different ways in different adversaries as a wide range of state and non-state actors from different cultures and background seek to conduct deception against the UK and Allies. There are potential limitations with this approach as how each item is assessed may be interpreted differently according to the biases and motivations of the analyst, to

counter this an awareness of decision-making biases is required and it is recommended that analysts discuss their findings to counter such biases. Some items are likely to be more measureable than others presenting further challenges in assessing risk, and further research is required to identify such items and establish further guidance for use of the risk assessments.

Measures of Effectiveness

Measures of effectiveness (MoE) of risk assessments are often judged by their ability to predict recidivism rates amongst offenders, for example, Hanson et al. (2014) examined the predictive ability of the Static-99/R in assessing recidivism of sex offenders. This approach to MoE often argues that actuarial and SPJ approaches to risk assessment are roughly equal in predicting future risk (McDermott, Dualan & Scott, 2011; Yang, Wong & Coid, 2010). However, such claims require further examination as SPJ approaches often integrate risk management as part of case formulation and advise strategies to reduce risk (e.g. Kropp et al., 2011), which would have a biasing effect on any future comparisons between approaches.

A systems approach to examining MoE (Mackay & Tatham, 2011) would examine change in the adversary's behaviour across multiple sources. ISR capabilities can be deployed to monitor adversary behaviour and identify changes in behaviour that may indicate risk reduction, for example, a return to usual behavioural patterns, or the identification of false information. In assessing risk of violence Wilson et al. (2013) conducted risk assessments regularly over the course of a year to monitor changes in levels of risk and violence and such an approach of regularly assessing adversary risk is required to ensure that risk management can adapt to risks posed. Once risk of deception has been identified clear ways of measuring adversary behaviour change are required which can be measured via ISR capabilities to ensure that these changes have been met, or to adjust risk management strategies depending upon context. Further research should seek to explore ways of measuring reductions in risk of adversary deception following identification and management.

Content Validation

The content of the risk assessment requires further refinement and validation to ensure its usefulness as a diagnostic instrument. One technique for such validation

and refinement is through prototypical analysis as a method of analysing a construct's core components (Broughton, 1990). Such a technique has been used in the analysis of psychopathy assessments (Kreis, Cooke, Michie, Hoff & Logan, 2012) to examine how far items are representative of the constructs being examined. Further research should examine how representative of deception, its detection and associated behaviours the items in the DARN and DRAT are, as considered by SMEs in deception.

Case Studies

Conducting the risk assessments on case studies of strategic deception will provide an illustration of how the DARN can effectively screen for potential deception before the full DRAT assessment is conducted in operational environments. Case studies have frequently been used to assess predictive ability of counter-deception approaches, for example, Elsaesser and Stech (2006) outline how ACH-CD can be applied to the Battle of Midway, suggesting that case studies of historical and current threats will provide useful initial assessment of these techniques. Previous research into deception detection has often been conducted at group level and a requirement for adopting case studies is needed to examine whether deception detection approaches are effective in single cases (Evans, Houston & Meissner, 2012). However, as case studies do not allow strong inferences of validity and reliability to be made (Cook et al., 2014) further testing via simulation and in operational conditions is required.

Red Teaming

The development of recent DRE approaches to detecting deception (Colwell et al., 2013) have primarily used student populations (e.g. Leal, Vrij, Mann & Fisher, 2010) to examine the ability of such approaches in detecting deceit. However, this approach may not reflect the reality of high-stakes strategic deception by state and non-state actors where adversaries may have particular skill sets in conducting deception. In testing the DARN and DRAT, red teaming (DCDC, 2013) is the preferred option. Red teaming is beneficial across a range of areas related to defence science including in testing intelligence and security and testing systems from an adversary perspective (DCDC, 2013). Red teaming the DARN and DRAT will enable

thorough testing and assessment of the models alongside the identification of strengths, weaknesses and further ways of improving the outlined approach to identifying risk of deception before operational implementation (DCDC, 2013). Red team members should be experienced practitioners in the areas of deception and influence as such individuals will be able to present a credible challenge in assessing the ability of the DARN and DRAT to identify risk of deception.

Conclusion:

This chapter examines the research surrounding risk assessments used in forensic and clinical environments for assessing risk of violence, stalking and sex offences and approaches to assessing risk in security environments. Actuarial and probabilistic approaches to risk assessment were found wanting, whilst SPJ approaches to assessing risk whilst providing risk management strategies were identified as a logical next step in assessing adversary risk of deception.

Through a review of relevant empirical and practitioner research related to deception across different domains a screening tool and risk assessment were developed for assessing risk of adversary deception. The DARN proposes a decision-making model which leads to the identification of potential and apparent adversary threats, leading to the activation of the DRAT which conducts a full risk assessment, before outlining potential future scenarios based on adversary behaviour and risk management strategies which negate risk posed by the adversary to friendly capabilities. Further steps are required to validate and refine this approach to risk assessment through case studies of existing and current threats and red teaming to identify, strengths, weaknesses and areas for improvement of this approach to mitigating adversary threat.

Chapter 9: Future Threat Scenario Assessment and Development: A Proactive Approach to Deception Detection.

Introduction

In deception detection research, approaches have traditionally focused upon previously experienced events or in response to current operational challenges, however, in forensic, security and intelligence domains there is an intrinsic need for understanding the risk of future threats and to incorporate consideration of deception into this process, both in real-time and to proactively respond to forthcoming challenges. Technological interconnectedness creates ever more complex challenges which can occur where future threats will not only come from state and terrorist actors, but from the increasing sophistication of Organised Crime Groups (OCGs – EUROPOL, 2013). Hence the multi-faceted nature of future threats which cross multiple criminal domains and occur on a transnational basis illustrate the requirement to develop UK capabilities to proactively detect and investigate (HM Government, 2013) while increasing resilience against such threats (Fussey, 2011; McFarlane & Hills, 2013).

Through developing potential scenarios of future threats a comprehensive risk assessment may be conducted and a response developed in order to negate risk to UK interests (Buytendijk, Hatch & Micheli, 2010; Fotr, Špaček, Souček & Vacík, 2015; Miller & Waller, 2003). Scenarios for the purposes of the current research are defined as "d*escriptions of possible futures that reflect different perspectives on the past, the present and the future*" (van Notten, Rotmans, van Asselt & Rothman, 2003, p. 424). This provides a useful focus on the construction of future scenarios although Ramírez and Selin (2014) argue for the need to include context and purpose. This chapter explores and presents reactive, active and proactive approaches to deception detection and outlines the need for a future-focussed approach to detecting deception, presents scenarios and risk assessments of future threats. Chapter 9 develops further the work of Chapter 8 through developing future scenarios of the potential threats that the risk assessments will be tasked with mitigating. Following the development of potential future scenarios the risk assessments developed in Chapter 8 were conducted on two of the scenarios to provide an example of this new approach towards deception detection.

Reactive Approaches to Past Transgressions

Methods of examining materials as an assessment of credibility have been historically employed (see Chapter 2 for a detailed description). This includes SVA (Rassin, 2000) and RM (Sporer, 2004). There is limited evidence focusing on the use of such tools in the determination of future threat although there are elements of both methods that could be usefully applied to understanding risk. Recent evidence (Akehurst, et al., 2015) has supported the use of elements of such tools in the detection of malingering in regard of physical and psychological illness. Although nonverbal approaches to deception detection have sought to examine facial expressions, microexpressions (Ekman, 2001) and hand and finger movements (DePaulo et al., 2003) for cues to deceit there is limited evidence to support the utility of such approaches and therefore multi-modal approaches are considered to warrant further investigation and supports a holistic approach.

Deception detection in military environments is often reactive in nature with intelligence analysis often conducted ad hoc to accommodate the dynamic nature of theatres of operation (Heuer, 2005). Techniques for detecting deception in military environments include ACH (Heuer, 1999; Stech & Elsässer, 2003; Stech & Elsässer, 2004), the Busby-Whaley Ombudsman technique (Whaley & Busby, 2002) and a counter-deception approach advocated by Bennett and Waltz (2007) (See Chapters 4 and 6). ACH uncovers deception through generating multiple hypotheses and weighing these against available evidence (Stech & Elsässer, 2003). This approach parallels that of police investigations where evidence is sought to identify suspects. The use of ACH in detecting future threat has the potential for operational utility, particularly if based on a considered understanding of the target of the assessment and the potential options open to them. The Busby-Whaley Ombudsman technique detects deception through examining discrepancies, misdirection and irrelevancies alongside indirect thinking (Whaley & Busby, 2002) – this incorporates a focus that enables a broader consideration of innovative thought and maintaining openness in decision-making – therefore potentially avoiding confirmation bias. The holistic approach to counter-deception advocated by Bennett and Waltz (2007) comes into effect once an awareness of deception has occurred (Bennett & Waltz, 2007) therefore identifying potential future threats for which strategies may be developed to mitigate the effects of adversary deception while giving the impression of being deceived.

Active Approaches

Active approaches to detecting deception in interpersonal interactions have sought to increase behavioural differences between truth-tellers and deceivers through increasing cognitive load (Vrij, 2015b), adapting questioning strategies to circumvent deceiver's impression management strategies through asking unanticipated questions (Vrij, 2015b) and contrasting interviewee's statements to evidence (Dando & Bull, 2011; Granhag & Hartwig, 2015 – See Chapter 2). Active approaches in deception detection involving interactions between sender and target are assumed to be closer to reality (George, Marett & Tilley, 2004). However, such approaches focus primarily on increasing cognitive load to detect deception and ignore how future deception occurs from the surrounding context, whether political or social.

Active strategies in detecting mediated deception have sought to examine cues to deceit across grammar, plausibility, claims and inconsistencies with experiential norms (Grazioli, 2004). However, features-based models of credibility (e.g. Grazioli, 2004; Johnson et al., 1992) are reliant upon an individual's experience of using a communication medium and suggesting that unfamiliarity will result in difficulties in detecting deceit. In protecting organisations from insider threat a more active approach to deception detection is required where individuals' deviations from usual behaviour and normal language may indicate threat (Santos et al., 2008; Taylor et al., 2013) enabling a response to be developed to mitigate further risk. Individuals within organisations may further be vulnerable to threats posed by social engineering approaches (Larson, Jones, Rashid & Baron, 2015; Stajano & Wilson, 2015); therefore a holistic understanding of deception and the multiple ways in which organisations may come under threat is required alongside means of increasing resilience against threats through strategic planning.

Active approaches towards mediated deception have applied interviewing techniques from interpersonal environments (Colwell et al., 2013; George et al., 2008). ACID (Colwell et al., 2013 – See Chapter 2) has been adapted to detecting deception in synchronous computer-mediated communication (CMC) and found that honest statements are often longer and more detailed than deceptive ones. Although these approaches are more active in their assessment of credibility through seeking to challenge deceivers' accounts, they are focussed around an individual act of deception

rather than deception at a strategic or operational level and do not provide techniques for target inoculation.

Proactive Approaches

To reduce future risk recent approaches in deception research have focussed on uncovering malign intent (Burgoon et al., 2009; Mac Giolla, Granhag & Vrij, 2015), illicit planning activities (Morgan, Rabinowitz, Hilts, Weller & Coric, 2013; Morgan, Rabinowitz, Leidy & Coric, 2014) and deterring individuals from committing deception (Leal, Vrij & Mann, 2015; Palasinski & Svoboda, 2014). In particular, these approaches have assumed that it may be possible to counter potential acts of terrorism such as in public spaces including airports and borders (Burgoon et al., 2009; Nunamaker, Golob, Elkins, Burgoon & Derrick, 2015; Vrij, Granhag et al., 2011b). Vrij, Granhag et al. (2011b) argue that malign intent in airport settings can be uncovered through examining cues to plausibility, contradictions and spontaneous corrections. Furthermore, Vrij, Leal et al. (2011) found that when questioning individuals engaged in a mission to deliver a package to another 'agent' that cues to plausibility enabled discrimination between truth-tellers and deceivers.

Strategic interviewing of individuals on their intentions and corresponding planning activities has also been advocated to detect future threats (Clemens, Granhag & Strömwall, 2011). Although useful in securing evidence for prosecution before incidents may occur (Clemens et al., 2011), this approach relies upon previously gathered evidence with which to question subjects so may not be applicable to all situations. Further issues may arise when seeking to detect deception in highly complex, low-base rate environments where adversaries may construct credible appearances over a period of time in preparation for deception operations.

In detecting deception related to bio-threats in low-base rate environments, Morgan et al. (2014) and Morgan et al. (2013) found that modified cognitive interviewing outperforms human judgement, apart from experienced interviewers, in detecting bio-threats. Morgan et al. (2014) and Morgan et al. (2013) increased the validity of their research through recruiting participants who worked with chemicals and would have knowledge of how bio-threats may be created reflecting the complexity of human behaviour in real-world interactions, highlighting the ability of

modified cognitive interview techniques to identify deception between both truth-tellers and deceivers with bio industry experience.

Undercover interviewing in field settings (Jundi, Vrij, Hope, Mann & Hillman, 2013; Vrij, Mann, Jundi, Hope & Leal, 2012) has sought to be proactive in detecting deception and presents an alternative to formal investigative interviews which may affect on-going investigations, including undercover operations. Through engaging a target before an official interview there is potential to aid future investigation through highlighting inconsistences in narrative and alibis between the undercover and formal interview (Jundi et al., 2013). However, undercover interviewing focusses on a target that has already been uncovered which does not reflect the reality of how all future threats are detected following their manifestation. To anticipate and respond to strategic deception an even more proactive response is required where a response is developed in advance to counter anticipated future threat.

Approaches to increasing resilience against crime and terrorism have focussed upon the use of surveillance, deterrence and target hardening against threats (Coaffee & Fussey, 2015; Fussey, 2011; Leal et al., 2015; Palasinski & Svoboda, 2014). Target hardening measures have sought to influence offenders' decision-making through decreasing the attractiveness of potential targets, for example, appearances of surveillance to decrease online fraud (Palasinski & Svoboda, 2014), whilst increasing the likelihood of the offender being caught and reducing the likelihood of the offender acting on their intentions (Fussey, 2011). Other approaches to resilience have focussed upon the proactive identification and resolution of systems vulnerabilities before they are exploited by adversaries (McFarlane & Hills, 2013; Wallace & Lofi, 2014). Such an approach highlights the benefits of anticipating threats and scenario planning will provide a useful lens with which to inoculate targets against deception.

Proactive surveillance of potential threats is required to reduce the risk of casualties from acts of terrorism, whether committed by '*lone wolves*' or groups (Gordon, Sharan & Florescu, 2015). A '*lone wolf*" will be harder to apprehend than a group, as there is less chance of intercepting communications, and identifying and infiltrating networks (Gordon et al., 2015). Techniques for tracing such individuals include, online monitoring of purchases, communications surveillance and 3rd party informants (Gordon et al., 2015). Highlighting the need for sophisticated approaches employing multiple techniques to detect future threats involving deception.

Warning and priming individuals about the possibility of deception in their online interactions may reduce the truth bias whilst increase their suspicion and subsequent effort towards detecting deception (George et al., 2008; Modic & Anderson, 2014). Warning and priming individuals increases their ability to detect deception in online environments (George et al., 2004; Grazioli, 2004), although this may also increase false positives which then need to be disconfirmed to detect truthful information (Biros, George & Zmud, 2002). If individuals are aware of the risks posed by being in a situation, particularly when there are threats posed by terrorism, then they will be less likely to engage in that situation (Gray & Wilson, 2009). Through proactively warning individuals about deception and risk processes of mitigation against such threats are activated and through exploring the potential of future risks comprehensive responses can be developed to meet such challenges.

Proactive policies are being adopted by various nations including the UK and Spain in order to mitigate current and future threats posed by terrorism (BBC, 2014; Gil-Alana & Barros, 2010). In the UK individuals returning from current conflict areas are being identified and arrested on their return, before they are placed into programmes run by the 'Prevent' strategy on counter-terrorism (BBC, 2014; HM Government, 2011). The 'Prevent' strategy will challenge those individuals who have become radicalised during their time in Syria, thus proactively seeking to prevent individuals from engaging in political violence upon their return to the UK. In challenging the activities of ETA in Spain, proactive strategies of banning political parties related to ETA were effective in reducing funding available to conduct terrorist activities and are far more effective than reactive punitive measures which further alienated the population (Gil-Alana & Barros, 2010). Through adopting proactive strategies for reducing risk it is anticipated that there will be less threat to UK interests.

Scenarios for Future Planning

There is a crucial need to focus on foresight and possible future environments to address future threats rather than focussing on reactive approaches (McFarlane & Hills, 2014). Individuals often form judgements based on available information which may be biased (Hogart & Soyer, 2014; Kahneman, 2011), creating scenarios will encourage creative thinking in response to future challenges. Scenario use for

examining futures has been conducted across a wide range of areas, including in strategic planning (Bakker, 2012; DCDC, 2010a; 2010b; 2014), management and business (Mante-Meijer, van der Duin & Abeln, 1998; Wright, 2005) and in the risk assessment and management of offenders (Douglas, 2014; Hart & Logan, 2011). Scenarios may be used as decision-making tools to overcome limitations and enable preparation for the unexpected and the construction of meaning from uncertainty and ambiguity through developing creative future responses (Amer, Daim & Jetter, 2013; Buytendijk et al., 2010; De Jouvenel, 2000; Bowman, MacKay, Masrani & McKiernan, 2013; Durance & Godet, 2010; Fotr et al., 2015; Godet & Roubelat, 1996; Inayatullah, 2008; Varum, & Melo, 2010; Wright, 2005). When organisations capacity to make sense is challenged by unexpected phenomena, which cannot be located within existing mental models, rejection of such phenomena can lead to potential threats (Wright, 2005). Constructing wide-ranging future scenarios enables future planning to be conducted in a holistic approach enhancing the ability to deal with uncertainty (Amer et al., 2013). Scenarios are argued to be socially constructed narratives which integrate predetermined events with critical uncertainties to encourage future-thinking and are not predictions or forecasts of the future (Wright, 2005). Scenario generation allows further exploration of futures that may not be influenced by understanding past behaviour of the actors involved but through exploring unknown unknowns, events which may be hard to probabilistically examine (Ramírez & Ravetz, 2011). DCDC (2014) refers to '*shocks'* and Ramírez and Ravetz (2011) refer to '*feral futures*' both of which are considered as low probability events which have large consequences and may be difficult to manage and control requiring a need for the development of techniques that may help to mitigate such threats.

Godet (2000) argues that acceptable solutions are needed to meet the challenges posed by future scenarios. Adapting this perspective if analysts are able to construct future scenarios involving deception and threat then new perspectives of deception detection can be developed and deployed to meet such challenges. In a proactive approach to deception detection an awareness of the unexpected is required and through scenario building it is argued that greater sense can be made out of potential future threats. However, as events are being examined into the future, some degree of extrapolation and imagination is required alongside the examination of current events (DCDC, 2014).

Rationale

Taking a proactive approach to deception is required to mitigate current and future threats. Through understanding how possible future deception will materialize a more comprehensive response may be developed to counter such threats, otherwise we will remain open to adversary exploitation. Whaley and Busby (2002) refer to 'predetection' as a method of detecting deception where through understanding and predicting an adversary's deception style, aims and capabilities will challenge adversary deception. This principle can be expanded to examine the future threats that adversaries may pose and proposing strategies to challenge those threats. A proactive approach to deception detection will examine potential future scenarios and construct a robust risk assessment for analysing emerging threat.

Scenario Development:

When seeking to take a proactive stance towards deception detection of future events it is pertinent to tailor responses to plausible future threats across a range of contexts (Douglas, 2014; Hart & Logan, 2011). A variety of threats may emerge from current on-going conflicts in Eastern Europe, Africa, the Middle East and Asia alongside a growth in OCGs (EUROPOL, 2013) and how these impact on UK interests requires an understanding of how global trends will shape the world to come. As part of the 'Strategic Trends Programme', the Development, Concepts and Doctrine Centre (DCDC) outlines future scenarios of key factors in science and technology, resources, social, geopolitical and military areas (DCDC, 2010a; DCDC, 2010b; DCDC, 2014) whilst EUROPOL (2013) conducts an assessment of serious and organised crime and how these effect European and UK interests. Although it is important for strategic purposes to propose potential future scenarios it is acknowledged that these scenarios may not actually occur, but rather are examples of how risk assessment approaches (See Chapter 8) can be used to examine deceit in potential future events. The current research will develop scenarios based upon the critical realist and constructivist '*Intuitive Logics*' methodology (Amer et al., 2013; Bradfield, Wright, Burt, Cairns & van der Heijden, 2005; Ramírez & Selin, 2014; Wilkinson, Kupers & Mangalagiu, 2013) where scenarios are developed primarily through qualitative techniques and offer narratives of potential futures rather than

probability-focused futures (Fotr et al., 2015; Ramírez & Selin, 2014; Wilkinson et al., 2013).

Method

The project goal

The explorative approach to scenarios is a qualitative approach examining the structural uncertainty of futures to gain awareness and critical insight (Börjeson, Höjer, Dreborg, Ekval & Finnveden, 2006; van Notten et al., 2003). The explorative approach has clearly defined goals (van Notten et al., 2003), and the current research focuses on deception issues-based scenarios to examine how risk assessment and management can be used to meet future challenges.

Process Design

An assessment of current events and the risks they pose to UK interests led to the development of scenarios for current and future threats. The explorative approach (Börjeson et al., 2006) examines a subject from a wide-range of perspectives, and is set in the future allowing for long-term change. In the current approach a wide-range of perspectives are required to analyse potential threats to the UK in the present and future. The explorative approach can be split into external and strategic scenarios, the current research focuses on external scenarios which examine factors beyond the control of actors and can be used to develop robust-strategies to meet such challenges (Börjeson et al., 2006). Qualitative or narrative scenarios are considered appropriate for analysis of complex situations where there are high levels of uncertainty as they enable greater flexibility in adapting to threats (van Notten et al., 2003). Probabilistic reasoning in assessing futures is often difficult to interpret by audiences providing further justification for the use of narrative formulations (Hogarth & Soyer, 2014).

When generating techniques from an explorative approach for external threats (Börjeson et al., 2006) surveys, workshops and the Delphi method may be used. The current approach modifies this in designing scenarios for current and future threats with a desk-based method of data collection (van Notten et al., 2003). This approach included a literature search of recent Government publications (DCDC, 2010a; DCDC, 2010b; DCDC, 2013; EUROPOL, 2013; HM Government, 2013), academic

and journalistic articles surrounding historical and current events (See Appendix 9.1), alongside SME knowledge generated from Chapter 6 to generate the future scenarios (See Appendix 9.2).

Scenario Content

In ensuring transparency in the construction of future scenarios (Coates, 2000; Godet, 2000), the scenarios developed are all examining potential threats to the UK from a variety of perspectives for which varying forms of deception by the adversary is required. These scenarios may be considered complex (van Notten et al., 2003) as they focus across multiple actors, factors, sectors and time and spatial areas and have differing amounts of information available to the analyst for assessing threat. Complex systems often have an unpredictable nature and are driven by the relationships within and between actors and their affects across the system (Wilkinson et al., 2013). Complex scenarios may more accurately reflect future events and the risk management strategies required to mitigate threat.

The ten scenarios developed focus around key themes with historical precedent related to: deception about weapons capabilities (e.g. Sadam Hussein and Iraq); energy conflicts (USAID, 2010), for example, Nigeria (Klare, 2014); radicalisation/diaspora (e.g the July 7th Bombers and recent Lee Rigby case); insider threat (e.g. Edward Snowden and Chelsea Manning); territory and resource disputes (e.g. UK-Argentina; Sudan-South Sudan); internal intercultural conflict (e.g. Highfields – Leicester); religious conflict (e.g. Pakistan – India); intelligence-gathering (e.g. BBC, 2013); UK organised crime (e.g. BBC, 2015); and exploitation of 3D printing (e.g. 3D printed guns – VICE, 2013) (See Appendix 9.2). Due to the wide-range of variables affecting potential future scenarios a holistic approach is required to face the myriad challenges to the UK.

Results - Scenario Assessment:

Scenario Validation

Consistency techniques are useful for ensuring consistency between or within scenarios, Börjeson et al. (2006) state that consistency testing is often carried our via qualitative and potentially implicit means. The current research used three SMEs in

deception with 3 – 26 years experience (M=15.67; SD=11.53) to validate each scenario on a Likert-type scale of one to five (1 = strongly disagree to 5 = strongly agree) across each scenarios plausibility, consistency, utility/relevance, challenge, novelty and creativity (Amer et al., 2013). The results of such validation are outlined in Table 9.1.

Table 9. 2: Scenario Validation Table

Scenario	**Plausibility**	**Consistency**	**Utility/ Relevance**	**Challenge**	**Novelty**	**Creativity**
Weapons Capabilities	5	5	5	5	4.17	4.17
Energy Conflicts	5	5	5	5	4.17	4.17
Radicalisation and Terrorism	5	5	5	5	4.17	4.17
Insider Threat	5	5	5	4.67	4.17	4.17
Territory and Resource Disputes	5	5	5	4.67	4.17	4.17
Internal Intercultural Conflict	5	5	5	4.67	4.17	4.17
Religious Conflict	5	5	5	4.67	4.17	4.17
Adversary Intelligence Gathering	5	5	5	4.67	4.17	4.17
UK OCGs	5	5	5	5	4.5	4.5
3D Printers	5	5	5	5	4.5	4.5

Scenario Risk to the UK

Following the scenario validation each scenario was further rated on a 5 point Likert-type scale by the three SMEs according to which area, for example, individual or group, each scenario effects (see Table 9.2) and which area of infrastructure each scenario effects (see Table 9.3). Taken together these assessments show that as each potential act of future deception effects differing areas of the UK in differing ways a more tailored approach to deception detection is required focussing across a wide-range of behaviours.

Table 9. 3: Scenario Impacted Area

Scenario	Individual	Group	Non-Governmental Organisation	National	Global
Weapons Capabilities	5	5	5	5	5
Energy Conflicts	4	3.33	3.33	5	5
Radicalisation and Terrorism	4	4.67	3.33	4.67	4.33
Insider Threat	3.67	3	3.33	4.67	4.33
Territory and Resource Disputes	3.57	3.67	3	5	4.33
Internal Intercultural Conflict	3.67	5	3.33	4.67	3.67
Religious Conflict	4.33	4.33	4.33	4.33	5
Adversary Intelligence Gathering	3.33	4.67	4.33	5	4
UK OCGs	3.33	3	3.33	4.33	4.33
3D Printers	3.33	4.67	3.33	4.67	4.33

Table 9. 4: Scenario Impacted Infrastructure

Scenario	Technology		Financial	Social	
	Development	Infrastructure		Internal Conflict	International Conflict
Weapons Capabilities	5	5	5	3	5
Energy Conflicts	4.33	4.67	4.67	2.33	5
Radicalisation and Terrorism	3	4	4	5	4.67
Insider Threat	4.67	4	4	2.67	3.67
Territory and Resource Disputes	3	3.67	3.67	2.67	5
Internal Intercultural Conflict	3	3.33	3.33	5	3
Religious Conflict	3.33	4	4	4	4.33
Adversary Intelligence Gathering	4.33	4.67	3.67	3.67	4.67
UK OCGs	2.67	2	3.33	3	2.67
3D Printers	4	4	3.33	4.33	4.67

Threat Response

The following section will outline a tailored strategy for analysing threat and risk of deception in two scenarios examining: diaspora groups susceptible to radicalisation; and detecting adversary intelligence gathering. The DARN and DRAT (See Chapter 8) propose groundwork for early-warning and identification of risk of deception, before outlining risk management strategies to negate risk of deception. In developing new risk assessments case studies of how these assessments work provide useful guidance in their application to assessing and managing risk (Beardsley & Beech, 2013; de Vogel, ven den Broek & de Vries Robbé, 2014; Logan, 2014). Risk formulations should be simple, coherent and informative (Logan, 2014) and this process is required in case formulation of risk of deception to ensure practitioners and stakeholders have awareness and understanding of risk management strategies. Adapting a perspective from violence risk assessment, evaluations of deception risk should take into account both factors which may harm the UK but also consideration and implementation of factors that may increase protection (de Vogel et al., 2014). Such an approach is taken in the current research where the DARN and DRAT are applied to two scenarios with potential consequences for the UK.

Radicalisation and terrorism in diaspora groups

<u>Risk Assessment:</u>

There is risk of terrorism by diaspora groups within the UK instigated by groups from their home nations. The major concern is the concealment of developing and coordinating attacks using homemade improvised explosive devices (IEDs). Such attacks will be targeted against the general public in an attempt to influence decision-makers and undermine public confidence in authorities. Identifying the potential location of such an attack is required to increase resilience against posed threats.

Actors will be highly motivated to use deception to conceal their activities from the general public and intelligence agencies. Such activities and deception operations will be guided by the actors' radicalised world views, with potential reference to religious texts and teaching from extremist scholars providing justification for violence and deception towards other ideologies. Deception will be

used in concealing in-real-life and online communications regarding their malign activities, in the purchasing of compounds used to make IEDs and the locations where the IEDs are constructed. Deception will also occur in target reconnaissance in-real-life and online environments and in the concealment of movement of IEDs to selected targets.

Analysts should anticipate deception by adversaries as there are large gains and little cost to the adversary even if they are apprehended. Prior to the identification of actors it is difficult to analyse their capabilities, knowledge and experience and the effect of personality on their behaviour although some tentative conclusions regarding adversary resources may be made from resources available to previously apprehended groups.

The stakes are high for analysts to accurately detect deception due to the potential casualties if the deception is not identified and this will increase the analysts' motivation to detect deception, from which decision-making biases may emerge. To counter potential biases analysts are recommended to discuss their findings with others. There are a large range of resources available to the analyst with which to detect deception and they can select tactics according to context.

Risk Formulation

There is an acute risk of deception by the actors towards the general public and intelligence agencies in real-life and online interactions where actors are sourcing materials for IEDs, conducting target reconnaissance and concealing their activities from others. The motive for the deceivers' behaviour is to conduct a terrorist attack to support ideological and political beliefs. Successful deception would lead to potential casualties and fatalities amongst the general public, damage to infrastructure and the economy and a loss of confidence in the security services and decision-makers.

Actors will use a variety of tactics to deceive others regarding their activities. Firstly actors need to conceal their activities through controlling information by blocking and concealing access to their behaviour and intentions. Secondly, actors will need to condition the targets that they are buying materials from to appear credible and will need to condition anyone they interact with in reconnaissance efforts to again appear credible. There are a range of tactics available to achieve these aims including verbal and non-verbal impression management, linguistic and behavioural characteristics that increase credibility (e.g. positivity, convincing and mimicry), and forms of influence (e.g. appearing authoritative and attractive).

Warning signs of increased risk may be linked to actors beginning to attempt to buy materials for IEDs, conducting reconnaissance and moving IEDs to the target location. Through conducting surveillance against such threats changes in behaviour may be identified and acted upon.

Risk Management

To increase resilience against malign activities the identification of individuals is required to monitor their in-real-life and online behaviour. Monitoring this behaviour will enable identification of when individuals are researching targets and purchasing materials capable of constructing IEDs. Techniques including HUMINT, image intelligence (IMINT) (photographs of activities) and COMINT (monitoring of phone conversations and online activity) will provide clearer evidence of the extremists' progress towards constructing IEDs and when they may be likely to conduct an attack, enabling intervention by authorities before the attack is conducted.

Activity should not be restricted until the actors' are in the final stages of planning the attack, unless there has been a sudden change in behaviour, in an attempt to uncover further actors or contacts through social network analysis and to ensure there is substantial evidence for prosecution. If there is a sudden change in adversary indicating escalating threat then they should be apprehended due to the risks involved.

A range of techniques can be utilised to increase resilience against this threat. Intelligence analysts should be made aware that deception may be occurring through concealment of information as well as other approaches. Companies selling materials that can be used in constructing IEDs should be informed of potentially deceptive buyers and should develop systems to record who buyers are (e.g. through ID and CCTV footage) and the reasons for which they require these materials. CCTV and visible guardianship should be displayed at potential target locations to reduce the likelihood of threats to these locations, although the effectiveness may depend on adversaries' willingness to conduct the attack in the face of punitive consequences.

Analysts should be aware of changes in domestic and foreign affairs that may have an effect on the adversary behaviour and whether this will require a reassessment of risk accordingly.

(See appendix 9.3 for full scale risk assessment)

Detecting adversaries and their intelligence-gathering

Risk Assessment

Current risk reflects on-going in-real-life and online adversary intelligence gathering efforts by multiple known and unknown actors affecting UK capabilities and interests, with particular cause for concern regarding the spreading of misinformation and potential for information theft whether through social engineering or insiders and the resultant damage this can cause to UK interests, use of resources and image.

Adversary doctrine highlights the use of deception across a range of contexts and communication modes and is often used in interactions with other nations to increase global strategic position. Previous experience of adversary behaviour has indicated their wide-range of resources and consistent usage of deception across a range of contexts in achieving a range of goals, focussing usual adversary deception strategies and tactics enables a profile of their behaviour to be developed.

Actors will be highly motivated to convince others that they and the information they present is credible and their cognitive and language abilities will reflect their planning spontaneity and selection of strategies they perceive as effective in deceiving others across multiple channels. Personality will affect adversary behaviour, with a minority of individuals potentially having more Machiavellian behavioural characteristics in their exploitation of the target.

In detecting adversary intelligence-gathering and misinformation there are important stakes in identifying and protecting areas of exploitation, which will increase target motivation to detection deception based upon empirically validated behavioural cues to deceit rather than subjective beliefs. Vulnerabilities occur amongst deception detection amongst lay individuals who lack awareness of deception cues across communication channels. Analysts have a large number of analysis and surveillance techniques which can be deployed to meet challenges posed in uncovering adversary intelligence-gathering and deception operations, however, the general public may not have these techniques or knowledge and may be influenced by adversary misinformation, which in turn, may affect wider concerns in the UK.

Risk Formulation

Deception will be potentially already occurring and on-going and may only stop once adversary aims have been met or they have been apprehended. Concealment of intelligence-gathering will be targeted towards intelligence analysts and decision-makers. Verbal and non-verbal impression management skills will enable adversary

actors to condition and develop trust with the target over a period of time so that the target is likely to find later behaviour credible. Tactics will be used to exploit the targets' hopes, fears and emotional state, alongside the use of ruses to direct the target's attention and resources away from key areas of exploitation. Such tactics make prove more effective in deceiving the general public than intelligence analysts.

Adversaries' will use a range of context-dependent tactics to control information presented to others (e.g. decreasing, deflecting and blocking). Revealed information with have simple narratives, including partial truth to avoid inconsistencies. Adversary actors will engage in a number of tactics to appear credible to others including fluency, positivity, objectivity, subtlety, committed and convincing in their interactions with others. Actors may also choose to emphasise certain areas of information to direct target attention away from other areas and will also need to mimic behavioural norms to appear credible to the target.

Adversary actors have the potential to use a variety of influence tactics to appear credible to others including referent power, being attractive, reciprocating behaviour, social proof and presenting scarce information to the target.

There is potential harm to the target from the adversary gaining information on new technologies leading to potential economic harm from waste of resources, alongside security implications if the adversary can successfully uncover sensitive information. There is a chance that the deception could proliferate across multiple mediums and sources and this will reflect adversary attempts to develop credible persona and the spread of misinformation may occur in both in-real-life and online environments.

Risk Management

The main areas of risk management consist of monitoring, supervision, target inoculation planning and other considerations. The risks posed by adversaries conducting intelligence-gathering and deception operations within the UK means that once they have been identified they should be routinely monitored to identify threat. Surveillance techniques including HUMINT, IMINT (e.g. photographic evidence) and COMINT (e.g. phone and CMC based communications) should be used to monitor individuals to ascertain their targets, identify further actors and establish when intelligence-gathering operations have begun.

Only if serious threat is posed by identified adversary actors they should have their movements restricted – if the threat they pose is not large then they should be monitored to identify further actors and this will also enable them to be fed with misinformation to send back to the adversary.

Inoculation of targets against deception is required, including monitoring and informing key industries when they are being targeted by adversaries, and that such attempts will be made in-real-life and online. Companies with links to key infrastructure require that individuals approaching their business are verified across a range of sources to ensure their credibility, and reduce the chance of being deceived.

Changes in international affairs may increase or decrease risk reflecting the adversary's aims in those situations. A reassessment of risk should be conducted if the adversary's nation is involved in conflict as the potential for deception and selected strategies and tactics will change to reflect the operational context. A reassessment of risk will also be required if there is an increased number of identified adversaries operating in the UK in order to ascertain motives and reasons for their presence. CI assets may also be deployed to feed misinformation to adversaries in their intelligence-gathering operations.

(See appendix 9.4 for full scale risk assessment)

Discussion:

Findings

The current chapter explores reactive, active and proactive approach to deception detection before constructing scenarios of potential threats and conducting theoretical risk assessment of Scenarios 3 and 8. Although the presented risk assessments are theoretical they provide an important illustration of the range of application of the DARN and DRAT in addressing and responding to threats, whilst increasing target resilience. An important stage of constructing new risk assessment measures is to provide such illustrative examples before further testing and development is conducted (de Vogel et al., 2014). Through treating deception from a risk assessment perspective, risk management strategies can be developed responding to the key tactics and strategies used by the adversary to appear credible to others rather than relying upon singular approaches towards deception and its detection. Next steps should consider applying the DARN and DRAT to historical and current

case studies, alongside developing user guidance for practitioners. Risk formulation is an expanding area of research within psychology and research is only beginning to examine the value of risk formulation in hypothesising the management plans required for reducing risk (Logan, 2014). However, such an approach is promising towards reducing and managing the risk posed by adversary deception and future work will develop this further.

Limitations

There may be limitations associated with constructing scenarios with entrenched thinking in present solutions, possibilities, limitations (Börjeson et al., 2006) and biases (Buytendijk et al, 2010; Ecken, Gnatzy & van der Gracht, 2011; Ramírez & Ravetz, 2011, van Notten et al., 2003). These limitations may be countered through an iterative approach where scenarios and strategies are reformed and adjusted according to advances in technological capabilities, for example, DCDC (2014) presents updated scenarios to DCDC (2010a) reflecting advances in technology and associated areas of development. McFarlane and Hills (2014) consider that to ensure resiliency to threat system testing should be conducted continuously to ensure that vulnerabilities are identified before adversaries uncover them.

Scenario development of potential future events is often accused of being subjective and that different scenarios may be produced by different analysts who have access to the same reference material. Furthermore, future scenarios may fail to examine outlying factors which may influence the way in which future deception threats manifest. However, the current research sought to address this issue by providing scenarios of a range of potential future threats to increase innovative thinking regarding future challenges rather than as predictions of the future. Some of the scenarios may not be considered as plausible versions of the future, however, such scenarios may actually increase ability to think outside of existing mental models and approaches helping to create further inquiry (Ramírez & Selin, 2014) justifying the current approach to scenario development.

In conducting risk assessment, formulation and management practitioners should be required to conduct this process from a consensus perspective which is argued to increase quality in judgements (de Vogel et al., 2014). Such an approach will be required in future risk assessments to enable practitioners to discuss areas of

risk and reduce rater biases, although de Vogel et al. (2014) acknowledge that such a process may be time consuming and maybe impractical in some contexts.

Future Directions

The current chapter highlights the need for developing strategies to reduce risk from future threats, through target hardening and increasing resiliency in the target towards deception. As technological advances occur and global relations change reflecting aims and aspirations further potential futures will occur increasing the need for further scenario development. To anticipate such challenges future scenario development of potential futures should utilise the real-time Delphi approach to scenario development (Gordon et al., 2015), which enables SMEs to develop scenarios in a real-time basis through online communications, enhancing the decision-making process.

In assessing the ability of ACH to detect military deception, historical case studies have been conducted (Stech & Elsässer, 2003; Stech & Elsässer, 2004). Future research examining high-stakes deception should consider explanatory case study methods to analyse the ways in which strategic deception is conducted and uncovered. Explanatory case studies consider links that need to be examined over time (Yin, 2003) and may uncover how events have developed, suggesting the application of case study methodology to deception research using risk assessment approaches may prove fruitful in analysing individual cases of deceit.

Conclusion:

Proactive approaches will enable a faster identification of deception and the ability to counter it. Through developing potential current and future scenarios responses can be developed which focus upon the source of the deception, the intent to deceive, the deceptive content, the strategies used to uncover the deception and the target itself. There is a requirement for scenarios to be developed for multiple future threats across differing contexts to reflect the changing balance of power within and between nations across time. A focus on risk formulation and management is required in meeting such challenges. Risk formulation enables the exploration of why individuals and groups decide to engage in deception and this will lead to the development of appropriate strategies to manage risk, including focussing beyond

identifying deception, towards managing such individuals' behaviour to reduce the potential for deception and increasing the resilience of targets towards deception.

Chapter 10: Conclusion

Through adopting a holistic approach, this thesis expands current understanding of the deception and deception detection process and provides a clear outline to both researchers and practitioners of a new approach to how deception may be detected across converging communications modes covering tactical, operational and strategic levels of engagement.

Contributions to Research and Practice:

Key contributions to research and practice have been developed for use in research and applied environments. The HMD has been developed from a theoretical approach followed by validation by deception SMEs. This approach has increased understanding of the deceiver, how context and intent shape the tactics used in deception across communication channels, outlined a range of techniques that can be used in examining information for credibility, and discussed the decision-making processes of the deception target. This approach of examining the entire deception process will prove useful for practitioners in increasing their understanding of deception whilst enabling the development of tailored deception detection strategies to match specific challenges. Empirical and applied validation of the HMD is required before it can be used in applied settings.

One relatively neglected area of understanding regarding deception is the strategies that individuals from other cultures employ in assessing credibility across different communication channels and in contexts with differing levels of interaction (see Taylor et al., 2015 for a recent discussion). An examination of the similarities and differences in such strategies used by different cultures has expanded knowledge of the strategies that individuals believe they use in detecting truth and deception, with one key difference between cultures in willingness to challenge authority. Although these may not be the strategies that individuals actually use when they detect deception, it still expands understanding of how people detect deception across a wider range of strategies than previously thought (Global Deception Research Team, 2006). Furthermore, some of the mentioned strategies are currently being used to detect deception in psychological research highlighting the potential that educating and improving individuals' awareness of these strategies might bring in increasing resilience against deception.

One of the major implications of this thesis has been the need to adjust approaches to deception detection towards understanding and monitoring the risks posed by deceivers rather than seeking to achieve an unattainable 100% accuracy rate in deception-truth discrimination. Through adopting a risk management approach to deception, adversary deception may be identified and monitored across tactical, operational and strategic levels whilst analysts explore how such threats manifest and design appropriate risk mitigation strategies. Theoretical examples of how the DRAT may be deployed to examine future threats affecting UK interests were conducted. An in-depth profile of the adversary was developed from the available information, before a case formulation of the risk they present was conducted before recommendations for risk management were made in further monitoring of adversary behaviour and target inoculation strategies.

A final contribution to research and practice is the development of a future-focussed, proactive approach to deception detection. Recent approaches to deception detection have sought to become proactive through uncovering harmful intentions (Mac Giolla et al., 2015) and more covert attempts at detection (Jundi et al., 2013). Although these approaches have sought to negate threat in the near future, an understanding of how deception may be identified and monitored further into the future requires more innovative thinking. The current proactive approach to deception detection examines potential future threats to the UK through scenario-construction. This enables strategies to be developed to identify, monitor, and respond to a wide-range of deception that may affect the UK in future events. Although the current scenario building has focussed upon non-predictive scenarios to encourage innovative decision-making, future research may easily explore predictive futures and provide strategies to deal with such challenging threats.

The Ethics of Deception in Warfare:

Deception in military environments including warfare is primarily focussed on conducting deception against the adversary to achieve a tactical, operational or strategic objective. Deception has been used throughout history in warfare to achieve such objectives (Whaley, 2007).This contrasts with the majority of research into deception which has sought to identify behavioural cues with which to detect deception. Deception in everyday life is perceived as being immoral and as a

character flaw, whilst in warfare it may be seen as a coveted skill (Glenney, 2009). Whilst conducting deception in warfare will remain a contentious issue there are positive and negative aspects of its use. In warfare deception may actually save lives, both of friendly and adversary forces, as objectives may be obtained without the need for extensive or prolonged conflict. In such circumstances deception may be seen as more ethical, however, one form of deception in warfare that is not considered ethical is perfidy. Perfidy is regarded as unethical as it involves the deception and betrayal of an adversary who has already surrendered and should no longer be regarded as a legitimate target in warfare. Although deception in warfare has been seen as immoral throughout history (Whaley, 2007), if through conducting deception in warfare the number of casualties and fatalities on all sides can be reduced then deception remains a legitimate option.

Limitations:

One limitation arose during the SME validation and refinement of the HMD. This study used an opportunity sampling technique to recruit SMEs in deception and surrounding areas, although 42 SMEs were approached only 19 agreed to participate in the current research. Across the interpersonal and online deception SME samples *theoretical saturation* emerged (Glaser, 1965; Guest, Bunce & Johnson, 2006), however, difficulties were faced in gaining access to SMEs from military and intelligence backgrounds due to the sensitivity of this research and associated security restrictions. It is argued to be intuitively obvious that a larger sample is sensible in uncovering further themes (Fugard & Potts, 2015) and it may be that there are further techniques available to detect deception in military and intelligence environments beyond ACH, which have not been identified and incorporated into the HMD. However, the SME validated HMD still provides a comprehensive examination of deception and its detection, whilst further analytical techniques may be easily adopted as part of the 'toolbox' approach.

In seeking to understand the strategies that individuals from different cultures use to detect deception and truth across different communication channels an opportunity sample was used to recruit participants from Western and Eastern cultural backgrounds living in a city in the East of the UK. This sample comprised of 22 Western participants and 16 Eastern participants which may limit some of the findings

from this study. Although this sample size is representative of qualitative research conducted in others areas (e.g. Merdian, Wilson, Thakker, Curtis & Boer, 2013) and a point of *theoretical saturation* was reached (Glaser, 1965; Guest et al., 2006) these findings may not be found across all individuals from Western and Eastern cultural backgrounds. However, these findings do suggest that individuals may not be as naïve in strategies used to detect deception as previous research (Global Deception Research Team, 2006) examining in-real-life deception has suggested, whilst exploring online deception detection strategies provides researchers with a starting point for the further exploration of such strategies. Future research should seek to examine the prevalence of such strategies across a wider and more culturally varied population sample.

Exploring potential futures is required to develop a more responsive approach to deception detection, however, there are different techniques for constructing scenarios. The current research used a non-actuarial qualitative approach based upon approaches outlined by the '*Intuitive Logics*' methodology. This approach uses qualitative techniques to develop future scenarios narratives rather than predicting the likelihood of a future occurring. This approach may be open to bias in the construction of scenarios, however, to overcome this scenarios were validated across three SMEs to ensure that they matched criteria outlined by Amer et al. (2013) for validating scenarios.

The DARN and DRAT approaches to deception risk assessment are currently in construction phase and have not yet been validated in experimental, real-life case study or applied environments. Theoretical case studies of the DRAT have been conducted in how the DRAT may be applied in the risk assessment of potential future threats to the UK that will involve deception by the adversary (See Chapter 8). It is currently not known how effective the DARN and DRAT will be in identifying and responding deception. However, the techniques recommended for detecting deception are currently being examined in research environments to test their effectiveness and through focussing on case formulation in how the deception forms as a product of behaviour and the environment strategies may be developed to challenge deceivers. Case formulation is an emerging area in risk assessment and researchers and practitioners have only begun to explore how case formulation relates to risk management plans (Logan, 2014), although logically through understanding to a greater extent the circumstances in which risk behaviour occurs will enable a more

effective response in managing such risks. Future research validating the DARN and DRAT is required.

Ways Forward:

Red Teaming

The *in vivo* approach to constructing understanding of psychological phenomena states that only when a model of reality has been developed should it be tested empirically (Boon & Gozna, 2009). The HMD and the DARN and DRAT have been developed from an extensive review of the literature alongside input from deception SMEs from research and practitioner domains. Initial refinement and validation of the HMD has been conducted through the deception SME input, the next stage is to conduct empirical testing of the model. Such testing is argued to lead to either rejection of the model or to conduct an iterative process of refinement (Boon & Gozna, 2009).

Practitioners require deception detection methodologies that have been validated in high-stakes complex environments, however, this is difficult to replicate in artificial experiments (Van Koppen, 2012) posing questions as to how valid recent developments in deception detection approaches (Granhag et al., 2015) actually are. Recent approaches have sought to increase validity through requiring participants to perform complex tasks in environments in which they are familiar, for example, using participants from bio-industry backgrounds in research examining detection of bio-threats (Morgan et al., 2014). In defence environments red teaming is recommended and has been used to challenge emerging concepts, reduce risks and improve problem solving (DCDC, 2013; Heckman et al., 2013). Red teaming will seek to test the deception detection and risk management capabilities of the HMD, DARN and DRAT through the eyes of an adversary seeking to exploit the target. Such an approach meets requirements of ensuring concepts are empirically validated in complex real-world simulations, which further enables the generation of relevant feedback to practitioners aiding the development of intuition and expertise in deception detection (Kahneman & Klein, 2009). Once the models have been subjected and validated through extensive red teaming they will fulfil the criteria outlined by Boon and Gozna (2009) for use by practitioners in applied environments.

Risk Assessment Guidelines and Training

The DARN and DRAT provide practitioners with an evidence-based screening tool and SPJ risk assessment technique for detecting and monitoring adversary tactical, operational and strategic deception across communication channels. By proactively seeking to identify adversary behaviour indicative of deception, strategies that increase resilience against such threats may be deployed. To ensure the reliability of the DARN and DRAT for use by practitioners clear guidelines and training need to be developed. Procedural guidelines should be developed indicating: the circumstances under which the tools will be used to aid decision-making; how the DRAT should be scored to indicate the level of threat posed by the adversary; how case formulations should be constructed; the construction of risk management strategies; and who the appropriate users will be and what training they will require.

Further development of the DARN and DRAT would be to create a computerised version where analysts will be able to input intelligence into the relevant risk factors before conducting risk formulation and management plans. This approach for data entry would enable ease of access for other analysts to the risk assessment and a linear view of the decision-making process in addressing adversary threats. Through further addendums to the DARN and DRAT risk assessment approaches would enable them to be used by analysts monitoring terrorist and OCGs.

Cultural Understanding

In an increasingly globalised world where everyday communication across a range of environments and communication channels may involve actors from multiple cultural backgrounds and different worldviews an advanced understanding of cultural similarities and differences is required. Following the September 11th terrorist attacks this work has turned towards detecting deception in Arabic (Colwell et al., 2013, Morgan et al., 2008) although other research has explored Chinese (Fu et al., 2001; Zhou & Sung, 2008), Korean (Lewis & George, 2008), Vietnamese (Morgan et al., 2010), Spanish (Colwell et al., 2013) and Russian (Hazlett & Morgan, 2009) speakers. Further research is required to explore these and other cultures beliefs regarding deception to a greater depth, particularly where individuals, groups and organisations from other cultures engage with critical UK infrastructure and industry or where they

may pose current or potential future threat related to criminal, terrorist, espionage or military behaviours.

Deception Database

One recommendation that has been drawn from the overall research is the need for real-life case-studies of military deception across tactical, operational and strategic domains. Such a recommendation seems commonsensical, but reflects a previous call by Whaley (2007) for in-depth examination of tactical and strategic level military deception. Developing a database incorporating such known cases of deception will highlight the impact that deception has in operating environments, whilst providing potential to analyse long-term deception patterns and trends and how these reflect the situational context and operating environment (Cali & Romanych, 2005). Such a resource will have the potential to enable practitioners to gain valuable experience and knowledge of deception and the environments in which they may conduct deception or counter-deception operations. Including in-depth information on how such deceptions were conducted or identified will also enable researchers to fully explore the nature of military deception and increase the applied nature of their research, reflecting the scientist-practitioner model (Jones & Mehr, 2007; Shapiro, 2002).

Scenario Development

Alongside the recommendation of developing a deception database reflecting military deception operations, there is a further need for expanding the use of scenario development in addressing future threats and the deception which may be used to increase the effectiveness of such threats. This requires an advanced understanding of adversary target selection, alongside their motives, capabilities, associated decision-making processes and the contexts which will lead to deception.

The current research applied a qualitative scenario construction technique with which to increase creativity in decision-making regarding future events, such an approach can and should be expanded upon to ensure wider knowledge of potential future threats. In-real-time Delphi approaches (Gordon et al., 2015) offer a cost-effective, and relative fast approach to generating scenarios based upon SME knowledge. Future scenario construction should be focussed towards emerging local and global threats that will affect the UK and allies, and towards emerging technologies that may aid the communication of deception. To counter deception

across technologies there is a strong requirement to understand that technology and how deceivers may construct deception within that form of communication.

Conclusion:

In conclusion, this thesis advocates a holistic, risk, and futures based approach to deception detection. Such an approach enables practitioners to develop tailored strategies to identify potential deceivers, select an appropriate strategy to detect deception reflecting the context in which deception occurs, and identify areas where there are potential vulnerabilities to deception. Through focussing on risk management strategies the deceiver's behaviour may be monitored for changes indicative of escalating threat, whilst target vulnerabilities may be reduced ensuring reduced susceptibility to deception. With increasing global uncertainty, anticipation of future deception is required alongside forward-thinking approaches to counter such deception.

References

Aamodt, M. G., & Custer, H. (2006). Who can best catch a liar? A meta-analysis of individual differences in detecting deception. *The Forensic Examiner. 15,* 6-11.

Acosta, D. A. (2008). Hizballah: Deception in the 2006 Summer war. *IO Sphere.* Winter 2008, 15-23.

Adams, S. H., & Harpster, T. (2008). 911 homicide calls and statement analysis. *FBI Law Enforcement Bulletin, 77,* 22-30.

Adams, S. H., & Jarvis, J. P. (2004). Are you telling me the truth? Indicators of veracity in written statements. *FBI Law Enforcement Bulletin, 73,* 7-12.

Akehurst, L., Easton, S., Fuller, E., Drane, G., Kuzmin, K., & Litchfield, S. (2015). An evaluation of a new tool to aid judgements of credibility in the medico-letting setting. *Legal and Criminological Psychology.* doi:10.1111/lcrp.12079.

Akehurst, L., Manton, S., & Quande, S. (2011). Careful calculation or a leap of faith? A field study of the translation of CBCA ratings to final credibility judgements. *Applied Cognitive Psychology, 25,* 236-243.

Al-Simadi, F. A. (2000). Detection of deceptive behaviour: A cross-cultural test. *Social Behavior and Personality, 28,* 455-462.

Amer, M., Daim, T. U., & Jetter, A. (2013). A review of scenario planning. *Futures, 46,* 23-40. doi: 10.1016/j.futures.2012.10.003.

American Psychiatric Association (1994). *Diagnostic and statistical manual of mental health disorders (4th ed).* Washington DC: American Psychiatric Association.

Anderson, D. E., DePaulo, B. M., & Ansfield, M. E. (2002). The development of deception detection skill: A longitudinal study of same-sex friends. *Personality and Social Psychology Bulletin, 28,* 536-545.

Ansarra, R., Colwell, K., Hiscock-Anisman, C., Hines, A., Fleck, R., Cole, L., & Belarde, D. (2011). Augmenting ACID with affective details to assess credibility. *The European Journal of Psychology Applied to Legal Context,* 3, 141-158.

Aven, T., & Renn, O. (2009). The role of quantitative risk assessment for characterizing risk and uncertainty and delineating appropriate risk

management options, with emphasis on terrorism risk. *Risk Analysis, 29,* 587-600. doi: 10.1111/j.1539-6924.2008.01175.x.

Babchishin, K. M., Hanson, R. K., & Helmus, L. (2012). Communication risk for sex offenders: Risk rations for Static-2002R. *Sexual Offender Treatment, 7.* Retrieved from http://www.sexual-offender-treatment.org/111.html.

Baker, A., ten Brinke, L., & Porter, S. (2012). Will get fooled again: Emotionally intelligent people are easily duped by high-stakes deceivers. doi.1111/j.2044-8333.2012.02054.x.

Bakker, E. (2012). Forecasting terrorism: The need for a more systematic approach. *Journal of Strategic Security, 5,* 69-84. doi: 10.5038/1944-0472.5.4.5.

BBC. (2013c). http://www.bbc.co.uk/iplayer/episode/b03kpnjl/Today_09_12_2013/ (From 1:09:42)

BBC. (2014). *Britons Returning from Syria Face Arrest, Says Police Chief.* http://www.bbc.co.uk/news/uk-25893040.

BBC. (2015, January 30). *Three jailed over organised crime offences in Edinburgh.* Retrieved from http://www.bbc.co.uk/news/uk-scotland-edinburgh-east-fife-31064709.

Beardsley, N. L., & Beech, A. R. (2013). Applying the violent extremist risk assessment (VERA) to a sample of terrorist case studies. *Journal of Aggression, Conflict and Peace Research, 5,* 4-15. doi: 10.1108/17596591311290713.

Bell, J. B. (1982). *Cheating: Deception in war & magic, games & sports, sex & religion, business & con games, politics & espionage, art & science.* New York: St Martin's Press.

Bell, J. B. (2003). Toward a theory of deception. *International Journal of Intelligence and Counterintelligence, 16,* 244-279. doi: 10.1080/08850600390198742.

Bennett, M., & Waltz, E. (2007). *Counterdeception Principles and Applications for National Security.* Artech House: London.

Birnholtz, J., Guillory, J., Hancock, J., & Bazarova, N. (2010). *"on my way": Deceptive texting and interpersonal awareness narratives.* Paper presented at CSCS 2010, Savannah, Georgia, USA.

Biros, D. P., Daly, M., & Gunsch, G. (2004). The influence of task load and automation trust on deception detection. *Group Decision and Negotiation, 13,* 173-189.

Biros, D., George, J., & Zmud, R. (2002). Inducing sensitivity to deception in order to improve decision making performance: A field study. *MIS Quarterly, 26,* 119-144.

Blacker, J., Beech, A. R., Wilcox, D. T., & Boer, D. P. (2011). The assessment of dynamic risk and recidivism in a sample of special needs sexual offenders. *Psychology, Crime and Law, 17,* 75-92. doi: 10.1080/10683160903392376.

Blanchard, A. L., Welbourne, J. L., & Boughton, M. D. (2011). A model of online trust. *Information, Communication & Society, 14,* 76-106. doi: 10.1080/13691181003739633.

Bobko, P., Barelka, A. J., & Hirshfield, L. M. (2014). The construct of state-level suspicion: A model and research agenda for automated and information technology (IT) contexts. *Human Factors, 56,* 489-508. doi: 10.1177/0018720813497052.

Bobko, P., Barelka, A. J., Hirshfield, L. M., & Lyons, J. B. (2014). The construct of suspicion and how it can benefit theories and models in organizational science. *Journal of Business Psychology, 29,* 335-342. doi: 10.1007/s10869-014-9360-y.

Boer, D. P., Tough, S., & Haaven, J. (2004). Assessment of risk manageability of intellectually disabled sex offenders. *Journal of Applied Research in Intellectual Disabilities, 17,* 275-283.

Bond, C.F., Jr., & Atoum, A.O. (2000). International deception. *Personality and Social Psychology Bulletin, 26,* 385-395.

Bond, C. F., Jr., & DePaulo, B. M. (2006). Accuracy of deception judgements. *Personality and Social Psychology Review, 10,* 214-234.

Bond, C.F., Jr., & Rao, S.R. (2004). Lies travel: mendacity in a mobile world. In P.A. Granhag & L.A. Strömwall (Eds.). *The detection of deception in forensic contexts.* (pp. 127-147). Cambridge: Cambridge University Press.

Bond, G. D., & Lee, A. Y. (2005). Language of lies in prison: Linguistic classification of prisoners' truthful and deceptive natural language. *Applied Cognitive Psychology, 19*, 313-329.

Bond, G. D., & Speller, L. F. (2009). Gray area messages. In M. S. McGlone & M. L. Knapp (Eds.). *The interplay of truth and deception: New agendas in communication.* (pp. 35-53). London: Routledge.

Boon, J. C. W. (2012). Personal Communication.

Boon, J.C.W., & Gozna, L.F. (2009). Firing pea-shooters at elephants. *Psychologist, 22*, 762-764.

Börjeson, L., Höjer, M., Dreborg, K. H., Ekval, T., & Finnveden, G. (2006). Scenario types and techniques: Towards a user's guide. *Futures, 38,* 723-739. doi: 10.1016/j.futures.2005.12.002.

Bowman, G., MacKay, R. B., Masrani, S., & McKiernan, P. (2013). Storytelling and the scenario process: Understanding success and failure. *Technological Forecasting and Social Change, 80,* 735-748. doi: 10.1016/j.techfore.2012.04.009.

Boyle, R. J., Kacmar, C. J., & George, J. F. (2008). Distributed deception: An investigation of the effectiveness of deceptive communication in a computer-mediated environment. *International Journal of e-Collaboration, 4,* 14-39.

Bradfield, R., Wright, G., Burt, G., Cairns, G., & van der Heijden, K. (2005). The origins and evolution of scenario techniques in long range business planning. *Futures, 47,* 795-812. doi: 10.1016/j.futures.2005.01.003.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3,* 77-101. doi: 10.1191/1478088706qp063oa.

Braun, V., & Clarke, V. (2013). *Successful Qualitative Research.* London: Sage.

Briggs, P., Burford, B., De Angeli, A., & Lynch, P. (2002). Trust in online advice. *Social Science Computer Review, 20,* 321-332. doi: 10.1177/089443930202000309.

Broughton, R. (1990). The prototype concept in personality assessment. *Canadian Psychology, 31,* 26-37.

Brown, G. G., & Cox, L. A., Jr. (2011). How probabilistic risk assessment can mislead terrorism risk analysts. *Risk Analysis, 31,* 196-204. doi: 10.1111/j.1539-6924.2010.01492.x.

Brown, J. (2010). Statement validity analysis. In J. Brown & E. Campbell (Eds.), *The Cambridge Handbook of Forensic Psychology*. Cambridge: Cambridge University Press.

Buchanan, T., & Whitty, M. T. (2013). The online dating romance scam: Causes and consequences of victimhood. *Psychology, Crime & Law.* doi; 10.1080/1068316X.2013.772180.

Buller, D. B, & Burgoon, J. K. (1996). Interpersonal deception theory. *Communication Theory, 6*, 203-242.

Burgoon, J. K., Buller, D. B., & Floyd, K. (2001). Does participation affect deception success? A test of the interactivity principle? *Human Communication Research, 27*, 503-534.

Burgoon, J. K., Buller, D. B., White, C. H., Afifi, W., & Buslig, A. L. S. (1999). The role of conversational involvement in deceptive interpersonal interactions. *Personality and Social Psychology Bulletin, 25*, 669-686.

Burgoon, J.K., Chen, F. & Twitchell, D.P. (2010). Deception and its detection under synchronous and asynchronous computer-mediated communication. *Group Decision and Negotiation, 19*, 345-366.

Burgoon, J.K. & Nunamaker, J.F., Jr. (2010). Toward computer-aided support for the detection of deception – Volume 3. *Group Decision and Negotiation, 19*, 323-325.

Burgoon, J. K., & Qin, T. (2006). The dynamic nature of deceptive verbal communication. *Journal of Language and Social Psychology*, *25*, 76-96.

Burgoon, J. K., Twitchell, D. P., Jensen, M. L., Meservy, T. O., Adkins, M., Kruse, J., Deokar, A. V., Tsechpenakis, G., Lu, S., Metaxas, D. N., Nunamaker, J. F., & Younger, R. E. (2009). Detecting concealment of intent in transportation screening: A proof of concept. *IEEE Transactions on Intelligent Transportation Systems, 10,* 103-112. doi: 10.1109/TITS.2008.2011700.

Burt, G. (2007). Why are we surprised at surprises? Integrating disruption theory and system analysis with the scenario methodology to help identify disruptions and discontinuities. *Technological Forecasting and Social Change, 74,* 731-749. doi: 10.1016/j.techfore.2006.08.010.

Buytendijk, F., Hatch, T., & Micheli, P. (2010). Scenario-based strategy maps. *Business Horizons, 53,* 335-347. doi: 10.1016/j.bushor.2010.02.002.

Cali, C., & Romanych, M. (2005). Counterpropaganda: An important capability for joint forces. *IO Sphere.* (Fall 2005). 11-13.

Campbell, A. (2006). Iran and deception modalities: The reach of *taqiyya, kitman khod'eh* and *taarof*. *National Observer, 70,* 25-48.

Carlson, J.R., & George, J.F. (2004). Media appropriateness in the conduct and discovery of deceptive communication: The relative influence of richness and synchronicity. *Group Decision and Negotiation, 13,* 191-210.

Carlson, J.R. & Zmud, R.W. (1994). Channel expansion theory: A dynamic view of media and information richness perceptions. *Proceedings of the Annual Meeting of the Academy of Management.* 280-284.

Carlson, J.R. & Zmud, R.W. (1999). Channel expansion theory and the experiential nature of media richness perceptions. *Academy of Management Journal, 42,* 153-170.

Caspi, A. & Gorsky, P. (2006). Online deception: Prevalence, motivation, and emotion. *Cyberpsychology and Behavior. 9,* 54-59.

Ceruti, M. G., McGirr, S. C., & Kaina, J. L. (2010). Interaction of language, culture and cognition in group dynamics for understanding the adversary. *Proceedings of the National Symposium on Sensor and Data Fusion (NSSDF).* Las Vegas, USA.

Chen, C. D., & Huang, L. T. (2011). Online deception investigation: Content analysis and cross-cultural comparison. *International Journal of Business and Information, 6,* 91-111.

Cheng, K. H. W., & Broadhurst, R. (2005).The detection of deception: The effects of first and second language on lie detection ability. *Psychiatry, Psychology and Law, 12,* 107-118.

Christie, R., & Geis, F. L. (1970). *Studies in Machiavellianism*. New York: Academic Press.

Cialdini, R. B. (2007). *Influence: The Psychology of Persuasion.* New York: Harper Collins.

Cleckley, H. (1982). *The Mask of Sanity.* New York: Plume.

Clemens, F., Granhag, P. A., & Strömwall, L. A. (2011). Eliciting cues to false intent: A new application of strategic interviewing. *Law and Human Behavior, 35,* 512-522. doi: 10.1007/s10979-010-9258-9.

Coaffee, J., & Fussey, P. (2015). Constructing resilience through security and surveillance: The politics, practices and tensions of security-driven resilience. *Security Dialogue, 46*, 86-105. doi: 10.1177/0967010614557884.

Cohen, K., Johansson, F., Kaati, L., & Mork, J. C. (2014). Detecting linguistic markers for radical violence in social media. *Terrorism and Political Violence, 26,* 245-256. doi: 10.1080/09546553.2014.849948.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44,* 588-608.

Coles, J.P. (2006). Incorporating cultural intelligence into joint doctrine. *IO Sphere.* (Spring 2006), 7-13.

Collins, S. (2002). NATO and Strategic PSYOPS: Policy Pariah or Growth Industry? *Journal of Information Warfare, 1,* 72-78.

Colwell, K. (2007). Assessment criteria indicative of deception (ACID): An integrated system of investigative interviewing and detecting deception. *Journal of Investigative Psychology and Offender Profiling, 4,* 167-180.

Colwell, K., Hiscock-Anisman, C., & Fede, J. (2013). Assessment criteria indicative of deception: An example of the new paradigm of differential recall enhancement. In B. S. Cooper, D. Griesel, & M. Ternes (Eds.). *Applied Issues in Investigative Interviewing, Eyewitness Memory, and Credibility Assessment.* (pp. 259-291). London: Springer

Colwell, K., Hiscock-Anisman, C. K., Memon, A., Taylor, L., & Prewett, J. (2007). Assessment criteria indicative of deception (ACID): An integrated system of investigative interviewing and detecting deception. *Journal of Investigative Psychology and Offender Profiling, 4*, 167-180. doi: 10.1002/jip.73.

Colwell, K., Hiscock, C. K., & Memon, A. (2002). Interviewing techniques and the assessment of statement credibility. *Applied Cognitive Psychology, 16*, 287-300. doi: 10.1002/acp.788.

Colwell, L. H., Miller, H. A., Miller, R. S., & Lyons, P. M., Jr. (2006). US police officer's knowledge regarding behaviors indicative of deception: Implications for eradicating erroneous beliefs through training. *Psychology, Crime & Law, 12*, 489-503.

Cook, A N., Murray, A. A., Amat, G., & Hart, S. D. (2014). Using structured professional judgement guidelines in threat assessment and management:

Presentation, analysis, and formulation of a case of serial intimate partner violence. *Journal of Threat Assessment and Management, 1,* 67-86. doi: 10.1037/tam0000011.

Cooke, D. J., Hart, S. D., Logan, C., & Michie, C. (2012). Explicating the construct of psychopathy: Development and validation of a conceptual model, the comprehensive assessment of psychopathic personality (CAPP). *International Journal of Forensic Mental Health, 11,* 242-252. doi: 10.1080/14999013.2012.746759.

Cornish, P. (2009). *Cyber security and politically, socially and religiously motivated cyber attacks.* Brussels: European Parliament.

Cornish, P., Hughes, R. & Livingstone, D. (2009). *Cyberspace and the national security of the United Kingdom.* London: Chatham House.

Cornish, P., Livingstone, D., Clemente, D. & Yorke, C. (2010). *On cyber warfare.* London: Chatham House.

Dando, C. J., & Bull, R. (2011). Maximising opportunities to detect verbal deception: Training police officers to interview tactically. *Journal of Investigative Psychology and Offender Profiling, 8,* 189-292.

Daniel, D., & Herbig, K. (1982). Propositions on military deception. In D. Daniel & K. Herbig (Eds.). *Strategic Military Deception.* Elmsford: Pergamon Press.

Dauber, C. E. (2009). The truth is out there: Responding to insurgent disinformation and deception operations. *Military Review,* January-February 2009, 13-24.

Davies, J., Black, S., Bentley, N., & Nagi, C. (2013). Forensic case formulation: Theoretical, ethical and practical issues. *Criminal Behavior and Mental Health, 23,* 304-314. doi: 10.1002/cbm.1882.

Davis, M., & Markus, K.A. (2006). Misleading cues, misplaced confidence: An analysis of deception detection patterns. *American Journal of Dance Therapy, 28,* 107-126.

DCDC. (2007). *OPSEC, deception and PSYOPS.* Swindon: DCDC.

DCDC. (2010a). *Global Strategic Trends – Out to 2040.* Swindon: DCDC.

DCDC. (2010b). *Future Character of Conflict.* Swindon: DCDC.

DCDC. (2011). *Understanding and Intelligence Support to Joint Operations.* Swindon: DCDC.

DCDC. (2013). *Red Teaming Guide.* Swindon: DCDC.

DCDC. (2014). *Global Strategic Trends – Out to 2045.* Swindon: DCDC.

DeAnda, L. (2012). What the Western media doesn't say about green on blue attacks in Afghanistan. Retrieved from: http://www.defenceiq.com/army-and-land-forces/articles/green-on-blue-the-nature-of-the-beast-in-afghanist/&mac=DFIQ_OI_Featured_2011&utm_source=defenceiq.com&utm_medium=email&utm_campaign=DFIQOptIn&utm_content=9/4/12?elq=7c5b0a55f3544d16abc720602b870ef5&elqCampaignId=353.

Dearth, D.H. (2000). The human factor in future conflict: Continuity and change. In A.D Campen & D.H Dearth (Eds). *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict.* AFCEA International Press: Fairfax, Virginia.

De Caro, C. (2000). SOFTWAR & Grand Strategy: Liddell-Hart Updated. In A.D Campen & D.H Dearth (Eds). *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict.* AFCEA International Press: Fairfax, Virginia.

De Jouvenel, H. (2000). A brief methodological guide to scenario building. *Technological Forecasting and Social Change, 65,* 37-48.

DePaulo, B. (1992). Nonverbal behavior and self-presentation. *Psychological Bulletin, 111,* 203-243.

DePaulo, B. M., & Kirkendol, S. E. (1988). The motivational impairment effect in the communication of deception. In J. Yuille (Ed.). *Credibility Assessment.* (pp. 50-69). Belgium: Kluwer Academic Publishers.

DePaulo, B. M., Kirkendol, S. E., Tang, J., & O'Brien, T. P. (1988). The motivational impairment effect in the communication of deception: replications and extensions. *Journal of Nonverbal Behavior, 12,* 177–202. doi:10.1007/BF00987487.

DePaulo, B. M., Lindsay, J. J., Malone, B. E., Muhlenbruck, L., Charlton, K., & Cooper, H. (2003). Cues to deception. *Psychological Bulletin, 129,* 74-118.

DePaulo, B. M, & Morris, W. L. (2004). Discerning lies from truth: behavioural cues to deception and the indirect pathway of intuition. In P.A. Granhag & L.A. Strömwall (Eds.). *The detection of deception in forensic contexts.* (pp. 15-40). Cambridge: Cambridge University Press.

De Vogel, V., van den Broek, E., & de Vries Robbé, M. (2014). The use of the HCR-20^{V3} in Dutch forensic psychiatric practice. *International Journal of Forensic Mental Health, 13,* 109-121. doi: 10.1080/14999013.2014.906518.

Douglas, K. S. (2014). Version 3 of the Historical-Clinical-Risk Management-20 (HCR-20^{V3}): Relevance to violence risk assessment and management in forensic conditional release cases. *Behavioral Sciences and the Law, 32,* 557-576. doi: 10.1002/bsl.2134.

Douglas, K. S., Cox, D. N., & Webster, C. D. (1999). Violence risk assessment: Science and practice. *Legal and Criminological Psychology, 4,* 149-184.

Douglas, K. S., & Reeves, K. A. (2010). Historical-Clinical-Risk Management-20 (HCR-20) Violence Risk Assessment Scheme. In R. K. Otto & K. S. Douglas (Eds.). *Handbook of Violence Risk Assessment* (pp. 147-185). London: Routledge.

Douglas, K. S., & Skeem, J. L. (2005). Violence risk assessment: Getting specific about being dynamic. *Psychology, Public Policy and Law, 11,* 347-383. doi: 10.1037/1076-8971.11.3.347.

D'Ovidio, R. (2007). The Evolution of Computers and Crime: Complicating Security Practice. *Security Journal, 20*, 45-49.

Doyle, M., & Dolan, M. (2006). Predicting community violence from patients discharged from mental health services. *British Journal of Psychiatry, 189,* 520-526. doi: 10.1192/bjp.bp.105.021204.

Dunbar, N. E., Jensen, M. L., Burgoon, J. K., Kelley, K. M., Harrison, K. J., Adame, B. J., & Bernard, D. R. (2013). Effects of veracity, modality, and sanctioning on mediated and unmediated interviews. *Communication Research.* doi: 10.1177/0093650213480175.

Durance, P., & Godet, M. (2010). Scenario building: Uses and abuses. *Technological Forecasting and Social Change, 77,* 1488-1492. doi: 10.1016/j.techfore.2010.06.007.

Ecken, P., Gnatzy, T., & van der Gracht, G. (2011). Desirability bias in foresight: Consequences for decision quality based on Delphi results. *Technological*

Forecasting and Social Change, 78, 1654-1670. doi: 10.1016/j.techfore.2011.05.006.

Ekman, P. (2001). *Telling lies: Clues to deceit in the marketplace, politics and marriage.* London: W. W. Norton & Company.

Ekman, P., & O'Sullivan, M. (1991). Who can catch a liar? *American Psychologist, 46,* 913-920.

Elliot, L. (2014, August 31). *Russia and economic warfare: RIP the free market new world order.* Retrieved from www.the guardian.com/business/2014/aug/31/Russia-economic-warfare-rip-free-market-new-world-order.

Elsässer, C., & Stech, F. J. (2006). Detecting Deception. In A. Kott & W. M. McEneaney (Eds.). *Adversarial Reasoning: Computational Approaches to Reading the Opponent's Mind.* London: Chapman & Hall/CRC. (pp. 101-124).

Ericson, R. V. (2006). Ten uncertainties of risk-management approaches to security. *Canadian Journal of Criminology and Criminal Justice, June 2006,* 345-357.

EUROPOL (2013). *EU Serious and Organised Crime Threat Assessment.* Deventer: European Police Office.

Evanoff, C., Porter, S., & Black, P. J. (2014). Video killed the radio star? The influence of presentation modality on detecting high-stakes, emotional lies. *Legal and Criminological Psychology.* doi: 10.1111/lcrp.12064.

Evans, J. R., Houston, K. A., & Meissner, C. A. (2012). A positive, collaborative, and theoretically-based approach to improving deception detection. *Journal of Applied Memory in Research and Cognition.* doi: 10.1016/j.jarmac.2012.02.004.

Evans, J. R., Meissner, C. A., Brandon, S. E., Russano, M. B., & Kleinman, S. M. (2010). Criminal versus HUMINT interrogations: The importance of psychological science to improving interrogative practice. *Journal of Psychiatry & Law, 38,* 215- 249.

Ewens, S., Vrij, A., Jang, M., & Jo, E. (2014). Drop the small talk when establishing baseline behaviour in interviews. *Journal of Investigative Psychology and Offender Profiling.* doi: 10.1002/jip.1414.

Fallon, M. (2014). Collaboration between practice and science will enhance interrogations. *Applied Cognitive Psychology, 28,* 949-950. doi: 10.1002/acp.3091.

Flanagin, A. J., & Metzger, M. J. (2007). The role of site features, user attributes, and information verification behaviors on the perceived credibility of web-based information. *New Media & Society, 9,* 319-342. doi: 10.1177/1461444807075015.

Flavin, W. J. (2013). The dogs that do not bark: Prevention as the path to strategic stability. *Small Wars Journal.* http://smallwarsjournal.com/jrnl/art/the-dogs-that-do-not-bark-prevention-as-the-path-to-strategic-stability.

Fogg, B. J. (2002). *Prominence-Interpretation Theory: Explaining how people assess credibility.* http://credibility.stanford.edu/pit.html.

Fogg, B. J., Soohoo, C., Danielson, D. R., Marable, L., Stanford, J., & Tauber, E. R. (2003). How do users evaluate the credibility of web sites? A study with over 2,500 participants. In *Proceedings of the 2003 conference on designing for user experiences (DUX'03).* http://portal.acm.org/citation.cfm?id=997097&coll=ACM&dl=ACM&CFID=36236037&CFTOKEN=18606069.

Forgas, J. P., & East, R. (2008). On being happy and gullible: Mood effects on scepticism and the detection of deception. *Journal of Experimental Social Psychology, 44,* 1362-1367. doi:10.1016/j.jesp.2008.04.010.

Forster, P. K. (2012). Countering individual jihad: Perspectives on Nidal Hasan and Colleen LaRose. *Counterterrorism Exchange, 2,* 1-11.

Fotr, J., Špaček, M., Souček, I., & Vacík, E. (2015). Scenarios, their concept, elaboration and application. *Baltic Journal of Management, 10,* 73-97. doi: 10.1108/BJM-01-2014-0004.

Fowler, K. A., Lilienfeld, S. O., & Patrick, C. J. (2009). Detecting psychopathy from thin slices of behavior. *Psychological Assessment, 21,* 68-78. doi: 10.1037/a0014938.

Frank, M.G. (2009). Thoughts, feelings, and deception. In B. Harrington (Ed.). *Deception: From ancient empires to internet dating.* (pp. 55-73). Stanford: Stanford University Press.

Fu, G., Lee, K., Cameron, C. A., & Xu, F. (2001). Chinese and Canadian adults' categorization and evaluation of lie- and truth-telling about prosocial and antisocial behaviours. *Journal of Cross-Cultural Psychology, 32,* 720-727. doi: 10.1177/0022022101032006005.

Fugard, A. J. B., & Potts, H. W. W. (2015). Supportive thinking on sample sizes for thematic analyses: a quantitative tool. *International Journal of Social Research Methodology.* doi: 10.1080/13645579.2015.1005453.

Fuller, C. M., Biros, D. P., & Delen, D. (2011). An investigation of data and text mining methods for real world deception detection. *Expert Systems with Applications, 38,* 8392-8398. doi: 10.1016/j.eswa.2011.01.032.

Furner, C. P., & George, J. F. (2012). Cultural determinants of media choice for deception. *Computers in Human Behavior, 28,* 1427-1438. doi: 10.1016/j.chb.2012.03.005.

Fussey, P. (2011). Deterring terrorism? Target-hardening, surveillance and the prevention of terrorism. In A. Silke (Ed.). *The Psychology of Counter-Terrorism.* (pp. 164-185). London: Routledge.

Galanxhi, H., & Nah, F. F-H. (2007). Deception in cyberspace: A comparison of text-only vs. avatar-supported medium. *International Journal of Human-Computer Studies, 65,* 770-783.

Garrick, B. J., Hall, J. E., Kilger, M., McDonald, J. C., O'Toole, T., Probst, P. S., Rindskopf Parker, E., Rosenthal, R., Trivelpiece, A. W., Van Arsdale, L. A., & Zebroski, E. L. (2004). Confronting the risks of terrorism: Making the right decisions. *Reliability Engineering and System Safety, 86,* 129-176. doi: 10.1016/j.ress.2004.04.003.

George, J. F., & Carlson, J. R. (2010). Lying at work: A deceiver's view of media characteristics. *Communications of the Association for Information Systems, 27,* 820-829.

George, J. F., Marett, K., & Tilley, P. (2004). Deception detection under varying electronic media and warning conditions. *Proceedings of the 37th Hawaii International Conference on Systems Science,* 1-9.

George, J. F., Marett, K., & Tilley, P. A. (2008). The effects of warnings, computer-based media, and probing activity on successful lie detection. *IEEE Transactions on Professional Communication, 51,* 1-17.

Gerwehr, S. (2006). Cross-cultural variation in denial and deception. *Defense Intelligence Journal, 15,* 51-78.

Gil-Alana, L., & Barros, C. P. (2010). A note on the effectiveness of national anti-terrorist polices: Evidence from ETA. *Conflict Management and Peace Science, 27,* 28-46. doi: 10.1177/0738894209352130.

Giordano, G., & George, J. F. (2013). The effects of task complexity and group member experience on computer-mediated groups facing deception. *IEEE Transactions on Professional Communication, 56,* 210-225.

Giordano, G., George, J., Marett, K., & Keane, B. (2011). Reviewers and the detection of deceptive information in recorded interviews. *Journal of Applied Social Psychology, 41,* 252-269.

Giordano, G.A., Stoner, J.S., Brouer, R.L. & George, J.F. (2007). The influences of deception and computer-mediated communication on dyadic negotiations. *Journal of Computer-Mediated Communication. 12,* 362-383.

Glaser, B. (1965). The constant comparative method of qualitative analysis. *Social Problems, 12,* 436-446.

Glenney, W., IV. (2009). Military deception in the information age: Scale matters. In B. Harrington (Ed.). *Deception: From ancient empires to internet dating.* (pp. 254-274). Stanford: Stanford University Press.

Global Deception Research Team (2006). A world of lies. *Journal of Cross-Cultural Psychology, 37,* 60-74.

Goble, R., & Bier, V. M. (2013). Risk assessment can be a game-changing information technology – But too often it isn't. *Risk Analysis, 33,* 1942-1951. doi: 10.1111/risa.12055.

Godet, M. (2000). The art of scenarios and strategic planning: Tools and pitfalls. *Technological Forecasting and Social Change, 65,* 3-22.

Godet, M., & Roubelat, F. (1996). Creating the future: The use and misuse of scenarios. *Long Range Planning, 29,* 164-171.

Godson, R., & Wirtz, J. J. (2002). Strategic denial and deception. In R. Godson & J. J. Wirtz (Eds.). *Strategic Denial and Deception: The Twenty-First Century Challenge.* (pp. 1-14). London: Transaction Publishers.

Gordon, T., Sharan, Y., & Florescu, E. (2015). Prospects for lone wolf and SIMAD terrorism. *Technological Forecasting and Social Change*. doi: 10.1016/j.techfore.201.01.013.

Gozna, L. F. (2011, November). *New developments in the CHAMELEON approach to interviewing.* Paper presented at the Investigator Conference, Rothley, UK.

Gozna, L.F., & Boon, J.C.W. (2007, May). *The Chameleon offender: The synergising of psychology and psychiatry to meet the challenge.* Paper presented at the Conference of Research in Forensic Psychiatry, Regensburg, Germany.

Gozna, L. F., & Boon, J. C. W. (2010). Interpersonal deception detection. In J.M. Brown & E.A. Campbell (Eds.). *The Cambridge handbook of forensic psychology*. (pp. 484-491). Cambridge: Cambridge University Press.

Gozna, L. F., & Lawday, R. (2015). *An applied scientist-practitioner model for the assessment of high-stake deceptive future intent in forensic and security settings: Incorporating critical consideration of personality, motive, mindet and risk.* Poster presented at DECEPTICON 2015: International Conference on Deceptive Behavior, University of Cambridge, Cambridge, UK.

Gozna, L. F. & Prendergast, J. (2008). Increasing innovation in applied research: Bridging the investigative/clinical divide. In L. Rayment & L. Falshaw (Eds.) *Issues in Forensic Psychology (No.8)* (pp. 12-22). Leicester: The British Psychological Society.

Gozna, L.F., Vrij, A. & Bull, R. (2001). The impact of individual differences on perceptions of lying in everyday life and in a high stake situation. *Personality and Individual Differences.* 31, 1203-1216.

Granhag, P. A. (2010). On the psycho-legal study of true and false intentions: Dangerous waters and some stepping stones. *The Open Criminology Journal*, *3*, 37-43.

Granhag, P. A., & Hartwig, M. (2015). The strategic use of evidence technique: A conceptual overview. In P. A. Granhag, A. Vrij & B. Verschuere (Eds.). *Detecting Deception: Current Challenges and Cognitive Approaches.* (pp. 231-251). Chichester: Wiley Blackwell.

Granhag, P.A. & Knieps, M. (2011). Episodic future thought: Illuminating the trademarks of forming true and false intentions. *Applied Cognitive Psychology, 25*, 274-280.

Granhag, P.A. & Strömwall, L.A. (2000). Effects of preconceptions on deception detection and new answers to why lie-catchers often fail. *Psychology, Crime and Law*. 6, 197-218.

Granhag, P.A., & Strömwall, L.A. (2002). Repeated interrogations: Verbal and nonverbal cues to deception. *Applied Cognitive Psychology, 16,* 243-257.

Granhag, P.A. & Strömwall, L.A. (2004). Research on deception detection: intersections and future challenges. In P.A. Granhag & L.A. Strömwall (Eds.). *The detection of deception in forensic contexts.* (pp. 317-330). Cambridge: Cambridge University Press.

Granhag, P. A., Strömwall, L. A., & Jonsson, A. C. (2003). Partners in crime: How liars in collusion betray themselves. *Journal of Applied Social Psychology,33*, 848-868.

Granhag, P. A., Strömwall, L. A., Willen, R. M., & Hartwig, M. (2012). Eliciting cues to deception by tactical disclosure of evidence: The first test of the Evidence Framing Matrix. *Legal and Criminological Psychology.* doi: 10.1111/j.2044-8333.2012.02047.x.

Granhag, P.A. & Vrij, A. (2010). Interviewing to detect deception. In P.A. Granhag (Ed.). *Forensic psychology in context: Nordic and international approaches.* Devon: Willan Publishing.

Granhag, P. A., Vrij, A., & Verschuere, B. (2015). *Detecting Deception: Current Challenge and Cognitive Approaches.* Chichester: Wiley Blackwell.

Grann, M., Belfrage, H., & Tengström, A. (2000). Actuarial assessment of risk for violence: Predictive validity of the VRAG and the historical part of the HCR-20. *Criminal Justice and Behavior, 27*, 97-114.

Gray, J. M., & Wilson, M. A. (2009). The relative risk perception of travel hazards. *Environment and Behavior, 41*, 185-204. doi: 10.1177/0013916507311898.

Grazioli, S. (2004). Where did they go wrong? An analysis of the failure of knowledgeable Internet consumers to detect deception over the Internet. *Group Decision and Negotiation, 13,* 149-172.

Grazioli, S., & Jarvenpaa, S. L. (2000). Perils of internet fraud: An empirical investigation of deception and trust with experienced internet consumers. *IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans, 30,* 395-410.

Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough?: An experiment with data saturation and variability. *Field Methods, 18,* 59-82. doi: 10.1177/1525822X05279903.

Guest, G., MacQueen, K. M., & Namey, E. E. (2012). *Applied Thematic Analysis.* Los Angeles: Sage.

Gurney, D., Pine, K., & Wiseman, R. (2013). The gestural misinformation effect: skewing eyewitness testimony through gesture. *American Journal of Psychology, 126,* 301-14.

Hancock, J. T. (2009). Digital deception: The practice of lying in the digital age. In B. Harrington (Ed.). *Deception: From ancient empires to internet dating.* (pp. 109-120). Stanford: Stanford University Press.

Hancock, J. T. (2015). *Technology and lie detection.* Paper presented at DECEPTICON 2015: International Conference on Deceptive Behavior, University of Cambridge, Cambridge, UK.

Hancock, J., Birnholtz, J., Bazarova, N., Guillory, J., Perlin, J., & Barrett, A. (2009). *Butler lies: Awareness, deception and design.* Paper presented at CHI 2009, Boston, MA, USA.

Hancock, J. T., Curry, L., Goorha, S., & Woodworth, M. (2005). *Automated linguistic analysis of deceptive and truthful synchronous computer-mediated communication.* Paper presented at 38th Hawaii International Conference on System Sciences, Hawaii, USA.

Hancock, J.T., Curry, L.E., Goorha, S. & Woodworth, M. (2008). On lying and being lied to: A linguistic analysis of deception in computer-mediated communication. *Discourse Processes, 45,* 1-23.

Hancock, J.T. & Dunham, P.J. (2001). Impression formation in computer-mediated communication revisited: An analysis of the breadth and intensity of impressions. *Communication Research, 28,* 325-347.

Hancock, J.T., Woodworth, M. & Goorha, S. (2010). See no evil: The effect of communication medium and motivation on deception detection. *Group Decision and Negotiation, 19,* 327-343.

Hansen, J. K. (2008). *Military deception and the non-state actor.* Newport: Naval War College.

Hanson, R. K., Babchishin, K. M., Helmus, L., & Thornton, D. (2012). Quantifying the relative risk of sex offenders: Risk ratios for Static-99R. *Sexual Abuse, 25,* 482-515. doi: 10.1177/1079063212469060.

Hanson, R. K., Lunetta, A., Phenix, A., Neeley, J., & Epperson, D. (2014). The field validity of Static-99/R sex offender risk assessment tool in California. *Journal of Threat Assessment and Management, 1,* 102-117. doi: 10.1037/tam0000014.

Hanson, R. K., Sheahan, C. L., & VanZuylen, H. (2013). STATIC-99 and RRASOR predict recidivism among developmentally delayed sexual offenders: A cumulative meta-analysis. *Sexual Offender Treatment, 8,* Retrieved from http://www.sexual-offender-treatment.org/119.html.

Hare, R. D. (1970). *Psychopathy: Theory and research*. New York: John Wiley.

Harpster, T., Adams, S. H., & Jarvis, J. P. (2009). Analyzing 911 homicide calls for indicators of guilt or innocence: An exploratory analysis. *Homicide Studies, 13,* 69, 93. Doi: 10.1177/108876790832807s.

Hart, S. D. (1998). The role of psychopathy in assessing risk for violence: Conceptual and methodological issues. *Legal and Criminological Psychology, 3,* 121-137.

Hart, S. D., & Logan, C. (2011). Formulation of violence risk using evidence-based assessments: The structured professional judgement approach. In P. Sturmey & M. McMurran (Eds.). *Forensic Case Formulation.* Chichester: Wiley-Blackwell.

Hartwig, M., & Bond, C. F., Jr. (2011). Why do lie-catchers fail? A lens model meta-analysis of human lie judgements. *Psychological Bulletin, 137,* 643-659. doi: 10.1037/a0023589.

Hartwig, M., Granhag, P. A., & Strömwall, L. A. (2007). Guilty and innocent suspects' strategies during police interrogations. *Psychology, Crime & Law, 13,* 213-227. doi: 10.1080/10683160600750264.

Hartwig, M., Granhag, P.A., Strömwall, L.A., & Andersson, L.O. (2004). Suspicious minds: Criminal's ability to detect deception. *Psychology, Crime & Law, 10,* 83-95.

Hartwig, M., Granhag, P. A., Strömwall, L. A., & Doering, N. (2010). Impression and information management: On the strategic self-regulation of innocent and guilty suspects. *The Open Criminology Journal, 3,* 10-16.

Hartwig, M., Granhag, P. A., Strömwall, L. A., & Kronkvist, O. (2006). Strategic use of evidence during police interviews: When training to detect deception works. *Law and Human Behavior, 30,* 603-619. doi: 10.1007/s10979-006-9053-9.

Hartwig, M., Granhag, P. A., Strömwall, L. A., & Vrij, A. (2004). Police officers' lie detection accuracy: Interrogating freely vs observing video. *Police Quarterly, 7,* 429-456.

Hartwig, M., Granhag, P. A., Strömwall, L. A., Wolf, A. G., Vrij, A., & Roos af Hjelmsater, E. (2011). Detecting deception in suspects: Verbal cues as a function of interview strategy. *Psychology, Crime & Law, 17,* 643-656. doi: 10.1080/10683160903446982.

Hazlett, G., & Morgan, C. A. (2009). Efficacy of forced-choice testing in detecting deception in Russian. *Journal of Intelligence Community Research and Development.* 1-9.

Heckman, K. E., Walsh, M. J., Stech, F. J., O'Boyle, T. A., DiCato, S. R., & Herber, A. F. (2013). Active cyber defense with denial and deception: A cyber-wargame experiment. *Computers & Security, 37,* 72-77. doi: 10.1016/j/cose.2013.03.015.

Heilbrun, K., O'Neill, M. L., Stevens, T. N., Strohman, L. K., Bowman, Q., & Lo, Y. W. (2004). Assessing normative approaches to communicating violence risk: A national survey of psychologists. *Behavioral Sciences and the Law, 22,* 187-196. doi: 10.1002/bsl.570.

Helman, S. (2007). Detecting deception in individuals: underlying psychological factors, operational implementation, and relevance to strategic deception in the military. QinetiQ/D&TS/CS/CR0614999/1.1

Helmus, L., Babchishin, K. M., & Hanson, R. K. (2013). The predictive accuracy of the Risk Matrix 2000: A meta-analysis. *Sexual Offender Treatment, 8,* Retrieved from http://www.sexual-offender-treatment.org/125.html.

Henderson, S. (2007). Deception – A guide to exploiting the psychological basis of deception in military planning. MIST/06/07/702/21/1.0.

Henderson, S.M. & Lee, J.M. (2008). An assessment of the role of camouflage, concealment and decoys in strategic deception. QINETIQ/EMEA/TS/CR0800307/1.0

Henderson, S.M. & Pascual, R.G. (2008). The psychology of Counter-ISTAR: Concepts and discussion. QINETIQ/EMEA/TS/CR0801237/1.1

Henderson, S.M., Pascual, R.G., Outteridge, C., Cowx, R.W., Helman, S., & Lambillion, S.M. (2007). A Review of Deception in non-military domains: Psychological principles. QINETIQ/D&TS/C&IS/CR0702827/1.1.

Heuer, R. J. (1981). Strategic deception and counterdeception. *International Studies Quarterly, 25,* 294-327.

Heuer, R. J. (1999). *Psychology of Intelligence Analysis.* Washington, DC: U. S. Government Printing Office.

Heuer, R. J. (2005). Limits of intelligence analysis. *Orbis, 49,* 75-94. DOI: 10.1016/j.orbis.2004.10.007.

Hilligoss, B., & Rieh, S. Y. (2008). Developing a unifying framework of credibility assessment: Construct, heuristics, and interaction in context. *Information Processing and Management, 44,* 1467-1484. doi: 10.1016/j.ipm.2007.10.001.

Hines, A., Colwell, K., Hiscock-Anisman, C., Garrett, E., Ansarra, R., & Montalvo, L. (2010). Impression management strategies of deceivers and honest reporters in an investigative interview. *The European Journal of Psychology Applied to Legal Context,* 2, 73-90.

HM Government (2011). *CONTEST: The United Kingdom's Strategy for Countering Terrorism.* London: Home Office.

HM Government. (2013). *Serious and Organised Crime Strategy.* London: Home Office.

Ho, H., Thomson, L., & Darjee, R. (2009). Violence risk assessment: The use of the PCL-SV, HCR-20, and VRAG to predict violence in mentally disordered discharged from a medium secure unit in Scotland. *The Journal of Forensic Psychiatry & Psychology, 20,* 523-541. doi: 10.1080/14789940802638358.

Hofstede, G. (1980). *Culture's consequences: International differences in work-related values.* Beverley Hills, CA: Sage.

Hofstede, G. (1983). Dimensions of national cultures in fifty countries and three regions. In J. Deregowski, S. Dzuirawiec, and R. Annis (Eds.). *Explications in cross-cultural psychology*. Lisse: Swets and Zeitlinger.

Hogart, R. M., & Soyer, E. (2014). Providing information for decision-making: Contrasting description and simulation. *Journal of Applied Research in Memory and Cognition.* doi: 10.1016/j.jarmac.2014.01.005.

Hogg, M. A., & Vaughan, G. M. (2005). *Social Psychology*. Harlow: Pearson Education Limited.

Hooi, R., & Cho, H. (2012). Deception in avatar-mediated virtual environment. *Computers in Human Behavior*. doi: 10.1016/j.chb.2012.09.004.

Hurst, M., & Oswald, M. (2011). Mechanisms underlying response bias in deception detection. *Psychology, Crime & Law*. doi: 10.1080/1068316X.2010.550615

Inayatullah, S. (2008). Six pillars: futures thinking for transforming. *Foresight, 10,* 4-21. doi: 10.1108/1463668081085591.

Jacobson, M. (2010). Terrorist financing and the Internet. *Studies in Conflict & Terrorism. 33,* 353-363.

Jacques, K., & Taylor, P. J. (2008). Male and female suicide bombers: Different sexes, different reasons? *Studies in Conflict & Terrorism, 31,* 304-326. doi: 10.1080/10576100801925695.

Jajko, W. (2002). Deception: An appeal for acceptance; discourse on doctrine; preface to planning. *Comparative Strategy, 21,* 351-363 doi: 10.1080/01495930290043092.

Jenkins, M. C., & Dando, C. J. (2012). Computer-mediated investigative interviews: A potential screening tool for the detection of insider threat. In S. Tomblin, N. MacLeod, R. Sousa-Silva, & M. Coulthard (Eds.). *Proceedings of the 10th Biennial Conference of the International Conference of Forensic Linguistics,* Birmingham: Center for Forensic Linguistics.

Jessee, D. D. (2006). Tactical means, strategic ends: Al Qaeda's use of denial and deception. *Terrorism and Political Violence, 18,* 367-388. doi: 10.1080/09546550600751941.

Johnson, M., & Meyeraan, J. (2003). *Military Deception: Hiding the real – showing the fake,* Unpublished Article, Joint Forces Staff College, USA.

Johnson, M. K., Foley, M. A., Suengas, A. G. & Raye, C. L. (1988). Phenomenal characteristics of memories for perceived and imagined autobiographical events. *Journal of Experimental Psychology: General, 117,* 371-376.

Johnson, P. E., Grazioli, S., Jamal, K., & Berryman, G. (2001). Detecting deception: Adversarial problem solving in a low base rate world. *Cognitive Science, 25,* 355-392.

Johnson, P. E., Grazioli, S., Jamal, K., & Zualkernan, I. A. (1992). Success and failure in expert reasoning. *Journal of Organizational Behavior and Human Decision Processes, 53,* 173-203.

Joinson, A. N., & Dietz-Uhler, B. (2002). Explanations for the perpetration of and reactions to deception in a virtual community. *Computer Social Science Review, 20,* 275-289. doi: 10.1177/089443930202000305.

Jones, J. L., & Mehr, S. L. (2007). Foundations and assumptions of the scientist-practitioner model. *American Behavioral Scientist, 50,* 766-771. doi: 10.1177/0002764206296454.

Jundi, S., Vrij, A., Hope, L., Mann, S., & Hillman, J. (2013). Establishing evidence through undercover and collective intelligence interviewing. *Psychology, Public Policy and Law. 19,* 297-306. doi: 10.1037/a0033571.

Kahneman, D. (2011). *Thinking, fast and slow*. London: Penguin.

Kahneman, D., & Klein, G. (2009). Conditions for intuitive expertise: A failure to disagree. *American Psychologist, 64,* 515-526. doi: 10.1037/a0016755.

Kaina, J., Ceruti, M. G., Liu, K., McGirr, S. C., & Law, J. B. (2011, June). *Deception detection in multicultural coalitions: Foundations for a cognitive model.* Paper presented at the 16th International Command and Control Research and Technology Symposium (ICCTRS), Quebec, Canada.

Kashy, D. A., & DePaulo, B. M. (1996). Who lies? *Journal of Personality and Social Psychology, 70*, 1037-1051.

Kaufmann, G., Drevland, G. C. B., Wessel, E., Overskeid, G., & Magnussen, S. (2003). The importance of being earnest: Displayed emotions and witness credibility. *Applied Cognitive Psychology, 17*, 21-34. doi: 10.1002/acp.842.

Kebbell, M. R., & Porter, L. (2012). An intelligence assessment framework for identifying individuals at risk of committing acts of violent extremism against the West. *Security Journal, 25,* 212-228. doi: 10.1057sj.2011.19.

Kim, R. K., & Levine, T. R. (2011). The effect of suspicion on deception detection accuracy: Optimal level or opposing effects? *Communication Reports, 24*, 51-62. doi: 10.1080/08934215.2011.615272.

Klare (2014, July 15). *Twenty-first century energy wars: how oil and gas are fuelling global conflicts.* Retrieved from http://www.energypost.eu/twenty-first-century-energy-wars-oil-gas-fuelling-global-conflicts/.

Koblentz, G. D. (2011). Predicting peril or the peril of prediction? Assessing the risk of CBRN terrorism. *Terrorism and Political Violence, 23,* 501-520. doi: 10.1080/09546553.2011.575487.

Köhnken, G. (2004). Statement Validity Analysis and the 'detection of the truth'. In P.A. Granhag & L.A. Strömwall (Eds.). *The detection of deception in forensic contexts.* (pp. 41-63). Cambridge: Cambridge University Press.

Kreis, M. F. K., Cooke, D. J., Michie, C., Hoff, H. A., & Logan, C. (2012). The comprehensive assessment of psychopathic personality (CAPP): Content validation using prototypical analysis. *Journal of Personality Disorders, 26,* 402-413.

Kropp, P. R., Hart, S. D., Lyon, D. R., & Storey, J. E. (2011). The development and validation of the guidelines for stalking assessment and management. *Behavioral Science and the Law, 29,* 302-316. doi: 10.1002/bsl.978.

Kuhn, G., Caffaratti, H. O., Teszka, R., & Rensink R. A. (2014). A psychologically-based taxonomy of misdirection. *Frontiers in Psychology, 5,* 1-14. doi: 10.3389/fpsyg.2014.01292.

Kuhn, G., & Martinez, L. M. (2012). Misdirection – past, present, and the future. *Frontiers in Human Neuroscience, 5,* 1-7. doi: 10.3389/fnhum.00172.

Lakhani, M., & Taylor, R. (2003). Beliefs about the cues to deception in high- and low-stake situations. *Psychology, Crime & Law, 9,* 357-368. doi: 10.1080/1068316031000093441.

Larson, R., Jones, H., Rashid, A., & Baron, A. (2015). *Detecting sophisticated social engineering attacks through linguistic indicators of deception.* Poster presented at DECEPTICON 2015: International Conference on Deceptive Behavior, University of Cambridge, Cambridge, UK.

Latimer, J. (2001). *Deception in warfare.* Woodstock, NY: Overlook Press.

Leal, S., Vrij, A., & Mann, S. (2015). *Please be honest and provide details I can check: Deterrents of deception in an online insurance fraud context.* Paper presented at DECEPTICON 2015: International Conference on Deceptive Behavior, University of Cambridge, Cambridge, UK.

Leal, S., Vrij, A., Mann, S., & Fisher, R. P. (2010). Detecting true and false opinions: The Devil's Advocate approach as a lie detection aid. *Acta Psychologia, 134,* 323-329. doi: 10.1016/j.actpsy.2010.03.005.

Leins, D. A., Fisher, R. P., & Ross, S. J. (2012). Exploring liars' strategies for creating deceptive reports. *Legal and Criminological Psychology.* doi: 10.1111/j.2044-8333.2011.02041.x

Leins, D., Fisher, R. P., & Vrij, A. (2012). Drawing on liar's lack of cognitive flexibility: Detecting deception through varying report modes. *Applied Cognitive Psychology,* doi: 10.1002/acp.2837.

Leins, D., Fisher, R. P., Vrij, A., Leal, S., & Mann, S. (2011). Using sketch drawing to induce inconsistency in liars. *Legal and Criminological Psychology, 16,* 253-265. doi: 10.1348/135532510X501775.

LeMire, G. A. (2002). *Employing special operations forces to conduct deception in support of shaping and decisive operations.* Fort Leavenworth: School of Advanced Military Studies.

Levine, T. R. (2014). Truth-default theory (TDT): A theory of human deception and deception detection. *Journal of Language and Social Psychology, 33,* 378-392. doi: 10.1177/0261927X14535916.

Levine, T. R., Shaw, A., & Shulman, H. C. (2010). Increasing deception detection accuracy with strategic questioning. *Human Communication Research, 36,* 216-231. doi: 10.1111/j.1468-2958.2010.01374.x.

Lewis, C. C., & George, J. F. (2008). Cross-cultural deception in social networking sites and face-to-face communication. *Computers in Human Behavior, 24,* 2945-2964. doi: 10.1016/j.chb.2008.05.002.

Logan, C. (2014). The HCR-20 Version 3: A case study in risk formulation. *International Journal of Forensic Mental Health, 13,* 172-180. doi: 10.1080/14999013.2014.906516.

Lu, H.Y. (2008). Sensation-seeking, internet dependency, and online interpersonal deception. *CyberPsychology & Behavior, 11,* 227-231.

Mac Giolla, E., Granhag, P. A., & Liu-Jönsson, M. (2013). Markers of good planning behavior as a cue for separating true and false intent. *PsyCh Journal.* doi: 10.1002/pchj.36.

Mac Giolla, E., Granhag, P. A., & Vrij, A. (2015). Discriminating between true and false intentions. In P. A. Granhag, A. Vrij & B. Verschuere (Eds.). *Detecting Deception: Current Challenges and Cognitive Approaches.* (pp. 155-173). Chichester: Wiley Blackwell.

Macdonald, S. (2007). *Propaganda and Information Warfare in the Twenty-First Century: Altered Images and Deception Operations.* London: Routledge.

Mackay, A., & Tatham, S. (2011). *Behavioural Conflict: Why Understanding People and Their Motivations Will Prove Decisive in Future Conflict.* Saffron Walden: Military Studies Press.

Magnussen, S., & Wessel, E. (2010). Displayed emotions in court: Effects on credibility judgements. In P. A. Granhag (Ed.). *Forensic Psychology in Context: Nordic and International Approaches.* (pp. 247-263). Cullompton: Willon.

Mante-Meijer, E., van der Duin, P., & Abeln, M. (1998). Fun with scenarios. *Long Range Planning, 31,* 628-637.

Martin, C.L. (2008). *Military deception reconsidered.* Unpublished MSc Thesis. Naval Postgraduate School, Monterey, California.

Masip, J., Garrido, E., & Herrero, C. (2004). Facial appearance and impressions of credibility: The effects of facial babyishness and age on person perception. *International Journal of Psychology,* 39, 276-289. doi: 10.1080/00207590444000014.

Masip, J., Sporer, S. L., Garrido, E., & Herrero, C. (2005). The detection of deception with the reality monitoring approach: A review of the empirical evidence. *Psychology, Crime & Law, 11,* 99-122. doi: 10.1080/10683160410001726356.

McDermott, B., Dualan, I., & Scott, C. (2011). The predictive ability of the Classification of Violence Risk (COVR) in a forensic psychiatric hospital. *Psychiatric Services, 62,* 430-433. doi: 10.1176/appi.ps.62.4.430.

McFarlane, P., & Hills, M. (2013). Developing immunity to flight security risk: Prospective benefits from considering aviation security as a socio-technical

eco-system. *Journal of Transportation Security, 6,* 221-234. doi: 10.1007/s12198-013-0113-3.

McFarlane, P., & Hills, M. (2014). Towards a higher plane of air transportation security: From hubris to knowledge. *Journal of Transportation Security, 7,* 115-121. doi: 10.1007/s12198-013-0133-2.

McGuffog, A., Green, J., & Crombie, N. (2004). *Micro-facial expression technique – Results of evaluation trial.* QINETIQ/KI/CHSCR042212.

McLeod, B. A., & Genereux, R. L. (2008). Predicting the acceptability and likelihood of lying: The interaction of personality with type of lie. *Personality and Individual Differences, 45,* 591-596. doi: 10.1016/j.paid.2008.06.015.

McPherson, D. E. (2010). *Deception recognition: Rethinking the operational commander's approach,* Unpublished Thesis, Naval War College, Newport, USA.

Melloy, J. R., Hoffmann, J., Guldimann, A., & James, D. (2012). The role of warning behaviors in threat assessment: An exploration and suggested typology. *Behavioral Sciences and the Law, 30,* 256-279. doi: 10.1002/bsl.999.

Meloy, J. R., Hoffmann, J., Roshdi, K., & Guldimann, A. (2014). Some warning behaviors discriminate between school shooters and other students of concern. *Journal of Threat Assessment and Management, 1,* 203-211. doi: 10.1037/tam0000020.

Memon, A., Fraser, J., Colwell, K., Odinot, G., & Mastroberardino, S. (2010). Distinguishing truthful from invented accounts using reality monitoring criteria. *Legal and Criminological Psychology, 15,* 177-194. doi: 10.1348/135532508X401382.

Merdian, H. L., Wilson, N., Thakker, J., Curtis, C., & Boer, D. P. (2013). "So why did you do it?": Explanations provided by child pornography offenders. *Sexual Offender Treatment, 8,* 1-19.

Metzger, M. J., & Flanagin, A. J. (2013). Credibility and trust of information in online environments: The use of cognitive heuristics. *Journal of Pragmatics, 59,* 210-220. doi: 10.1016/j.pragma.2013.07.012.

Metzger, M. J., Flanagin, A. J., & Medders, R. B. (2010). Social and heuristic approaches to credibility evaluation online. *Journal of Communication, 60,* 413-439. doi: 10.1111/j.1460-2466.2010.01488.x.

Miller, K. D., & Waller, H. G. (2003). Scenarios, real options and integrated risk management. *Long Range Planning, 36,* 93-107. doi: 10.1016/S0024-6301(02)00205-4.

Mocanu, D., Rossi, L., Zhang, Q., Karsai, M., & Quattrociocchi, W. (2015). Collective attention in the age of (mis)information. *Computers in Human Behavior.* doi: 10.1016/j.chb.2015.01.024.

Modic, D., & Anderson, R. (2014). Reading this may harm your computer: The psychology of malware warnings. *Computers in Human Behavior, 41,* 71-79. doi: 10.1016/j.chb.2014.09.014.

Monahan, J. (2012). The individual risk assessment of terrorism. *Psychology, Public Policy, and Law, 18,* 167-205. doi: 10.1037/a0025792.

Monahan, J., & Steadman, H. J. (1996). Violent storms and violent people: How meteorology can inform risk communication in mental health law. *American Psychologist, 51,* 931-938.

Morgan, C. A., Colwell, K., & Hazlett, G. A. (2011). Efficacy of forensic statement analysis in distinguishing truthful from deceptive eyewitness accounts of highly stressful events. *Journal of Forensic Science, 56,* 1227-1234. doi: 10.1111/j.1556-4029.2011.01896.x.

Morgan, C. A., Mishara, A., Christian, J., & Hazlett, G. A. (2008). Detecting deception through automated analysis of translated speech: Credibility assessments of Arabic-speaking interviewees. *Journal of Intelligence Community Research and Development, 8,* 1-22.

Morgan, C. A., Rabinowitz, Y. G., Hilts, D., Weller, C. E. & Coric, V. (2013). Efficacy of modified cognitive interviewing, compared to human judgements in detecting deception related to bio-threat activities. *Journal of Strategic Security, 6,* 100-119.

Morgan, C. A., Rabinowitz, W. Kallivrousis, G., & Hazlett, G. (2010). Efficacy of automated forced-choice testing dilemmas in detecting deception in Vietnamese. *Journal of Intelligence Community Research and Development, 6,* 1-11.

Morgan, C. A., Rabinowitz, Y., Leidy, R., & Coric, V. (2014). Efficacy of combining interview techniques in detecting deception related to bio-threat issues. *Behavioral Sciences and the Law, 32,* 269-285. doi: 10.1002/bsl.2098.

Nacos, B.L. (2007). Al-Qaeda's propaganda advantage and how to counter it. *Perspectives on Terrorism. 1,* 3-6.

Nahari, G., Vrij, A., & Fisher, R. P. (2012). Exploiting liars' verbal strategies by examining the verifiability of details. *Legal and Criminological Psychology.* doi: 10.1111/j.2044-8333.2012.02069.x.

Nahari, G., Vrij, A., & Fisher, R. P. (2013). The verifiability approach: Countermeasures facilitate its ability to discriminate between truths and lies. *Applied Cognitive Psychology.* doi: 10.1002/acp.2974.

Navarro, J. (2003). A four-domain model of detecting deception. *FBI Law Enforcement Bulletin* (June), 19-24.

Navarro, J. (2011b). *How to Spot a Borderline Personality.* USA: Smashwords.

Navarro, J. (2011c). *How to Spot a Histrionic Personality.* USA: Smashwords.

Newman, M. L., Pennebaker, J. W., Berry, D. S., & Richards, J. M. (2003). Lying words: Predicting deception from linguistic styles. *Personality and Social Psychology Bulletin, 29,* 665-675. doi: 10.1177/0146167203251529.

Nguyen, X. T. (2002). Threat Assessment in Tactical Airborne Environments. *Proceedings of the Sixth International Conference on Information Fusion, 2,* 1102-1109.

Nisbett, R. E., Peng, K., Choi, I., & Norenzayan, A. (2001). Culture and systems of thought: Holistic versus analytic cognition. *Psychological Review, 108,* 291-310. doi: 10.1037//0033-295X.108.2.291.

Norenzayan, A., & Nisbett, R. E., (2000). Culture and casual cognition. *Current Directions in Psychological Science, 9,* 132-132.

Nunamaker, J., Golob, A., Elkins, A., Burgoon, J., & Derrick, D. (2015). *From lab to field: The evolution of the AVATAR for credibility assessment.* Paper presented at DECEPTICON 2015: International Conference on Deceptive Behavior, University of Cambridge, Cambridge, UK.

O'Brien, F., & Meadows, M. (2013). Scenario orientation and use to support strategy development. *Technological Forecasting and Social Change, 80,* 643-656. doi: 10.1016/j.techfore.2012.06.006.

O'Sullivan, M. (2003). The fundamental attribution error in detecting deception: The boy who cried wolf effect. *Personality and Social Psychology Bulletin*, 29, 1316-1327. doi: 10.1177/0146167203254610.

O'Sullivan, M. & Ekman, P. (2004). The wizards of deception detection. In P.A. Granhag & L.A. Strömwall (Eds.). *The detection of deception in forensic contexts.* (pp. 269-286). Cambridge: Cambridge University Press.

Ott, M., Cardie, C., & Hancock, J. (2012). *Estimating the prevalence of deception in online review communities*. Paper presented at WWW 2012, April 16–20, 2012, Lyon, France.

Ott, M., Choi, Y., Cardie, C., & Hancock, J. (2011). Finding deceptive opinion spam by any stretch of the imagination. *Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics,* 309-319.

Palasinski, M., & Svoboda, S. (2014). Reducing the risk of insurance fraud by appearances of online surveillance. *Psychology, Crime & Law*. doi: 10.1080/1068316X.2013.871012.

Park, H. S., Levine, T. R., McCornack, S. A., Morrison, K., & Ferrara, M. (2002). How people really detect lies. *Communication Monographs, 69,* 144-157.

Paulhus, D. L. (2013). Personal communication.

Paulhus, D. L., & Williams, K. M. (2002). The Dark Triad of personality: Narcissism, Machiavellianism and psychopathy. *Journal of Research in Personality, 36,* 556-563.

Pennebaker, J. W., Booth, R. J., & Francis, M. E. (2007). Linguistic Inquiry and Word Count: LIWC [Computer software]. Austin, TX: LIWC.net.

Piegorsch, W. W., Cutter, S. L., & Hardisty, F. (2007). Benchmark analysis for quantifying urban vulnerability to terrorist incidents. *Risk Analysis, 27,* 1411-1425. doi: 10.1111/j.1539-6924.2007.00977.x.

Pope, S., Jøsang, A. & McAnally, D. (2006). Formal Methods of Countering Deception and Misperception in Intelligence Analysis. *Proceedings of the 11th International Command and Control Research Technology Symposium (ICCRTS'06)*, Cambridge, UK, 2006. Available at http://persons.unik.no/josang/papers/PJM2006-ICCRTS.pdf Accessed 31/08/2010.

Porter, S., Campbell, M. A., Stapleton, J., & Birt, A. R. (2002). The influence of judge, target, and stimulus characteristics on the accuracy of detecting deceit. *Canadian Journal of Behavioural Science, 34*, 172-185.

Porter, S., England, L., Juodis, M., ten Brinke, L., & Wilson, K. (2008). Is the face a window to the soul? Investigation of the accuracy of intuitive judgements of the trustworthiness of human faces. *Canadian Journal of Behavioural Science, 40*, 171-177. doi: 10.1037/0008-400X.40.3.171.

Porter, S., Korva, N., & Baker, A. (2011). Secrets of the human face: New insights into the face and cover emotions. *Psychology Aotearoa.*

Porter, S., McCabe, S., Woodworth, M., & Peace, K. A. (2007). 'Genius is 1% inspiration and 99% perspiration'… or is it? An investigation of the impact of motivation and feedback on deception detection. *Legal and Criminological Psychology, 12*, 297-309. doi: 10.1348/135532506X143958.

Porter, S., & ten Brinke, L. (2008b). Reading between the lies: Identifying concealed and falsified emotions in universal facial expressions. *Psychological Science, 19*, 508-514.

Porter, S., & ten Brinke, L. (2009). Dangerous decisions: A theoretical framework for understanding how judges assess credibility in the courtroom. *Legal and Criminological Psychology, 14*, 119-134. doi: 10.1348/135532508X281520.

Porter, S., & ten Brinke, L. (2010). The truth about lies: What works in detecting high-stakes deception? *Legal and Criminological Psychology, 15*, 57-75. doi: 10.1348/135532509X433151.

Porter, S., ten Brinke, L., Baker., & Wallace, B. (2011). Would I lie to you? "leakage" in deceptive facial expressions relates to psychopathy and emotional intelligence. *Personality and Individual Differences.* doi: 10.1016/j.paid.2011.03.031.

Porter, S., ten Brinke, L., & Wallace, B. (2012). Secrets and lies: Involuntary leakage in deceptive facial expressions as a function of emotional intensity. *Journal of Nonverbal Behavior, 36*, 23-37. doi. 10.1007/s10919-011-0120-7.

Porter, S., Woodworth, M., & Birt, A. R. (2000). Truth, lies and videotape: An investigation of the ability of federal parole officers to detect deception. *Law and Human Behavior, 24*, 643-658.

Paulhus, D. L., & Williams, K. M. (2002). The dark triad of personality: Narcissism, Machiavellianism, and psychopathy. *Journal of Research in Personality, 36,* 556-563.

Ramírez, R., & Ravetz, J. (2011). Feral futures: Zen and aesthetics. *Futures, 43,* 478-487. doi: 10.1016/j.futures.2010.12.005.

Ramírez, R., & Selin, C. (2014). Plausibility and probability in scenario planning. *Foresight, 16,* 54-74. doi: 10.1108/FS-08-2012-0061.

Ramsay, G. (2008). Conceptualising online terrorism. *Perspectives on Terrorism. 2,* 3-10.

Raskin, R., & Hall, C. S. (1979). A Narcissistic Personality Inventory. *Psychological Reports, 45,* 590.

Rassin, E. (2000). Criteria based content analysis: The less scientific road to truth. *Expert Evidence, 7,* 265-278.

Reid, I. D., Gozna, L. F., & Boon, J. C. W. (2012). *Towards a holistic model of deception: The challenge of the cyber CHAMELEON.* Poster presented at the 2nd MilDec Symposium, Defence Academy of the United Kingdom, Shrivenham, UK, 7-8 November.

Reynolds, L., Smith, M. E., Birnholtz, J., & Hancock, J. (2013). *Butler lies from both sides: Actions and perceptions of unavailability management in texting.* Paper presented at CSCW'13, San Antonio, Texas, USA.

Roberts, K., & Horgan, J. (2008). Risk assessment and the terrorist. *Perspectives on Terrorism, 2,* 3-9.

Rockmann, K. W., & Northcraft, G. B. (2008). To be or not to be trusted: The influence of media richness on defection and deception. *Organizational Behavior and Human Decision Processes, 107,* 106-122. doi:10.1016/j.obhdp.2008.02.002.

Roets, A., & Van Hiel, A. (2011). An integrative process approach on judgement and decision making: The impact of arousal, affect, motivation, and cognitive ability. *The Psychological Record, 61,* 497-520.

Sandham, A., Ormerod, T., Dando, C., Bull, R., Jackson, M., & Goulding, J. (2011). *Scent trails: Countering terrorism through informed surveillance.* Paper presented at Engineering Psychology and Cognitive Ergonomics – 9th International Conference, Orlando, Florida, USA.

Santos, E., Nguyen, H., Yu, F., Kim, K., Li, D., Wilkinson, J. T., Olson, A., & Jacob, R. (2008). *Intent-driven insider threat detection in intelligence analysis.* Proceedings of the 2008 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology, Sydney, Australia.

Scurich, N., & John, R. S. (2012). Prescriptive approaches to communicating the risk of violence in actuarial risk assessment. *Psychology, Public Police and Law, 18,* 50-78. doi: 10.1037/a0024592.

Sebanz, N., & Shiffrar, M. (2009). Detecting deception in a bluffing body: The role of expertise. *Psychonomic Bulletin & Review, 16*, 170-175. doi: 10.3758/PBR.16.1.170.

Sellers, B. E. (2009). *Case study: Operation Mincemeat,* Unpublished Thesis, Air Command and Staff College Air University, Alabama, USA

Shapiro, D. (2002). Renewing the scientist-practitioner model. *The Psychologist, 15,* 232-234.

Singh, J. P., Grann, M., & Fazel, S. (2011). A comparative study of violence risk assessment tools: A systematic review and metaregression analysis of 68 studies involving 25,980 participants. *Clinical Psychology Review*. doi: 10.1016/j.cpr.2010.11.009.

Skeem, J. L., & Monahan, J. (2011). Current directions in violence risk assessment. *Current Directions in Psychological Science, 20,* 38-42. doi: 10.1177/0963721410397271.

Smith, C. A. P., Johnston, J., & Paris, C. (2004). Decision support for air warfare: Detection of deceptive threats. *Group Decision and Negotiation, 13*, 129-148.

Smith, M. E., Hancock, J. T., Reynolds, L., & Birnholtz, J. (2014). Everyday deception or a few prolific liars? The prevalence of lies in text messaging. *Computers in Human Behavior, 41*, 220-227. doi: 10.1016/j.chb.2014.05.032.

Spencer, E. & Balasevicius, T. (2009). Crucible of success: Cultural intelligence and the modern battlespace. *Canadian Military Journal, 9*, 40-48.

Sporer, S. L. (2004). Reality monitoring and detection of deception. In P.A. Granhag & L.A. Strömwall (Eds.). *The detection of deception in forensic contexts.* (pp. 64-102). Cambridge: Cambridge University Press.

Stajano, F., & Wilson, P. (2015). *Understanding scam victims: Seven principles for systems security.* Poster presented at DECEPTICON 2015: International

Conference on Deceptive Behavior, University of Cambridge, Cambridge, UK.

Stech, F. J., & Elsässer, C. (2003). *Deception detection by analysis of competing hypotheses.* Mclean, Viginia: The MITRE Corporation.

Stech, F. J., & Elsässer, C. (2004). *Midway revisited: Detecting deception by analysis of competing hypothesis.* Mclean, Virginia: The MITRE Corporation.

Stein, G.J. (2000). Sun Tzu Conducts Information Warfare. In A.D Campen & D.H Dearth (Eds). *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict.* AFCEA International Press: Fairfax, Virginia.

Stempel, J. D. (2013). Religion and intelligence. *International Journal of Intelligence and Counterintelligence, 26,* 375-388. doi: 10.1080/08850607.2013.732451.

Strandberg, V. (2013). Rail bound traffic – A prime target for contemporary terrorist attacks? *Journal of Transport Security, 6,* 271-286. doi: 10.1007/s12198-013-0116-0.

Strömwall, L. A. (2010). Assessing reliability by analysing the verbal content: the case of Sweden. In P. A. Granhag (Ed.). *Forensic psychology in context: Nordic and international approaches.* (pp. 264-280). Cullompton: Willan Publishing.

Strömwall, L. A., & Granhag, P. A. (2003). How to detect deception? Arresting the beliefs of police officers, prosecutors and judges. *Psychology, Crime & Law, 9,* 19-36. doi: 10.1080/1068316021000057659.

Strömwall, L. A., Granhag, P. A., & Hartwig, M. (2004). Practitioners' beliefs about deception. In P. A. Granhag, & L. A. Strömwall (Eds.). *The detection of deception in forensic contexts.* (pp. 229-250). New York: Cambridge University Press.

Strömwall, L. A., Hartwig, M., & Granhag, P. A. (2006). To act truthfully: Nonverbal behaviour and strategies during a police interrogation. *Psychology, Crime & Law, 12*, 207-219. doi: 10.1080/10683160512331331328.

Strömwall, L. A., & Willén, R. M. (2011). Inside criminal minds: Offenders' strategies when lying. *Journal of Investigative Psychology and Offender Profiling, 8,* 271-281. doi: 10.1002/jip.148.

Suckle-Nelson, J. A., Colwell, K., Hiscock-Anisman, C., Florence, S., Youschak, K. E., & Duarte, A. (2010). Assessment criteria indicative of deception (ACID): Replication and gender differences. *The Open Criminology Journal, 3*, 23-30.

Tan, K. L. E. (2003). *Confronting Cyberterrorism with Cyber deception.* Unpublished MSc Thesis. Naval Postgraduate School, Monterey, California.

Taylor, P. J., Dando, C. J., Ormerod, T. C., Ball, L. J., Jenkins, M. C., Sandham, A., & Menacere, T. (2013). Detecting insider threats through language change. *Law and Human Behavior, 37,* 267-275. doi: 10.1037/lhb0000032.

Taylor, P. J., Jacques, K., Giebels, E., Levine, M., Best, R., Winter, J., & Rossi, G. (2008). Analysing forensic processes: Taking time into account. *Issues in Forensic Psychology, 8,* 45-57.

Taylor, P. J., Larner, S., Conchie, S. M., & van der Zee, S. (2015). Cross-cultural deception detection. In P. A. Granhag, A. Vrij & B. Verschuere (Eds.). *Detecting Deception: Current Challenges and Cognitive Approaches.* (pp. 175-201). Chichester: Wiley Blackwell.

Taylor, R., & Gozna, L. F. (2011). *Deception: A Young Person's Life Skill?* Hove: Psychology Press.

Taylor, R., & Hick, R. F. (2007). Believed cues to deception: Judgements in self-generated trivial and serious situations. *Legal and Criminological Psychology, 12,* 321-331. doi: 10.1324/135532506X116101.

Ten Brinke, L., MacDonald, S., Porter, S., & O'Connor, B. (2011). Crocodile tears: Facial, verbal and body language behaviours associated with genuine and fabricated remorse. *Law and Human Behavior*. doi: 10.1007/s10979-011-9265-5.

Ten Brinke, L., & Porter, S. (2011b, in press). Friend or foe? The role of intuition in interpersonal trustworthiness and vulnerability assessments.

Ten Brinke, L., & Porter, S. (2012). Cry me a river: Identifying the behavioral consequences of extremely high-stakes interpersonal deception. *Law and Human Behavior, 36,* 469-477. doi: 10.1037/h0093929.

Ten Brinke, L., Porter, S., & Baker, A. (2011, in press). Darwin the detective: Observable facial muscle contractions reveal emotional high-stakes lies. *Evolution and Human Behavior.* doi:10.1016/j.evolhumbehav.2011.12.003.

Ten Brinke, L., Stimson, D., & Carney, D. R. (2014). Some evidence for unconscious lie detection. *Psychological Science.* doi: 10.1177/0956797614524421.

Thomas, T.L. (2003). Al Qaeda and the Internet: The danger of "cyberplanning". *Parameters. 33,* 112-123.

Thomas, T.L. (2006). Cyber mobilization: A growing counterinsurgency campaign. *IO Sphere.* (Summer 2006), 23-28.

Thomas, T.L. (2008). Cyberskepticism: The mind's firewall. *IO Sphere.* (Spring 2008), 4-8.

Thomas, T.L. (2009). Countering internet extremism. *IO Sphere.* (Winter 2009), 14-19.

Thompson, P. (2009). Cognitive hacking: Detecting deception on the web. In B. Harrington (Ed.). *Deception: From ancient empires to internet dating.* (pp. 121-134). Stanford: Stanford University Press.

Thornton, D., Mann, R., Webster, S., Blud, L., Travers, R., Friendship, C., & Erikson, M. (2003). Distinguishing and combining risks for sexual and violent recidivism. In R. A. Prentky, E. S. Janus, & M. C. Seto (Eds.), *Annals of the New York Academy of Sciences: Vol. 989. Sexually coercive behavior: Understanding and management* (pp. 225-235). New York: New York Academy of Sciences.

Toma, C. L. (2010). *Perceptions of trustworthiness online: The role of visual and textual information.* Paper presented at CSCW2010, Savannah, Georgia.

Toma, C. J., & Hancock, J. T. (2012). What lies beneath: The linguistic traces of deception in online dating profiles. *Journal of Communication, 62,* 78-97. doi:10.1111/j.1460-2466.2011.01619.x.

Toma, C. L., Hancock, J. T., & Ellison, N. B. (2008). Separating fact from fiction: An examination of deceptive self-presentation in online dating profiles. *Personality and Social Psychology Bulletin, 34,* 1023-1036. doi: 10.1177/0146167208318067

USAID. (2010). *Energy Security and Conflict: A Country-Level Review of the Issues.* Washington: USAID.

Utz, S. (2005). Types of deception and underlying motivation: What people think. *Social Science Computer Review. 23,* 49-56.

Van Koppen, P. J. (2012). Deception detection in police interrogations: Closing in on the context of criminal investigations. *Journal of Applied Research in Memory and Cognition.* doi:10.1016/j.jarmac.2012.04.005.

van Notte, P. W. F., Rotmans, J., van Asselt, M. B. A., & Rothman, D. S. (2003). An updated scenario typology. *Futures, 35,* 423-443. doi: 10.1016/S0016-3287(02)00090-3.

Van Swol, L. M., Braun, M. T., & Kolb, M. R. (2013). Deception, detection, demeanour, and truth-bias in face-to-face and computer-mediated communication. *Communication Research.* doi: 10.1177/0093650213485785.

Varum, C. A., & Melo, C. (2010). Directions in scenario planning literature – A review of the past decades. *Futures, 42,* 355-359. doi: 10.1016/j.futures.2009.11.021.

Vego, M.N. (2002). Operation deception in the information age. *Joint Forces Quarterly.* (Spring 2002), 60-66.

Vess, J., Ward, T., & Collie, R. (2008). Case formulation with sex offenders: An illustration of individualized risk assessment. *Journal of Behavior Analysis of Offender and Victim: Treatment and Prevention, 1,* 284-295.

VICE. (2013, March 25). *3D Printed Guns (Documentary)* [Video file]. Retrieved from https://www.youtube.com/watch?v=DconsfGsXyA.

Vishwanath, A. (2015). Habitual facebook use and its impact on getting deceived on social media. *Journal of Computer-Mediated Communication, 20,* 83-98. doi:10.1111/jcc4.12100.

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems, 51,* 576-586. doi: 10.1016/j.dss.2011.03.002.

Vrij, A. (2000). *Detecting lies and deceit: The psychology of lying and the implications for professional practice.* Chichester: Wiley.

Vrij, A. (2004). Guidelines to catch a liar. In P. A. Granhag & L. A. Strömwall (Eds.). *The Detection of Deception in Forensic Contexts.* (pp. 287-314). Cambridge: Cambridge University Press.

Vrij, A. (2005). Criteria-based content analysis: A qualitative review of the first 37 studies. *Psychology, Public Policy, and Law, 11,* 3-41. doi: 10.1037/1076-8971.11.1.3.

Vrij, A. (2008). *Detecting lies and deceit: Pitfalls and Opportunities.* Chichester: Wiley.

Vrij, A. (2015b). A cognitive approach to lie detection. In P. A. Granhag, A. Vrij & B. Verschuere (Eds.). *Detecting Deception: Current Challenges and Cognitive Approaches.* (pp. 205-229). Chichester: Wiley Blackwell.

Vrij, A., Akehurst, L., Soukara, S., & Bull, R. (2004a). Detecting deceit via analysis of verbal and nonverbal behavior in children and adults. *Human Communication Research, 30*, 8-41.

Vrij, A., & Baxter, M. (1999). Accuracy and confidence in detecting truths and lies in elaborations and denials: Truth bias, lie bias and individual differences. *Expert Evidence,* 7, 25-36.

Vrij, A., Edward, K., Roberts, K. P., & Bull, R. (2000). Detecting deceit via analysis of verbal and nonverbal behavior. *Journal of Nonverbal Behavior, 24*, 239-263.

Vrij, A., Evans, H., Akehurst, L., & Mann, S. (2004). Rapid judgements in assessing verbal and nonverbal cues: Their potential for deception researchers and lie detection. *Applied Cognitive Psychology, 18*, 283-296. doi: 10.1002/acp.964.

Vrij, A., Fisher, R. P., Mann, S., & Leal, S. (2008). A cognitive load approach to lie detection. *Journal of Investigative Psychology and Offender Profiling, 5*, 39-43. doi: 10.1002/jip.82.

Vrij, A., & Graham, S. (1997). Individual differences between liars and the ability to detect lies. *Expert Evidence, 5*, 144-148.

Vrij, A., & Granhag, P. A. (2012a). Eliciting cues to deception and truth: What matters are the questions asked. *Journal of Applied Research in Memory and Cognition.* doi: 10.1016/j.jarmac.2012.02.004.

Vrij, A., Granhag, P.A., & Mann, S. (2004). Good Liars. *Unpublished Manuscript*

Vrij, A., Granhag, P.A., Mann, S., & Leal, S. (2011a). Outsmarting the liars: Towards a cognitive lie detection approach. *Current Directions in Psychological Science. 20,* 28-32. doi: 10.1177/0963721410391245.

Vrij, A., Granhag, P.A., Mann, S. & Leal, S. (2011b). Lying about flying: The first experiment to detect false intent. *Psychology, Crime & Law. 17*, 611-620.

Vrij, A., Jundi, S., Hope, L., Hillman, J., Gahr, E., Leal, S., Warmelink, L., Mann, S., Vernham, Z., & Granhag, P. A. (in press). Collective interviewing of suspects. *Journal of Applied Research in Memory and Cognition.* doi: 10.1016/j.jarmac.2011.12.002.

Vrij, A., Kneller, W., & Mann, S. (2000). The effect of informing liars about criteria-based content analysis on their ability to deceive CBCA-raters. *Legal and Criminological Psychology, 5,* 57-70.

Vrij, A., Leal, S., Granhag, P. A., Mann, S., Fisher, R. P., Hillman, J., & Sperry, K. (2009). Outsmarting the liars: The benefit of asking unanticipated questions. *Law and Human Behavior, 33,* 159-166. doi: 10.1007/s10979-008-9143-y.

Vrij, A., Leal, S., Mann, S., & Fisher, R. (2011). Imposing cognitive load to elicit cues to deceit: Inducing the reverse order technique naturally. *Psychology, Crime & Law*. doi: 10.1080/1068316X.2010.515987.

Vrij, A., Leal, S., Mann, S.A. & Granhag, P.A. (2011). A comparison between lying about intentions and past activities: Verbal cues and detection accuracy. *Applied Cognitive Psychology. 25*, 212-218.

Vrij, A., Leal, S., Mann, S., Warmelink, L., Granhag, P. A., & Fisher, R. P. (2011). Drawings as an innovative and successful lie detection tool. *Applied Cognitive Psychology, 24*, 587-594. doi: 10.1002/acp.1627.

Vrij, A., & Mann, S. (2001). Telling and detecting lies in a high-stake situation: The case of a convicted murderer. *Applied Cognitive Psychology, 15,* 187-203.

Vrij, A., & Mann, S. A. (2004). Detecting deception: The benefits of looking at a combination of behavioural, auditory and speech content related cues in a systematic manner. *Group Decision and Negotiation, 13,* 61-79.

Vrij A., Mann, S. A., Fisher, R. P., Leal, S., Milne, R., & Bull, R. (2008). Increasing cognitive load to facilitate lie detection: The benefit of recalling an event in reverse order. *Law and Human Behavior, 32*, 253-265. doi: 10.1007/s10979-007-9103-y.

Vrij, A., Mann, S., Jundi, S., Hope, L., & Leal, S. (2012). Can I take your picture? Undercover interviewing to detect deception. *Psychology, Public Policy and Law. 18,* 231-244. doi: 10.1037/a0025670.

Vrij, A., Mann, S., Kristen, S., & Fisher, R. P. (2007). Cues to deception and ability to detect lies as a function of police interview styles. *Law and Human Behavior, 31,* 499-518. doi: 10.1007/s10979-006-9066-4.

Vrij, A., Mann, S., Leal, S., & Fisher, R. (2010). 'Look into my eyes': can an instruction to maintain eye contact facilitate lie detection? *Psychology, Crime & Law, 16,* 327-348. doi: 10.1080/10683160902740633.

Vrij, A., Mann, S., Leal, S., & Granhag, P. A. (2010). Getting into the minds of pairs of liars and truth tellers: An examination of their strategies. *The Open Criminology Journal, 3,* 17-22.

Walczyk, J.J., Schwartz, J.P., Clifton, R., Adams, B., Wei, M., & Zha, P. (2005). Lying person-to-person about life events: A cognitive framework for lie detection. *Personnel Psychology. 58,* 141-170.

Wall, H. J., Taylor, P. J., Dixon, J., Conchie, S. M., & Ellis, D. A. (2013). Rich contexts do not always enrich the accuracy of personality judgements. *Journal of Experimental Social Psychology.* doi: 10.1016/j.jesp.2013.05.010.

Wallace, R. J., & Lofi, J. M. (2014). The unmitigated insider threat to aviation (Part 2): An analysis of countermeasures. *Journal of Transportation Security, 7,* 307-331. doi: 10.1007/s12198-014-0150-6.

Warkentin, D., Woodworth, M., Hancock, J. T., & Cormier, N. (2010). *Warrants and deception in computer mediated communication.* Paper presented at CSCW, Savannah, Georgia, USA.

Warmelink, L., Vrij, A., Mann, S., Jundi, S., & Granhag, P. A. (2012). The effect of question expectedness and experience on lying about intentions. *Acta Psychologia, 141,* 178-183. doi: 10.1016/j.actpsy.2012.07.011.

Warmelink, L., Vrij, A., Mann, S., Leal, S., Forrester, D. & Fisher, R.P. (2011). Thermal imaging as a lie detection tool at airports. *Law and Human Behavior. 35,* 40-48.

Webster, C., Douglas, K., Eaves, D., & Hart, S. (1997). *HCR-20: Assessing risk for violence (Version 2).* Vancouver, Canada: Simon Fraser University.

Weimann, G. (2004). www.terror.net: How modern terrorism uses the internet. *United States Institute of Peace: Special Report 116.*

Weimann, G. & Gorder, G.V. (2009). Al-Qaeda has sent you a friend request: Terrorists using online social networking. *InSITE. 2,* 20-26.

Werdin, K., Colwell, K., Hiscock-Anisman, C. K., Hartwig, M., Bessenoff, G., & Fede, J. (2012). ACID and computer-mediated deception: The use of Assessment Criteria Indicative of Deception to assess credibility via instant messaging. Manuscript under review.

Whaley, B. (1973). *Codeword BARBAROSSA.* Cambridge: MIT Press.

Whaley, B. (1982). Toward a general theory of deception. *Journal of Strategic Studies, 5,* 178-192.

Whaley, B. (2006). Interdisciplinary musings on the history of counterdeception. *Defense Intelligence Journal, 15,* 31-50.

Whaley, B. (2007). *Stratagem: Deception and Surprise in War.* London: Artech House.

Whaley, B., & Busby, J. (2002). Detecting deception: Practice, practitioners, and theory. In R. Godson & J. J. Wirtz. (Eds.). *Strategic Denial and Deception: The Twenty-First Century Challenge.* (pp. 181-221). London: Transaction Publishers.

Whitty, M. T. (2002). Liar, liar! An examination of how open, supportive and honest people are in chat rooms. *Computers in Human Behavior, 18,* 342-352.

Whitty, M. T., Buchanan, T., Joinson, A. N., & Meredith, A. (2012). Not all lies are spontaneous: An examination of deception across different modes of communication. *Journal of the American Society for Information Science and Technology, 63,* 208-216. doi: 10.1002/asi.21648.

Whitty, M. T., & Carville, S. E. (2008). Would I lie to you? Self-serving lies and other-oriented lies told across different media. *Computers in Human Behavior, 24,* 1021-1031. doi:10.1016/j.chb.2007.03.004.

Wilkinson, A., Kupers, R., & Mangalagiu, D. (2013). How plausibility-based scenario practices are grappling with complexity to appreciate and address 21st century challenges. *Technological Forecasting and Social Change, 80,* 699-710. doi: 10.1016/j.techfore.2012.10.031.

Willis, H. H., Morral, A. R., Kelly, T. K., & Medby, J. J. (2005). *Estimating Terrorism Risk.* Santa Monica: The RAND Corporation.

Willis, J., & Todorov, A. (2006). First impressions: Making up your mind after a 100-ms exposure to a face. *Psychological Science, 17,* 592-598. doi: 10.1111/j.1467-9280.2006.01750.x.

Wilson, C. M., Desmarais, S. L., Nicholls, T. L., Hart, S. D., & Brink, J. (2013). Predictive validity of dynamic factors: Assessing violence risk in forensic psychiatric inpatients. *Law and Human Behavior, 37,* 377-388. doi: 10.1037/lhb0000025.

Wilson, M. A., & Lemanski, L. (2013). Apparent intended lethality: Toward a model of intent to harm in terrorist bomb attacks. *Dynamics of Asymmetric Conflict: Pathways toward terrorism and genocide, 6,* 1-21. doi: 10.1080/17467586.2013.771277.

Wilson, M. A., Scholes, A., & Brocklehurst, E. (2010). A behavioural analysis of terrorist action: The assassination and bombing campaigns of ETA between 1980 and 2007. *British Journal of Criminology, 50,* 690-707. doi: 10.1093/bjc/azq023.

Wiseman, R., Watt, C., ten Brinke, L., Porter, S, Couper, S. L., & Rankin, C. (2012). The eye's don't have it: Lie detection and neuro-linguistic programming. *PloS One.* doi:10.1371/journal.pone.0040259.

Wolfe, A. L., & Arrow, H. (2013). Military influence tactics: Lessons learned in Iraq and Afghanistan. *Military Psychology.* doi: 10.1037/mil0000009.

Woodworth, M., Hancock, J., & Goorha, S. (2005). *The motivational enhancement effect: Implications for our chosen modes of communication in the 21st Century.* Proceedings of International Conference of Systems Science, Hawaii, USA.

Wright, A. (2005). The role of scenarios as prospective sensemaking devices. *Management Decision, 43,* 86-101. doi: 10.1108/00251740510572506.

Wright, R., Chakraborty, S., Basoglu, A., & Marett, K. (2010). Where did they go right? Understanding the deception in phishing communities. *Group Decision and Negotiation, 19,* 391-416. doi: 10.1007/s10726-009-9167-9.

Wright Whelan, C., Wagstaff, G. F., & Wheatcroft, J. M. (2013). High-Stakes Lies: Verbal and nonverbal cues to deception in public appeals for help with missing or murdered relatives. *Psychiatry, Psychology and Law.* doi: 10.1080/13218719.2013.839931.

Wright Whelan, C., Wagstaff, G., & Wheatcroft, J. M. (2015). High stakes lies: Police and non-police accuracy in detecting deception. *Psychology, Crime & Law, 21,* 127-138. doi: 10.1080/1068316X.2014.935777.

Yang, M., Wong, S., & Coid, J. (2010). The efficacy of violence prediction: A meta-analytic comparison of nine risk assessment tools. *Psychological Bulletin, 136,* 740-767. doi: 10.1037/a0020473.

Yang, Z. L., Wang, J., Bonsall, S., & Fang, Q. G. (2009). Use of fuzzy evidential reasoning in maritime security assessment. *Risk Analysis, 29,* 95-120. doi: 10.1111/j.1539-6924.2008.01158.x.

Yin, R. K. (2003). *Case Study Research: Design and Methods.* London: Sage.

Yue, S., Harmer, K., Guo, K., Adams, K., & Hunter, A. (2014). Automatic blush detection in 'concealed information' test using visual stimuli. *International Journal of Data Mining, Modelling and Management, 6,* 187-201.

Zhou, L., Burgoon, J. K., Nunamaker, J. F., Jr., & Twitchell, D. (2004). Automating linguistic-based cues for detecting deception in text-based asynchronous computer-mediated communication. *Group Decision and Negotiation, 13,* 81-106.

Zhou, L., & Sung, Y. W. (2008). Cues to deception in online Chinese groups. *Proceedings of the 41st Hawaii International Conference on System Science.*

Zhou, L., & Zhang, D. (2006). A comparison of deceptive behaviour in dyad and triadic group decision making in synchronous computer-mediated communication. *Small Group Research. 37,* 140-164.

Zhou, L., & Zhang, D. (2007). Typing or messaging? Modality effect on deception detection in computer-mediated communication. *Decision Support Systems, 44,* 188-201. doi: 10.1016/j.dss.2007.03.012.

Zimbler, M., & Feldman, R. S. (2011). Liar, liar, hard drive on fire: How media context affects lying behaviour. *Journal of Applied Social Psychology, 41,* 2492-2507.

Zuckerman, M., DePaulo, B. M., & Rosenthal, R. (1981). Verbal and nonverbal communication of deception. In L. Berkowitz (Ed.). *Advances in Experimental Social Psychology.* (Vol. 14, pp. 1-59). New York: Academic Press.

Appendices

Appendix 2.1 Content criteria for statement analysis

General characteristics

Logical structure

Unstructured production

Quantity of details

Specific contents

Contextual embedding

Descriptions of interactions

Reproduction of conversation

Unexpected complications during the incident

Unusual details

Superfluous details

Accurately reported details misunderstood

Related external associations

Accounts of subjective mental state

Attribution of perpetrator's mental state

Motivation-related contents

Spontaneous corrections

Admitting lack of memory

Raising doubts about one's own testimony

Self-deprecation

Pardoning the perpetrator

Offence-specific elements

Details characteristic of the offence

Source: adapted from Steller and Kohnken (1989)

Appendix 2.2 Reality Monitoring criteria

Clarity

Perceptual information

Spatial information

Temporal information

Affect

Reconstructability of the story

Realism

Cognitive operations

Source: adapted from Vrij (2008)

Appendix 2.3 The CHAMELEON Offender

C HARACTERISED BY CHANGE
H EALTH (PERSONALITY & MENTAL DISORDERS/PHYSICAL)
A TTITUDES, ALLEGIANGES & AFFILIATIONS
M INDSET & MOTIVATION & MALIGN INTENT
E YES (INTERACTIONS, INTERVIEWS & INTERVIEWERS)
L IES & LIMITATIONS
E NVIRONMENT
O FFENCES & OPPORTUNITIES
N UANCES, NEGATIVITY & NEEDS

Source: adapted from Gozna & Boon (2007)

Appendix 2.4 The CHAMELEONS

Malicious (venomous) CHAMELEON - contemptuous, anti-view of the world and feels no remorse for their actions;

Conceited (swaggering) CHAMELEON - grand and aloof with intellectual arrogance and the attitude of an alpha male;

Pseudo-charming CHAMELEON - apparent aspects of being a confident, attractive conversationalist;

Obsequious (slimy) CHAMELEON - portrayal of a victim and will be in awe of authorities and will attempt to 'suck up' to them;

Dissembling (sluggish) CHAMELEON - who will cover for deflecting questions and will feign vulnerabilities and claim incapacity in relation to their actions;

Unstable (chaotic) CHAMELEON - spectrum of moods, inconsistent loyalties and anger, be engaging, manipulative and self-centred, with their own biased sense of justice;

Rainbow CHAMELEON - anything at any time depending on their needs

Source: adapted from Gozna (2011)

Appendix 3.1 Psychological principles of social engineering

1. Trappings of role: The social engineer exhibits a few behavioural characteristics of the role he/she is masquerading in so the target will infer other attributes and act accordingly.

2. Authority: People are more likely, in the right situation, to be highly responsive to assertions of authority, even when the person who purports to be in a position of authority is not physically present.

3. Credibility: Establishing credibility is a key step in most SE arracks as it leads to trust.

4. Altercasting: A strategy for persuading people by forcing them into a social role, so that they will be inclined to behave according to that role.

5. Distracting from systematic thinking: Encouraging the target to process information, heuristically. People operating in a heuristic mode are more likely to use mental shortcuts, less likely to have access to their psychological defences and are less inclined to be suspicious, ask questions, or present objections to the attacker.

6. The desire to help: Helping has many benefits: it can make us feel empowered; it can get us out of a bad mood; and it can make us feel good about ourselves.

7. Liking and similarity: People prefer to say 'yes' to those they know and like. Factors that enhance liking include: similarity of attitude; background; physical attractiveness; dress; and the use of praise and cooperation.

8. Fear: A social engineer will sometimes make his/her target believe that some terrible thing is about to happen, but that the impending disaster can be averted if the target does as the attacker suggests.

9. Reactance: Psychological reactance is the negative reaction we experience when we perceive that our choices or freedoms are being taken away.

10. Reciprocation: People are more likely to comply with requests from those who have provided things first.

11. Commitment and consistency: People have a desire to look consistent through their words, beliefs, attitudes and deeds.

12. Social proof: People are more willing to take a recommended action if they see evidence that many others, especially similar others, are taking it.

Source: Adapted from Henderson et al. (2007)

Appendix 3.2 Credibility Topics

Topic of Credibility Comment	Incidence
Design Look	46.1%
Information Design/Structure	28.5%
Information Focus	25.1%
Company Motive	15.5%
Usefulness of Information	14.8%
Accuracy of Information	14.3%
Name Recognition & Reputation	14.1%
Advertising	13.8%
Bias of Information	11.6%
Tone of the Writing	9.0%
Identity of Site Sponsor	8.8%
Functionality of Site	8.6%
Customer Service	6.4%
Past Experience with Site	4.6%
Information Clarity	3.7%
Performance on a Test	3.6%
Readability	3.6%
Affiliations	3.4%

Source: Adapted from Fogg et al. (2003)

Appendix 5.1: Deception Framework Table

ELEMENTS	RESEARCH REFERENCE
Verbal	Colwell, K., Hiscock, C. K., & Memon, A. (2002). Interviewing techniques and the assessment of statement credibility. *Applied Cognitive Psychology, 16*, 287-300. doi: 10.1002/acp.788. DePaulo, B. M., Lindsay, J. J., Malone, B. E., Muhlenbruck, L., Charlton, K., & Cooper, H. (2003). Cues to deception. *Psychological Bulletin, 129*, 74-118. Global Deception Research Team (2006). A world of lies. *Journal of Cross-Cultural Psychology. 37*, 60-74. Hartwig, M., Granhag, P. A., Strömwall, L. A., Wolf, A. G., Vrij, A., & Roos af Hjelmsater, E. (2011). Detecting deception in suspects: Verbal cues as a function of interview strategy. *Psychology, Crime & Law, 17*, 643-656. doi: 10.1080/10683160903446982. Porter, S., & ten Brinke, L. (2010). The truth about lies: What works in detecting high-stakes deception? *Legal and Criminological Psychology, 15*, 57-75. doi: 10.1348/135532509X433151. ten Brinke, L., MacDonald, S., Porter, S., & O'Connor, B. (2011). Crocodile tears: Facial, verbal and

	body language behaviours associated with genuine and fabricated remorse. *Law and Human Behavior.* doi: 10.1007/s10979-011-9265-5. ten Brinke, L., & Porter, S. (2011a). Cry me a river: Identifying the behavioural consequences of extremely high-stakes interpersonal deception. *Law and Human Behavior.*
Physical	Cavina-Pratesi, C., Kuhn, G., Ietswaart, M., & Milner, A. D. (2011). The magic grasp: Motor expertise in deception. *PLoS ONE, 6*, e16568. doi: 10.1371/journal.pone.0016568. Sebanz, N., & Shiffrar, M. (2009). Detecting deception in a bluffing body: The role of expertise. *Psychonomic Bulletin & Review, 16*, 170-175. doi: 10.3758/PBR.16.1.170.
Social Engineering (Conning, Fraud etc)	Cui, J., Otero-Millan, J., Macknik, S. L., King, M., Martinez-Conde, S. (2011). Social misdirection fails to enhance a magic illusion. *Frontiers in Human Neuroscience, 5,* 103. doi: 10.3389/fnhum.2011.00103. Otero-Millan, J., Macknik, S. L.,

	Robbins, A., & Martinez-Conde, S. (2011). Stronger misdirection in curved than in straight motion. *Frontiers in Human Neuroscience, 5*, 133. doi: 10.3389/fnhum.2011.00133. Wiseman, R., & Greening, E. (2005). 'It's still bending': Verbal suggestion and alleged psychokinetic ability. *British Journal of Psychology, 96*, 115-127. doi: 10.1348/000712604X15428.
Impression Management (Body Language, Method Acting, CHAMELEON)	Gozna, L. F., & Boon, J. C. W. (2010). Interpersonal deception detection. In J.M. Brown & E.A. Campbell (Eds.). *The Cambridge handbook of forensic psychology.* (pp. 484-491). Cambridge: Cambridge University Press. Granhag, P. A., Strömwall, L. A., & Jonsson, A. C. (2003). Partners in crime: How liars in collusion betray themselves. *Journal of Applied Social Psychology,33*, 848-868. Hartwig, M., Granhag, P. A., & Strömwall, L. A. (2007). Guilty and innocent suspects' strategies during police interrogations. *Psychology, Crime & Law, 13*, 213-227. doi: 10.1080/10683160600750264.

	Navarro, J. (2003). A four-domain model of detecting deception. *FBI Law Enforcement Bulletin* (June), 19-24. Taylor, R., & Gozna, L. F. (2011). *Deception: A Young Person's Life Skill?* Hove: Psychology Press.
Written (SVA etc)	Akehurst, L., Manton, S., & Quandte, S. (2011). Careful calculation or a leap of faith? A field study of the translation of CBCA ratings to final credibility judgements. *Applied Cognitive Psychology. 25*, 236-243. Armistead, T. W. (2011). Detecting deception in written statements: The British Home Office study of Scientific Content Analysis (SCAN). (Unpublished Manuscript). Bond, G. D., & Lee, A. Y. (2005). Language of lies in prison: Linguistic classification of prisoners' truthful and deceptive natural language. *Applied Cognitive Psychology. 19*, 313-329. Brown, J. (2010). Statement validity analysis. In J. Brown & E. Campbell (Eds.), *The Cambridge Handbook of Forensic*

Psychology. Cambridge: Cambridge University Press.

Driscoll, L. N. (1994). A validity assessment of written statements from suspects in criminal investigations using the SCAN technique. *Police Studies, 17*, 77-88.

Köhnken, G. (2004). Statement Validity Analysis and the 'detection of the truth'. In P.A. Granhag & L.A. Stromwall (Eds.). *The detection of deception in forensic contexts.* (pp. 41-63). Cambridge: Cambridge University Press.

Masip, J., Sporer, S. L., Garrido, E., & Herrero, C. (2005). The detection of deception with the reality monitoring approach: A review of the empirical evidence. *Psychology, Crime & Law, 11*, 99-122. doi: 10.1080/10683160410001726356.

Newman, M. L., Pennebaker, J. W., Berry, D. S., & Richards, J. M. (2003). Lying words: Predicting deception from linguistic styles. *Personality and Social Psychology Bulletin, 29,* 665-675. doi: 10.1177/0146167203251529.

Pennebaker, J. W., Booth, R. J., & Francis, M. E. (2007). Linguistic Inquiry and Word Count: LIWC

[Computer software]. Austin, TX: LIWC.net.

Porter, S., & ten Brinke, L. (2010). The truth about lies: What works in detecting high-stakes deception? *Legal and Criminological Psychology, 15*, 57-75. doi: 10.1348/135532509X433151.

Porter, S., & Yuille, J. C. (1996). The language of deceit: an investigation of the verbal clues to deception in the interrogation context. *Law and Human Behavior, 20*, 443-459.

Rassin, E. (2000). Criteria based content analysis: The less scientific road to truth. *Expert Evidence, 7*, 265-278.

Sapir, A. (1987). *Scientific content analysis (SCAN)*. Phoenix, AZ: Laboratory for Scientific Interrogation.

Smith, N. (2001). Reading between the lines: An evaluation of the scientific content analysis technique (SCAN). Police research series paper 135. London: UK Home Office, Research, Development and Statistics Directorate.

Sporer, S. L. (2004). Reality monitoring and detection of deception. In P.A. Granhag & L.A. Stromwall

(Eds.). *The detection of deception in forensic contexts.* (pp. 64-102). Cambridge: Cambridge University Press.

Vrij, A. (2005). Criteria-based content analysis: A qualitative review of the first 37 studies. *Psychology, Public Policy, and Law, 11*, 3-41. doi: 10.1037/1076-8971.11.1.3.

Vrij, A., Akehurst, L., Soukara, S., & Bull, R. (2004a). Detecting deceit via analysis of verbal and nonverbal behavior in children and adults. *Human Communication Research, 30*, 8-41.

Vrij, A., Edward, K., Roberts, K. P., & Bull, R. (2000). Detecting deceit via analysis of verbal and nonverbal behavior. *Journal of Nonverbal Behavior, 24*, 239-263.

Vrij, A., Evans, H., Akehurst, L., & Mann, S. (2004). Rapid judgements in assessing verbal and nonverbal cues: Their potential for deception researchers and lie detection. *Applied Cognitive Psychology, 18*, 283-296. doi: 10.1002/acp.964.

Vrij, A., Kneller, W., & Mann, S. (2000). The effect of informing liars about criteria-based content analysis on their ability to deceive

	CBCA-raters. *Legal and Criminological Psychology, 5*, 57-70.
Audio	Leal, S., Vrij, A., Warmelink, L., Vernham, Z., & Fisher, R. P. (2013). You cannot hide your telephone lies: Providing a model statement as an aid to detect deception in insurance telephone calls. *Legal and Criminological Psychology*. doi: 10.1111/lcrp.12017. Porter, S., Campbell, M. A., Stapleton, J., & Birt, A. R. (2002). The influence of judge, target, and stimulus characteristics on the accuracy of detecting deceit. *Canadian Journal of Behavioural Science, 34*, 172-185.
Physiological	Meijer, E. H., Verschuere, B., & Merckelbach, H. (2010). Detecting criminal intent with the concealed information test. *Open Criminology Journal, 3*, 44-47. Wolpe, P. R., Foster, K. R., & Langleben, D. D. (2005). Emerging neurotechnologies for lie-detection: Promises and perils. *American Journal of Bioethics, 5*, 39-49. doi: 10.1080/15265160590923367.

Micro-expressions	Ekman, P. (2001). *Telling lies: Clues to deceit in the marketplace, politics and marriage.* London: W. W. Norton & Company. Porter, S., & ten Brinke, L. (2010). The truth about lies: What works in detecting high-stakes deception? *Legal and Criminological Psychology, 15*, 57-75. doi: 10.1348/135532509X433151. ten Brinke, L., MacDonald, S., Porter, S., & O'Connor, B. (2011). Crocodile tears: Facial, verbal and body language behaviours associated with genuine and fabricated remorse. *Law and Human Behavior.* doi: 10.1007/s10979-011-9265-5. ten Brinke, L., & Porter, S. (2011a). Cry me a river: Identifying the behavioural consequences of extremely high-stakes interpersonal deception. *Law and Human Behavior.* ten Brinke, L., Porter, S., & Baker, A. (2011). Darwin the detective: Observable facial muscle contractions reveal emotional high-stakes lies. *Evolution and Human Behavior.* doi: 10.1016/j.evolhumbehav.2011.12.003.

Non-Verbal	DePaulo, B. M., Lindsay, J. J., Malone, B. E., Muhlenbruck, L., Charlton, K., & Cooper, H. (2003). Cues to deception. *Psychological Bulletin, 129*, 74-118. Ekman, P. (2001). *Telling lies: Clues to deceit in the marketplace, politics and marriage.* London: W. W. Norton & Company. Global Deception Research Team (2006). A world of lies. *Journal of Cross-Cultural Psychology. 37*, 60-74. Hillman, J., Vrij, A., & Mann, S. (2011). Um… they were wearing…: The effect of deception on specific hand gestures. *Legal and Criminological Psychology.* doi: 10.1111/j.2044-8333.2011.02014.x Leal, S., & Vrij, A. (2008). Blinking during and after lying. *Journal of Nonverbal Behavior, 32*, 187-194. doi: 10.1007/s10919-008-0051-0. Porter, S., England, L., Juodis, M., ten Brinke, L., & Wilson, K. (2008). Is the face a window to the soul? Investigation of the accuracy of intuitive judgements of the trustworthiness of human faces. *Canadian Journal of Behavioural Science, 40*, 171-177. doi: 10.1037/0008-400X.40.3.171. ten Brinke, L., & Porter, S. (2011a). Cry

	me a river: Identifying the behavioural consequences of extremely high-stakes interpersonal deception. *Law and Human Behavior.* Vrij, A., Akehurst, L., Soukara, S., & Bull, R. (2004a). Detecting deceit via analysis of verbal and nonverbal behavior in children and adults. *Human Communication Research, 30*, 8-41. Vrij, A., Edward, K., Roberts, K. P., & Bull, R. (2000). Detecting deceit via analysis of verbal and nonverbal behavior. *Journal of Nonverbal Behavior, 24*, 239-263. Vrij, A., Evans, H., Akehurst, L., & Mann, S. (2004). Rapid judgements in assessing verbal and nonverbal cues: Their potential for deception researchers and lie detection. *Applied Cognitive Psychology, 18*, 283-296. doi: 10.1002/acp.964.
Identity	Wang, G., Chen, H., & Atabakhsh, H. (2004). Criminal identity deception and deception detection in law enforcement. *Group Decision and Negotiation, 13,* 111-127.
Plausibility of Communication	DePaulo, B. M., Lindsay, J. J., Malone,

	B. E., Muhlenbruck, L., Charlton, K., & Cooper, H. (2003). Cues to deception. *Psychological Bulletin, 129*, 74-118.
DRE Approaches	Colwell, K., Hiscock-Anisman, C., & Fede, J. (2013). Assessment criteria indicative of deception: An example of the new paradigm of differential recall enhancement. In B. S. Cooper, D. Griesel, & M. Ternes (Eds.). *Applied Issues in Investigative Interviewing, Eyewitness Memory, and Credibility Assessment.* (pp. 259-291). London: Springer Colwell, K., Hiscock-Anisman, C. K., Memon, A., Taylor, L., & Prewett, J. (2007). Assessment criteria indicative of deception (ACID): An integrated system of investigative interviewing and detecting deception. *Journal of Investigative Psychology and Offender Profiling, 4*, 167-180. doi: 10.1002/jip.73. Dando, C. J., & Bull, R. (2011). Maximising opportunities to detect verbal deception: Training police officers to interview tactically. *Journal of Investigative Psychology and Offender Profiling. 8*, 189-292.

Granhag, P. A., Stromwall, L. A., Willen, R. M., & Hartwig, M. (2012). Eliciting cues to deception by tactical disclosure of evidence: The first test of the Evidence Framing Matrix. *Legal and Criminological Psychology.* doi: 10.1111/j.2044-8333.2012.02047.x.

Granhag, P.A. & Vrij, A. (2010). Interviewing to detect deception. In P.A. Granhag (Ed.). *Forensic psychology in context: Nordic and international approaches.* Devon: Willan Publishing.

Hartwig, M., Granhag, P. A., Strömwall, L. A., Wolf, A. G., Vrij, A., & Roos af Hjelmsater, E. (2011). Detecting deception in suspects: Verbal cues as a function of interview strategy. *Psychology, Crime & Law, 17,* 643-656. doi: 10.1080/10683160903446982.

Leins, D., Fisher, R. P., & Vrij, A. (2012). Drawing on liar's lack of cognitive flexibility: Detecting deception through varying report modes. *Applied Cognitive Psychology,* doi: 10.1002/acp.2837.

Leins, D., Fisher, R. P., Vrij, A., Leal, S., & Mann, S. (2011). Using sketch drawing to induce inconsistency

in liars. *Legal and Criminological Psychology, 16,* 253-265. doi: 10.1348/135532510X501775.

Hartwig, M., Granhag, P. A., Strömwall, L. A., & Kronkvist, O. (2006). Strategic use of evidence during police interviews: When training to detect deception works. *Law and Human Behavior, 30*, 603-619. doi: 10.1007/s10979-006-9053-9.

Suckle-Nelson, J. A., Colwell, K., Hiscock-Anisman, C., Florence, S., Youschak, K. E., & Duarte, A. (2010). Assessment criteria indicative of deception (ACID): Replication and gender differences. *The Open Criminology Journal, 3*, 23-30.

Vrij, A., Granhag, P.A., Mann, S., & Leal, S. (2011a). Outsmarting the liars: Towards a cognitive lie detection approach. *Current Directions in Psychological Science. 20*, 28-32. doi: 10.1177/0963721410391245.

Vrij, A., Leal, S., Granhag, P. A., Mann, S., Fisher, R. P., Hillman, J., & Sperry, K. (2009). Outsmarting the liars: The benefit of asking unanticipated questions. *Law and Human Behavior, 33*, 159-166. doi: 10.1007/s10979-008-9143-y.

Vrij, A., Leal, S., Mann, S., & Fisher, R. (2011). Imposing cognitive load to elicit cues to deceit: Inducing the reverse order technique naturally. *Psychology, Crime & Law*. doi: 10.1080/1068316X.2010.515987.

Vrij, A., Leal, S., Mann, S., Warmelink, L., Granhag, P. A., & Fisher, R. P. (2011). Drawings as an innovative and successful lie detection tool. *Applied Cognitive Psychology, 24*, 587-594. doi: 10.1002/acp.1627.

Vrij A., Mann, S. A., Fisher, R. P., Leal, S., Milne, R., & Bull, R. (2008). Increasing cognitive load to facilitate lie detection: The benefit of recalling an event in reverse order. *Law and Human Behavior, 32*, 253-265. doi: 10.1007/s10979-007-9103-y.

Vrij, A., Mann, S., Leal, S., & Fisher, R. (2010). 'Look into my eyes': can an instruction to maintain eye contact facilitate lie detection? *Psychology, Crime & Law, 16*, 327-348. doi: 10.1080/10683160902740633.

Walczyk, J.J., Schwartz, J.P., Clifton, R., Adams, B., Wei, M., & Zha, P. (2005). Lying person-to-person about life events: A cognitive

	framework for lie detection. *Personnel Psychology. 58*, 141-170.
Interaction	Burgoon, J. K., Buller, D. B., White, C. H., Afifi, W., & Buslig, A. L. S. (1999). The role of conversational involvement in deceptive interpersonal interactions. *Personality and Social Psychology Bulletin. 25*, 669-686. Granhag, P. A., Strömwall, L. A., & Jonsson, A. C. (2003). Partners in crime: How liars in collusion betray themselves. *Journal of Applied Social Psychology,33*, 848-868.

Appendix 5.2: Individual Differences Framework Table

ELEMENTS (IND DIFF)	RESEARCH REFERENCE
Personality	Baker, A., ten Brinke, L., & Porter, S. (2012). Will get fooled again: Emotionally intelligent people are easily duped by high-stakes deceivers. doi.1111/j.2044-8333.2012.02054.x. Christie, R., & Geis, F. L. (1970). *Studies in Machiavellianism*. New York: Academic Press. Cleckley, H. (1982). *The Mask of Sanity*. New York: Plume. Fowler, K. A., Lilienfeld, S. O., & Patrick, C. J. (2009). Detecting

psychopathy from thin slices of behavior. *Psychological Assessment, 21*, 68-78. doi: 10.1037/a0014938.

Gozna, L.F., Vrij, A. & Bull, R. (2001). The impact of individual differences on perceptions of lying in everyday life and in a high stake situation. *Personality and Individual Differences. 31*, 1203-1216.

Hare, R. D. (1970). *Psychopathy: Theory and research*. New York: John Wiley.

Kashy, D. A., & DePaulo, B. M. (1996). Who lies? *Journal of Personality and Social Psychology, 70,* 1037-1051

McLeod, B. A., & Genereux, R. L. (2008). Predicting the acceptability and likelihood of lying: The interaction of personality with type of lie. *Personality and Individual Differences, 45*, 591-596. doi: 10.1016/j.paid.2008.06.015.

O'Sullivan, M., & Ekman, P. (2004). The wizards of deception detection. In P. A. Granhag & L. A. Strömwall (Eds.), *Deception detection in forensic contexts* (pp. 269–286). Cambridge, UK: Cambridge Press.

Paulhus, D. L. (2013). Personal

communication.

Paulhus, D. L., & Williams, K. M. (2002). The Dark Triad of personality: Narcissism, Machiavellianism and psychopathy. *Journal of Research in Personality, 36*, 556-563.

Porter, S., Campbell, M. A., Stapleton, J., & Birt, A. R. (2002). The influence of judge, target, and stimulus characteristics on the accuracy of detecting deceit. *Canadian Journal of Behavioural Science, 34*, 172-185.

Porter, S., ten Brinke, L., Baker., & Wallace, B. (2011). Would I lie to you? "leakage" in deceptive facial expressions relates to psychopathy and emotional intelligence. *Personality and Individual Differences.* doi: 10.1016/j.paid.2011.03.031.

Raskin, R., & Hall, C. S. (1979). A Narcissistic Personality Inventory. *Psychological Reports*, *45*, 590.

Taylor, R., & Gozna, L. F. (2011). *Deception: A Young Person's Life Skill?* Hove: Psychology Press.

Vrij, A., & Graham, S. (1997). Individual differences between liars and the ability to detect lies. *Expert Evidence, 5*, 144-148.

Walczyk, J.J., Schwartz, J.P., Clifton, R.,

	Adams, B., Wei, M., & Zha, P. (2005). Lying person-to-person about life events: A cognitive framework for lie detection. *Personnel Psychology. 58,* 141-170.
Motivation	Hancock, J. T., Woodworth, M. T., & Goorha, S. (2010). See no evil: The effect of communication medium and motivation on deception detection. *Group Decision and Negotiation, 19,* 327-343. doi: 10.1007/s10726. Porter, S., McCabe, S., Woodworth, M., & Peace, K. A. (2007). Genius is 1% inspiration and 99% perspiration…or is it? An investigation of the impact of motivation and feedback on deception detection. *Legal and Criminological Psychology, 12,* 297-309. doi: 10.1348/135532506X143958.
Stakes	Gozna, L.F., Vrij, A. & Bull, R. (2001). The impact of individual differences on perceptions of lying in everyday life and in a high stake situation. *Personality and Individual Differences. 31,* 1203-1216. Porter, S., & ten Brinke, L. (2010). The truth about lies: What works in

	detecting high-stakes deception? *Legal and Criminological Psychology, 15*, 57-75. doi: 10.1348/135532509X433151. ten Brinke, L., & Porter, S. (2011a). Cry me a river: Identifying the behavioural consequences of extremely high-stakes interpersonal deception. *Law and Human Behavior.* ten Brinke, L., Porter, S., & Baker, A. (2011). Darwin the detective: Observable facial muscle contractions reveal emotional high-stakes lies. *Evolution and Human Behavior*. doi: 10.1016/j.evolhumbehav.2011.12.003. Van Koppen, P. J. (2012). Deception detection in police interrogations: Closing in on the context of criminal investigations. *Journal of Applied Research in Memory and Cognition.* doi:10.1016/j.jarmac.2012.04.005.
Demographic	Aamodt, M. G., & Custer, H. (2006). Who can best catch a liar? A meta-analysis of individual differences in detecting deception. *The Forensic Examiner. 15*, 6-11. Suckle-Nelson, J. A., Colwell, K., Hiscock-Anisman, C., Florence,

	S., Youschak, K. E., & Duarte, A. (2010). Assessment criteria indicative of deception (ACID): Replication and gender differences. *The Open Criminology Journal*, *3*, 23-30.
Culture	Al-Simadi, F. A. (2000). Detection of deceptive behaviour: A cross-cultural test. *Social Behavior and Personality. 28*, 455-462. Bond, C.F., Jr., & Atoum, A.O. (2000). International deception. *Personality and Social Psychology Bulletin. 26*, 385-395. Bond, C.F., Jr., & Rao, S.R. (2004). Lies travel: mendacity in a mobile world. In P.A. Granhag & L.A. Strömwall (Eds.). *The detection of deception in forensic contexts.* (pp. 127-147). Cambridge: Cambridge University Press. Cheng, K. H. W., & Broadhurst, R. (2005). The detection of deception: The effects of first and second language on lie detection ability. *Psychiatry, Psychology and Law. 12*, 107-118. Global Deception Research Team (2006). A world of lies. *Journal of Cross-Cultural Psychology. 37*, 60-74.
Religion	Campbell, A. (2006). Iran and deception

	modalities: The reach of *taqiyya, kitman*, *khod'eh*, and *taarof*. *National Observer, 70*, 25-48. Fogel, J., & Friedman, H. H. (2008). Conflict of interest and the Talmud. *Journal of Business Ethics, 78*, 237-246. doi: 10.1007/s10551-006-9327-7.
Motive/Intent	Caspi, A., & Gorsky, P. (2006). Online deception: Prevalence, motivation, and emotion. *CyberPsychology & Behavior, 9*, 54-59. doi: 10.1089/cpb.2006.9.54. Spidel, A., Hervé, H., Greaves, C., & Yuille, J. C. (2011). 'Wasn't me!' A field study of the relationship between deceptive motivations and psychopathic traits in young offenders. *Legal and Criminological Psychology, 16*, 335-347. doi: 10.1348/135532510X518722.
Politics & Allegiances	Beahrs, J. O. (1996). Ritual deception: A window to the hidden determinants of human politics. *Politics and the Life Sciences, 15*, 3-12. Rea-Dix, C. L. (1993). *Deception: Past Experiences –Future Opportunities.* Newport: Naval War College.

Appendix 5.3: Theoretical Holistic Model of Deception Scenarios

Scenario 1: Police-Suspect Interview

Following an altercation outside a nightclub an individual, on suspicion of having committed GBH, is arrested at the scene by police officers. The following morning once the suspect has sobered up he is interviewed by police. During the interview the suspect claims that they were actually the victim and that the altercation had been started by another individual. The suspect provides the interviewing officers a plausible account of the event in question, however, this account differs from that provided by the victim. In addition - there are mixed accounts from witnesses present at the incident. CCTV evidence provided by the local council-operated CCTV suggests that the suspect started the altercation; however, this evidence does not provide a narrative of the time preceding the event.

Scenario 2: Online Deception

In an attempt to gain access to confidential government information a hacker sends an email to an employee in a government HR department claiming to be an employee of a government branch. Whilst claiming to be an employee the hacker requests that their password is changed as they are worried that their account has been compromised. The email provides an explanation as to why the details need to be changed, however, although the employee details are all correct the email has not been sent from a government email account, but from another email provider. As the email appears credible at first glance the HR employee is required to judge whether they should change an account password and provide new password details.

Scenario 3: Parole Interview

After serving a required time period a prisoner applies for parole, in order to appear convincing and sincere to the parole board the prisoner is required to say why they believe they should be released. The prisoner describes their behaviour in prison in a positive manner, and highlights their attendance of education classes which will provide them with the skills required to obtain and perform employment outside of prison. The parole board are required to consider the prisoner's account of their future intentions alongside their behaviour in prison and a psychologist's account of the risk that the prisoner may present once outside the prison environment. However, the psychologist's report was largely inconclusive regarding the risks posed.

Appendix 6.1: Interview Schedule – Interpersonal, Online and Military Deception

This schedule contains questions that cover deception across the domains of interpersonal, online and military deception. The interview discussion will be tailored to the particular subject matter experts identified to participate in this research study. The questions identified below are identified as the basis for a discussion with SMEs although it is acknowledged that there will be further questions that may be identified during the course of the discussion and therefore these will be included in the discussions as appropriate.

All participants will receive the initial brief before signing the consent form once they are content to continue the discussions. It will be identified that if there are areas of their work that are inappropriate to discuss within the remit of the interview, participants will be able to skip answering certain questions.

Interpersonal deception

Please give an overview of the work you conduct in relation to deception.

In your particular field, how do you define deception?

What do you think are the environments or domains that are most relevant when considering interpersonal deception?

If you could pass on one thing you have learned during you experience in the field of deception, what would it be?

What sort of lies do you consider people use in high-stake deception? Can you give examples of this?

What strategies do you believe that liars use in their attempts to influence people that they are telling the truth? (Include strategies related to verbal and nonverbal impression management, the concealment of emotions etc.).

Do you believe that a person's underlying personality can influence how they lie to others?

How does a liar's motivation impact on their ability to lie successfully?

Does psychopathy make for a good liar or for someone who lies indiscriminately and therefore is not as successful?

In which situations do / have you detect/ed deception? How do you personally detect another person's lie? (What areas of verbal and nonverbal behaviour do you focus on in your attempt to detect another person's deception?)

What current strategies of deception detection are currently used in your respective field? Do they work effectively?

Are there techniques that should be incorporated into the current approach to deception detection which would improve the methods currently used?

Do you think there are parallels from interpersonal deception that apply to the online environment? What situations are these?

If you were to develop a model of deception detection, what factors would you consider significant?

What do you think is the most significant contribution that has been made in the field of deception research / work?

How do we detect when someone is telling the truth? Is credibility a wholly behavioural or verbal presentation of information?

Online deception

In your field of work, how is online deception defined?

What do you class as the most significant challenges in the area of online deception?

It is possible to develop strategies to detect deceit online? If so, in which areas?

In which circumstances does online deception occur?

(For example, deception may occur in online videos, in text-based computer-mediated communication incl. social networking sites, and in attempts at social engineering)

Are there examples of high stake deceptions that have occurred online?

Do these influence the ways that future deceptions occur?

How do you think such deceptions would manifest online?

What strategies do you believe that liars use in their attempts to influence online?

To what extent is it possible to gauge an individuals or groups personality online?

Can we ever truly know who we are interacting with?

Is online deception more likely to be successful when conducted online than interpersonally?

Are there strategies available to assist in the detection of deception online?

How do you think it is possible to improve the detection of deception in online interactions? Which types of online interactions would most benefit from this?

If you were tasked with developing a model of online deception, what would be the main factors you would class as significant to consider?

Is it possible to detect the truth or credibility when interacting online? How do people attribute credibility to particular sites or sources of information?

Military deception

How would you define military deception?

Although there are records of significant deceptive actions that have been conducted historically in military combat, in modern warfare, how has deception changed?

In what circumstances does deception occur in the military domain?

How can we inoculate ourselves against this? Is it just a case of 'know your enemy' or does today's asymmetric warfare make for more complex targeting?

Which are the more concerning forms of deception in the military context – online or physical/behavioural?

What sort of deception occur in the military domain?

What deception strategies do you consider liars use in their attempts to influence?

In your experience, which strategies are the more effective?

To what extent can personality, motivation and other factors affect the ability to deceive and the ability to detect deception?

How do you detect another person's lie?

Do you have any particular methods you employ?

What areas of verbal and nonverbal behaviour do you focus on in your attempt to detect another person's deception?

Are you usually successful in detecting deceit?

What current strategies of deception detection are currently used in your field?

Are there any improvements you think could be made to increase the effectiveness of the detection of deceit?

What potential future threats are there from potential adversary deception strategies?

Is it possible to increase the likelihood of detecting future threats and how could this be achieved?

Were you to be tasked with developing a model of deception in order to combat deception in military domains, what elements would you include?

Appendix 6.2: Interview Schedule – Interpersonal and Online Deception

This schedule contains questions that cover deception across the domains of interpersonal and online deception. The interview discussion will be tailored to the particular subject matter experts identified to participate in this research study.

The questions identified below are identified as the basis for a discussion with SMEs although it is acknowledged that there will be further questions that may be identified during the course of the discussion and therefore these will be included in the discussions as appropriate.

All participants will receive the initial brief before signing the consent form once they are content to continue the discussions. It will be identified that if there are areas of their work that are inappropriate to discuss within the remit of the interview, participants will be able to skip answering certain questions.

Interpersonal deception

Please give an overview of the work you conduct in relation to deception.

In your particular field, how do you define deception?

What do you think are the environments or domains that are most relevant when considering interpersonal deception?

If you could pass on one thing you have learned during you experience in the field of deception, what would it be?

What sort of lies do you consider people use in high-stake deception? Can you give examples of this?

What strategies do you believe that liars use in their attempts to influence people that they are telling the truth? (Include strategies related to verbal and nonverbal impression management, the concealment of emotions etc.).

Do you believe that a person's underlying personality can influence how they lie to others?

How does a liar's motivation impact on their ability to lie successfully?

Does psychopathy make for a good liar or for someone who lies indiscriminately and therefore is not as successful?

In which situations do / have you detect/ed deception? How do you personally detect another person's lie? (What areas of verbal and nonverbal behaviour do you focus on in your attempt to detect another person's deception?)

What current strategies of deception detection are currently used in your respective field? Do they work effectively?

Are there techniques that should be incorporated into the current approach to deception detection which would improve the methods currently used?
Do you think there are parallels from interpersonal deception that apply to the online environment? What situations are these?
If you were to develop a model of deception detection, what factors would you consider significant?
What do you think is the most significant contribution that has been made in the field of deception research / work?
How do we detect when someone is telling the truth? Is credibility a wholly behavioural or verbal presentation of information?

Online deception

In your field of work, how is online deception defined?
What do you class as the most significant challenges in the area of online deception?
Is it possible to develop strategies to detect deceit online? If so, in which areas?
In which circumstances does online deception occur?
(For example, deception may occur in online videos, in text-based computer-mediated communication incl. social networking sites, and in attempts at social engineering)
Are there examples of high stake deceptions that have occurred online?
Do these influence the ways that future deceptions occur?
How do you think such deceptions would manifest online?
What strategies do you believe that liars use in their attempts to influence online?
To what extent is it possible to gauge an individuals or groups personality online?
Can we ever truly know who we are interacting with?
Is online deception more likely to be successful when conducted online than interpersonally?
Are there strategies available to assist in the detection of deception online?
How do you think it is possible to improve the detection of deception in online interactions? Which types of online interactions would most benefit from this?
If you were tasked with developing a model of online deception, what would be the main factors you would class as significant to consider?
Is it possible to detect the truth or credibility when interacting online? How do people attribute credibility to particular sites or sources of information?

Appendix 6.3: SME Participant Information Sheet

Attitudes towards interpersonal and online deception and its detection

Participant Information Sheet

You are invited to take part in a research study investigating interpersonal and online deception and credibility assessment.

Before you decide whether to consent to participate, you need to understand why the research is being done and the nature of your involvement. Please read the following information carefully. Please ask if there is anything that you are not clear about and take time to decide whether or not you want to take part in the research.

What is the purpose of study?

The purpose of the research is to identify what is known about interpersonal and online deception and to develop a theoretical model from which to test certain deceptive actions and behaviours.

What would be involved for you?

You will be asked to discuss a series of questions related to interpersonal and/or online deception (Please see the attached interview schedule). The interviews will be recorded using an electronic Dictaphone, recorded data will be stored in a secure environment. You have the right to request that your recording be destroyed but this will only be until the date that the data is being written up for publication. This will be August 2012.

Do I have to take part?

It is up to you decide whether you would like to participate in the research. If you agree to be involved you will be interviewed about the field of deception and credibility assessment. We have attached a copy of the interview schedual so that you can see the types of questions that will be asked. However it is also possible that other questions will be asked depending on the nature of the interview discussions we have. If once you have read through the interview schedule, you have any questions, please contact the Principal Investigator, Iain Reid on the contact details below. We will then arrange for a time for the interview to take place and a location that is convenient to you. You are able to withdraw your participation from the research at any time and you do not have to answer all the questions if you choose not to.

What will I have to do to take part?

If you agree to take part in the study, you will be provided with a consent form and will be asked to read and sign this. The interview is expected to last no more than 2 hours depending on the nature of the discussions and your own availability.

Will my taking part in the study be kept confidential?

Your involvement in the interview research will only be known by the research team identified below. Your electronic data from the audio recording and the subsequent transcript will be stored on an Ironkey for 7 years unless you request for any reason to withdraw from the study. Your identity will be altered to a numerical code and this will be used to refer you individuals during the analysis of the research. Data will be confidential and raw data may only be viewed by the research team. No names or identifiable information will ever be used in publications resulting from the study.

What if I have any concerns or queries?
Please contact the Principal Investigator Iain Reid at ireid@lincoln.ac.uk or 01522887366
or Director of Studies: Dr Lynsey Gozna at lgozna@lincoln.ac.uk or 01522 837328
or Dr Julian Boon at boo@le.ac.uk or 01162231480

Thank you for taking the time to read this information.

Appendix 6.4: SME Consent Form.

Attitudes towards interpersonal and online deception and its detection.

Consent Form

I have read and understood the Participant Information sheet and understand the purpose, nature and duration of the research and what is expected of me. All my questions have been answered fully to my satisfaction.

I understand that if I decide at any time during the research that I no longer wish to participate in this project, I can notify the researchers involved and be withdrawn immediately without having to give a reason.

I understand that the information I have submitted will ultimately be published as a PhD manuscript, potentially as a journal article and other forms of reports. Please note that confidentiality and anonymity will be maintained and it will not be possible to identify you from any publications.

I consent to the processing of my personal information for the purposes of this research study. I understand that such information will be treated as strictly confidential and handled in accordance with the provisions of the Data Protection Act 1998.

I agree to volunteer as a participant for the study described in the information sheet and give full consent to the study including the audio recording of the interview.

Signed: ……

Name: …….

Witnessed by:…….

The information you provide will be used only for research purposes.

Thank you very much for your help.

If you would like any more information please contact Iain Reid

ireid@lincoln.ac.uk or 01522 887366

Appendix 6.5: SME Debrief Sheet

Verbal debrief of the attitudes towards interpersonal and online deception project

Thank you very much for agreeing to take part in the current research. This project seeks to develop a new model of deception through building on the work and experiences of SMEs in the areas of interpersonal and online deception. If you would like a summary of the findings once research has been completed please contact the Principal Investigator – Iain Reid at ireid@lincoln.ac.uk or 01522 887366

Appendix 6.6: SME Study Ethical Approval

Lincoln, 4-3-2012
Dear Iain Reid,
The Ethics Committee of the School of Psychology would like to inform you that your project titled "To identify what has been learned about the nature of interpersonal and online deception and associated credibility assessment based upon the knowledge and experience of academic Subject Matter Experts (SMEs) who are experts in the field of deception and influence" has been:

☒approved
☐approved subject to the following conditions:
☐ invited for resubmission, taking into account the following issues:
☐ is rejected. An appeal can be made to the Faculty Ethics Committee against this decision (cawalker@lincoln.ac.uk).
☐is referred to the Faculty Ethics Committee. You will automatically be contacted by the chair of the Faculty Ethics Committee about further procedures.

Yours sincerely,
Emile van der Zee, PhD
Chair of the Ethics Committee of the School of Psychology University of Lincoln, Department of Psychology Brayford Pool Lincoln LN6 7TS United Kingdom telephone: +44 (0)1522 886140 fax: +44 (0)1522 886026 e-mail: evanderzee@lincoln.ac.uk http://www.lincoln.ac.uk/psychology/staff/683.asp

Appendix 6.7: Phases of thematic analysis

Phase	Description of the process
1. Familiarizing yourself with your data:	Transcribing data (if necessary), reading and re-reading the data, noting down initial ideas.
2. Generating initial codes:	Coding interesting features of the data in a systematic fashion across the entire data set, collating data relevant to each code.
3. Searching for themes:	Collating codes into potential themes, gathering all data relevant to each potential theme.
4. Reviewing themes:	Checking if the themes work in relation to the coded extracts (Level 1) and the entire data set (Level 2), generating a thematic 'map' of the analysis.
5. Defining and naming themes:	Ongoing analysis to refine the specifics of each theme, and the overall story the analysis tells, generating clear definitions and names for each theme.
6. Producing the report:	The final opportunity for analysis. Selection of vivid, compelling extract examples, final analysis of selected extracts, relating back of the analysis to the research question and literature, producing a scholarly report of the analysis.

Source: adapted from Braun & Clarke (2006)

Appendix 6.8: Holistic Model of Deception Detection Framework

Deceiver	Intent	Deception Tactics	Interpretation	Target
Stakes **Impression Management** (Inc countermeasures) **Motivation** **Background History** (BH, inc individual differences, personality and culture) **Target Audience Analysis** **Planning Spontaneity** **Deceiver Vulnerabilities** (Emotional arousal,	**Behaviour** **Attitude** **Motive** (Greed – Envy – Power – Revenge)	**Context** (Inc triadic communication, communication changed online, anonymity, medium, Inhibitions Reduced Online, Reach, Scalability, Uncertainty Online, Richness, Hyperpersonal, manipulate attention, Manipulate Perception, Manipulate Emotion, Focus other/self, Timing) **Control of Information** (Increase Information (Inc increase details, white-out) and Decrease Information (Inc	**Source Attributes** (Consistency, plausibility, responsivity, credibility, prominence) **Risk** **Questioning/Interviewing Strategy (QIS)** **Detection Methods** (including Behavioural Baseline, Verbal Methods of Detection, Neuropsychological Techniques, Pictorial Techniques, Physiological Techniques,	**Decision-Making (DM)** (Inc Expectations, Cognition, Emotion and Suspicion) **Stakes** **Individual Differences (ID)** (Inc Internal/External Pressures, individual or group) **Motivation** **Capabilities and Resources** (inc Preparation and Experience)

cognitive load, decision-making biases)		Deflection, denying, fewer words (inc exclusive words), blocking, black-outs, concealing, Feigned forgetfulness) **Influencers** (Inc Emphasise to influence, Higher Authority (Appeals to higher authority to enhance credibility), fluency, authority, objectivity, positivity, referent power, attractive, convincing, commitment (inc tentative words), influence increases over time, social engineering, distraction, Deception Gambits;	Non-Verbal Methods of Detection, Paralinguistic Techniques, Military/Intelligence Methods of Detection, verfication) **Surveillance/ISTAR** (inc channel availability and evidence/case details)	

		Subtlety) **Replicating Genuine Behaviour** (Replicate Genuine Behaviour, Mimicking, Dummies, Kernel of Truth, Decoy, Speech Control (Slower Speech), Normality)		

Appendix 7.1: Interview Schedule – Cultural Similarities and Differences

Interpersonal:

How would you describe deception to someone?

Are you able to tell when someone is lying to you? How? Are there any particular things that people do or say when they lie that help you to detect deception?

If you think back to a situation when someone lied to you and you were able to identify this (either at the time or subsequently), what in hindsight gave them away? (Verbal, e.g. their story; non-verbal, e.g. body language)

Do you consider yourself to be skilled at detecting deception? Why do you think this is?

So moving on to consider the other side of deception, how do you tell when a person is telling you the truth? Do you think there are cues that help you to know when someone is credible?

What in particular do you think illustrates a truthful person? (Verbal, e.g. their story; non-verbal, e.g. body language)

Thinking about your own deceptive and truthful behaviour, are there any particular things you do to be perceived as truthful by others?

How do you think we know whether we can trust other people? Is this all about the believability of what people say and do or is it more than that?

When you meet someone for the first time, what impression would they have to give you in order to be considered trustworthy and honest? What behaviours or speech?

Now think about what makes a person untrustworthy and dishonest, how would someone present to you in order for you to make that decision about them? What are the characteristics you would be looking for?

Online:

In general, what do you use the internet for? (e.g. social networking, research for university, general information, music and video, gaming)

Do you think it is easy for people to be deceived on the internet? If yes, how so? How do you think this might happen? (e.g. email, websites, online reviews, shopping, credit card details…)

Have you ever needed to assess the credibility of sites when you are online? How have you gone about doing this? What do you think are the characteristics of a site when you might be a little suspicious?

How do you identify whether a site or a person is credible when you are using the internet? E.g. social networking, shopping

What in particular would you focus on?

How do we know when we can trust someone online? Do you think there are particular characteristics that help to identify this?

Have you ever been duped when using the internet? What happened and what was the outcome? Have you altered your online behaviour as a result of this?

How might people who use gaming sites or sites such as 'second life' deceive others? Do you think it is possible to be immune from this?

Are there methods we can use to protect ourselves from deceptive interaction online? What do you think these are?

If you were going to advise a parent about the risks that might be relevant for their children using the internet, what are some of the issues you might need to cover with them?

If you were going to deceive someone on the internet, what do you think would be the best methods to use?

How would you try to be credible?

Do you think there are differences in how we judge credibility online and offline?

If yes, how do you think these differences present in the two interactions?

Is there anything else you think is relevant when thinking about deception online and offline?

Appendix 7.2: Cross-Cultural Study Consent Form

I have read and understood the Participant Information sheet and understand the purpose, nature and duration of the research and what is expected of me. All my questions have been answered fully to my satisfaction.

I understand that if I decide at any time during the research that I no longer wish to participate in this project, I can notify the researchers involved and be withdrawn immediately without having to give a reason.

I consent to the processing of my personal information for the purposes of this research study. I understand that such information will be treated as strictly confidential and handled in accordance with the provisions of the Data Protection Act 1998.

I agree to volunteer as a participant for the study described in the information sheet and give full consent to the study including the audio recording of the interview.

Signed: ……

Name: …….

The information you provide will be used only for research purposes.

Thank you very much for your help.

If you would like any more information please contact your interviewer

Email: …….

Or contact the research supervisor, Iain Reid.

ireid@lincoln.ac.uk or 01522 837366

Appendix 7.3: Western Codebook

Theme	Code	Quotes
Non-Verbal Behaviour	Nervous Behaviour (inc fidgeting) Gaze Direction Eye Contact Body Language (inc non-verbal movement) Blink Rate Facial Expression/Emotions (inc anger, smiling, less smiling, blushing, less blushing) Posture Self-manipulators (inc hand manipulation)	"nervousness, like twiddling with your fingers or playing with your hair or looking off at funny angles" (W1: 7-8) "A combination of uh oxygenated blood in their face if they're Caucasian erm because their facial emotions show up" (W4: 14-15) "quite often like eye contact erm like if people look at the ground" (W5: 6-7)
Judgement and Biases	Truth Bias (inc trusting online) F2F Bias Experience (inc Naivety & Unaware) No rapid judgements Intuition 'Shifty' Behaviour	"No I don't think I am, I'm far too trusting. I'll believe anything anyone tells me" (W1: 24) "I don't really know if there's like certain signs that people give off, like what particular sign they give off that will, you know, set me off and say oh he's lying to me" (W2: 12-13) "it's instinctive it's you like or you dislike them" (W4: 137)
Verbal Behaviour	Verbal Content (inc short sentences) Paralinguistic (inc tone of voice, voice change, speech hesitancy, free-flowing speech, laughter) Enthusiasm	"you can t-sometimes tell by like if their voice wavers" (W5: 6) "the way they speak and what they speak about. Like it they start talking about other people" (W6: 45-46) "I think it was mostly sort of reluctance to give away more information than they needed to, sentences were short, they didn't elaborate on anything, like conversation didn't flow

		naturally" (W7: 21-22)
Consistency	Statement Consistency Behavioural Consistency Consistency Content Consistency Maintain Consistency Consistency Across Time	"more dramatasism put on it in like later, like later, like tellings of the story. So first of all, something tiny happened, and then the next time you hear the story it was more than that" (W1: 19-21) "With a person if it's on like facebook or twitter or something like you might go on their profile and see like erm if like they're information stacks up so I I've had people adding me on facebook and they've got no mutual friends and not many friends on facebook in general it just makes y'no you think well why are you adding me" (W5: 81-85) "if things just don't add up in what they write on their website" (W6: 58) "or if what they're saying not making sense or contradicting something they have previously said" (W11: 18-19)
Behavioural Baseline	Normality Familiarity Characteristics Past Behaviour Socialising Behavioural Baseline	"I think people who you know better and spend a lot of time with will be easier to detect deception or not through whether their behaviour is like out of character or whether they're acting differently but if you don't really know the person well (pause) I think it would be harder to identify whether they're lying or not" (W3: 7-11) "unless of course you know you're talking to a friend and you know that you're talking to that friend" (W1: 79-80)

		Erm, if I know the person, if I've known them for a while, then I may be able to tell at some point, but if I don't know the person, then I might not be able to tell straight away. So it takes time, in my opinion, to get to know someone and see if they're being deceptive or not (W2: 6-9) "Whether or not someone is trustworthy for me depends on what I know about the person, cause anyone can tell a believable story, but.. it's whether or not you know that what that person's like" (W6: 31-33)
Social Influence	Friendly Reviews Reciprocity Authority Allegiance Attraction Value Joking Reputation Persuasion	"just come across as quite friendly really" (W1: 45) "buying something on eBay and then just checking them out like from their previous reviews of how they've been, like how they've been with other people, treated them that kind of thing" (W1: 85-87) "you have to build trust with someone and offer them to trust you back" (W2: 228) "are they involved in anything any groups or societies or anything like that" (W4: 150-151) "I guess you try to do a bit of research and then you can look at like if it's a website you can look at like customer reviews but again, they can be faked" (W5: 80-81) "I'd say that's

		because…I…I…tell a lot of lies fo-f-f-for jokes, no'-not like not like dramatically, but like I-I-I tell a lot of lies in like in humour and stuff" (W9: 25-27)
Plausibility	Confidence Genuine (inc honesty) Plausible (inc Scepticism) Overcompensation Sly Sincerity Determination Shy Relaxed/Open Behaviour (appears truthful) Closed/Reserved Behaviour (appears deceptive)	"just like what they said was just very over the top. Erm the story wasn't very realistic in a way" (W5: 12-13) "If they're more truthful, they're more relaxed" (W6: 14) "I think when i've met people and they've really exaggerate a story, there is that sort of little voice in the back of my head saying "nah that's rubbish" (W7: 69-70)
Website Presentation	Presentation Credibility Appearance Professionalism	"if it didn't look very, like I want to say clean and together but that doesn't quite make sense for the internet. I don't know just like sort of well, well-presented and erm, so if it wasn't well-presented that would kind of make me think okay, this is a bit funny" (W1: 90-92) "A lot of advertisements err, you know, it just looks cheap because obviously my experiences with it, because I've done marketing you know, I know when a website is trustworthy or not because internet's a huge part of, you know, my course that I did. Erm, but yeah, I don't know, there'd be a lot of advertising for example things saying "you've won a million dollars" or something, you know, you just wouldn't believe it

		because you know it's leading to somewhere you don't want to go" (W2: 140-145) "but if I think that a site looks quite unprofessional or a bit dodgy then I'd be more inclined to stay away from it" (W5: 76-77) "Erm... and generally how it looks, you will see a big difference between someone making their own website and the BBC website, if it looks professional then its more trustworthy, though thats not always the case" (W7: 138-140)
Experience of Internet	Channels Media Richness Anonymity Easier Online Large-Scale Usage Less Cues online	"because you've not got the social interaction, like like for example earlier I said that you could like see it in, it's more a, you can't tell that on the internet 'cos there's no physical interaction" (W1: 74-76) "But erm yeah, I think the main reason is because there's no face-to-face interaction and you don't know what the other person's motives are, you know, because they're not in front of you so, you know, you can't judge by their body language and stuff like that" (W2: 114-117) "so people will read it in a way or tone of voice that their head chooses for it, without considering how the person typing it meant it to come across, so you instantly lose any sort of... mannerisms and other, sort of body language

		that might cause you to sort of, implications to seem suspect" (W7: 95-98) "I am if it's someone, if its face to face, so you can see what their saying but i'm not very good at it by like text or something" (W12: 15-16)
Verification	Source Background Checks Supporting Evidence Verifiability Check Facts Warrants False Warrants Multiple Sources Multiple Cues	"obviously on Amazon; a user rating, you know, their rating. So I'll have a look at how many things they've sold, you know, err if they've been on the website a lot, so I'll just check their rating, as far as shopping goes" (W2: 148-150) "they don't trust people they rely on documentary evidence and taking a lot of time to consider the evidence that that person has provided them with whether or not they can or cannot be trusted" (W4: 125-127) "and you should always be a bit weary because you don't know especially if if there's no webcam, you don't know if it's they are who they say they are" (W5: 90-92) "And if it's a person.. I would probably look at their pictures, look at their friends, do I do I know anybody that they're with do they look like they're the person that they actually are saying they are. Do the people in the pictures actually look like they know who that person is" (W6: 64-67)
Aversion of Risk	Restrict Access Supervision Maintain Privacy Risk	"If I was going to advise their parents, err, you can lock websites you know like; you can make sure on the

	Vulnerability Awareness of Risk Caution	computer, you know, that the person can't go on certain websites" (W2: 201-202) "um you know there's thousand people out there on the Internet not just in terms of um the you know the sexual um predators but also uh financial um predators uh organised crime etcetera etcetera there are lots of websites that aren't real websites that are there just to um extract your financial details" (W4: 177-181) "again I think goes on with like some people are more susceptible like they're more easy to deceive because they're more willing to help or believe people or fall for stuff" (W5- 64-66) "think it could go either way, got a 50% chance that it's them telling the truth and 50% of them not" (W6: 73-74)
Impression Management	Impression Management Appearance (inc Demeanour, appear genuine/trustful, natural appearance) Stick to Truth Avoid Extra Detail Be Subtle Change conversation Eloquent Emphasise (inc exaggeration, understate, repeat claims, highlight honesty) Over-Elaboration Rehearsability Rapport	"you're in to that um second life and they've got an avatar that's a you know blonde bl- busty blonde eighteen year old and they're a fifty year old bald male erm then um then they have a a personality profile that um they i- is more attuned to that age range eighteen year old girl that actually has a fifteen year old male for some fifty year old male for some reason" (W4: 240-245) "Erm, and also I don't just their overall mannerisms would be quite they'd just feel quite genuine and like I don't

		know the emotion in their voice would be er, yeah more genuine" (W5: 22-24) "by the way they talk and the way they try to come across to people that they're talking to, they might come across as trustworthy even though you know you might not necessarily see them in person" (W6: 87-89) "Well, facebook was an easy one 'cause I knew a lot of people that had it. I used just a picture of myself but it didn't reveal my face so you couldn't see who it was. And I also used pictures of animals and stuff 'cause a lot of people do put photos of animals on. And I requested people that I did know and people that I didn't know – it was quite surprising that a lot of people that I didn't know even accepted it, so they didn't have friends in common, it was just complete strangers. So, social media's a good way" (W15: 119-125) "Like there's not, nothing, I don't add anything extra for me to say yeah, like, for me, for me, to you know, say to people, "yeah believe me," like believe me. I'll just tell them a story and it's up to them whether they believe me or not" (W2: 69-71) "I might insist upon something being true and then play it off as, a sort of... a lack of knowledge perhaps on the other persons part, so i'd say like "yeah course it is like it

		just is" and then sort of move on as if it wasnt a big deal" (W7: 54-56) "sometimes like I say, I know like I go like 'Ah yeah I know totally I'm being honest'…like…like…I-I-I enforce my honesty, but I always-I always maintain that if I promise something…then…tha-tha-that is my word, so…I always try to have tha- a-a level of truth- a truth…that..tha- people know they can trust me" (W9: 46-50)
Response to Questioning	Question Type Emotional Reaction Unexpected Answer Engagement (inc avoidance) Response Unforthcoming Elaboration	"be prepared to talk to me if they erm erm run away from me or erm you know don't want to have an- avoid me in the street then I wouldn't be inclined to trust them with anything or talk to them about anything" (W4: 133-136) "even if they say something a little bit differently and then by questioning further it will probably start to unravel a bit" (W11: 12-13) "Also people who tell elaborate stories they go into too much detail and try too hard to make something believable" (W20: 19-21)

Appendix 7.4: Eastern Codebook

Theme	Code	Quotes
Behavioural Baseline	Behavioural Baseline Normal Behaviour Aggressive Behaviour Past History Familiarity	"know he likes to lie to me but mm but you know because I'm I'm so familiar with his know his habit his you know err facial expression because when he lies he like you know will show some y'kno- som- y'kno- smile and uh kno- the kind I don't know how ho- ho- it's kind of hard to describe it but some uhh some some facial expression which not easy to to to notice" (E2: 40-44) "It may be just through knowing them that you know their stories just not right" (E4: 9-10) "I think, you can't very, you can not tell if a stranger is lying you cannot judge a stranger, but if you know someone, then you can tell if they're always telling the truth or lying" (E5: 24-25) "If you know someone before then it is easier to see if there is a behaviour change before and after a lie is told" (E9: 5-6)
Non-Verbal Behaviour	Body Language Eye Contact Facial Expression Gaze Direction	"they try to avoid eye contact" (E2: 23) "the body language if he's lying, too much body language…will be…presented" (E3: 38-39) "probably their body language, was very negative so I picked up on that" (E5: 9)

		"they look away when they talk to you" (E9: 11-12) "I can identify that one well someone, I, I read some essays when you lie as well you look in the left but I not sure that people use some body language I not sure like the real thing when they are doing the body language where it is yes it is true! But it is not; hmm maybe it is true can identify" (E11: 27-30)
Verbal Behaviour	Paralinguistic (inc speed of talking, response latency, laughter) Verbal Content/Statement	"spee-the speed when they talking" (E3: 43) "some people laugh. I have a friend who laughs when she's lying" (E4: 14-15) "plus their story is very detailed" (E5: 16) "First of all I would listen to their word that's the first clues and I will be looking for because when they're talking if they're telling me sentence quite like stop each words well they say what they are thinking when they are talking it's like such a lie" (E11: 91-93)
Judgement and Biases	Intuition Experience (inc target knowledge & Unaware) Truth Bias (inc trust over doubt) First Impressions Expertise	"I think basically because I think I'm a person who tend to who tend to believe believe others" (E2: 57-58) "I think…err…most of the time in (main parts)…you believe" (E3: 34) "everyone lies, so, I don't know how you tell if someone's telling the truth"

		(E4: 37-38) "So, but i don't know how i actually see it but you just get the feeling that something's wrong, the intuition, the stomach feeling, telling you that something is not right" (E6: 10-11) "Yeah in my culture when someone is close to me so I, he say anything I can believe so, don't doubt" (E11: 111-112)
Consistency	Consistency Across Topics Consistency Across Time Consistency Detailed Story Statement Consistency Statement-Behaviour Consistency	"they are lying they first say something and realise they've to lie to and they will use another story to covered the first thing they say... that day when I can realise they are telling lies" (E7: 8-10) "But sometimes I notice if my friends was lying to me by you know you can't find it out at the spot but you can later" (E8: 25-26) "Their story was conflicting, erm, they kept going back on what they were saying and they were different things to different people as well" (E10: 11-12) "Usually if someone is a professional lying I cannot know that, but maybe after a while, because our memories are quite well, I can remember some sentence maybe after couple time, a week, someone say something the truth and I can remember the older one now and I will feel identify someone" (E11: 18-21)

		"The person who seems to deceive a lot, they tend to spread stories, different forms to different people. So if you're in a group and that person is trying to deceive everyone else, he/she will tell different stories to each and every member" (E12: 47-49)
Website Presentation	Website Credibility Presentation Professionalism	"I didn't check before when I…online…But I think if the website is fake there is very similar to the real…so just depends on the err…text and the…err…font, something like that" (E3: 57-59) "well if the website has so many adverts I normally avoid it" (E5: 52) "Well usually check some, for study I just check for detail in the news, and like professional website like Google search and like BBC I can believe but most time" (E11: 144-145)
Plausibility	Plausibility (inc suspicion) Overcompensation (inc overly loud) Skepticism Open/Relaxed Behaviour Closed Behaviour Sleaziness Ingratiating Confidence	"general knowledge how can you get a mobile for just 10 pounds or 20 pounds (pause) you know something like that" (E1: 63-65) "I think a person should be mmm optimistic and uh y'know who are who are willing to help others who mmm mm who behave what they said" (E2: 83-84) "but I think most of the time, the feeling if someone is…I can feel when someone is lying because they aren't confident" (E3: 12-13)

		"I think ...it dependent on how the person give you the feeling because sometimes when they say something very confidently .. so you think that should be difficult then you believe that they telling the truth" (E7: 32-34) "Just being friendly and open, and not trying to make up stories that are completely unbelievable" (E10: 29-30)
Avoidance of Risk	Risk Caution Restrict Access Avoid Risk Risky Behaviours Vulnerability	"otherwise games and normal internet they are quite fine because you cannot urm otherwise you know something is bad you don't get into" (E1: 117-119) "If he if he was to ask ask my personal information and uh you know something like my mobile phone number my email address my even my y'know credit card account y'know I wi- you know try to avoid it s- you know to stay away from them perhaps" (E2: 240-242) "think because you need to fill in too much information when-when on internet, just like shopping on the internet, so…many details, just-err…address, telephone number and your credit card details, those are easy to let…other people to get it" (E3: 50-53) "actually I think deception is going on more online because so many people use the internet, so talking to someone offline is better than

		talking to them online because you are less likely to be deceived" (E9: 95-97)
Social Influence	Famous Attitude Reviews/Recommendation Respect/Reputation Greed Attractive Caring Friendly (inc approachability) Joking	"I think if they show respect show respect to me and err they err I mean they easier to to be approached and uh you know this kind of person" (E2: 123-124) "Using sexy pictures" (E4: 32) "well err the websites I use, are often used by many others so, I listen to what they say about the website then if they tell me something is wrong then I don't use it. So mainly my friends tell me whether or not the website is good or not" (E5: 48-50) "online mostly depends on what websites you can use. I'd use specific websites that were recommended to me and look at online review" (E9: 76-77)
Experience of Internet	Media Richness Anonymity Large-Scale Usage	"people do not make up who they want to be as you cannot see them nor is there emotion in the words" (E5: 41-42) "kind of.. if I do online shopping then you will do the online shopping from the stores that you know instead of stores that are not actual stores.. or you going to some social network .....social networking that most people use and you think it should be trustworthy" (E7: 83-86) "Erm… probably being anonymous like that's the biggest thing, like making

		sure that people can't track where the information's come from" (E10: 80-81)
Impression Management	Appearance (inc Serious appearance, comfortable) Impression Management (inc self-control, positive/nice behaviour, avoidance, supply information, fluidity of conversation, editability)	"Just generally being nice to me" (E5: 28) "when you actually stand and talk to them and you realise that they are listening, and then next day not everybody knows what you talked about , they kinda kept it to themselves, and they remember what you say" (E6: 47-49) "presentation, as this is important to make a good first impression, so I would be polite and nice" (E9: 86-87) "Well in the group work they are always meeting together and writing very quickly notes and telling this is what we need to do each one so it's very professional like so I cannot doubt any word he say because we want to get a good mark so it is not doubt because we want to get higher mark so" (E11: 126-129) "when you're online you should concentrate upon expressing yourself graphically and by giving all the relevant information which is easily seen by the viewers" (E1: 137-139) "try to avoid my questions cannot give a direct or immediate answer to my questions you know" (E2: 31-32)

		"I think…if I need to tell someone the truth I will…I'll use some figure, do some research and then…tell them that is the truth because I have something to…prove that" (E3: 29-31) "Maybe by discussing and talking with each other and sharing the views on what you think" (E8: 30-31) "they do not directly talk to us, they might talk to someone else to indirectly tell you a message" (E9: 41-42)
Verification	Warrants Check Facts Multiple Sources 3rd Party Unreliable Sources	"so you may have some customers that have used that site or some kind of contacts so that you can go back and check at any time or someone you can talk to or something like that" (E1: 130-132) "compare with what I know compare with what I know with what he said and you know it's a comparison (this.)" (E2: 11-12) "I think…it's…the website…is…owned by some-some organisation, just like you need to buy something's…you wont go to the…things that is….no-not popular…most of the time you use the Morrison, Tesco, this one…because many people…know this store is real" (E3: 62-65) "I look at who's written it basically, and how many people have written it. If it's just one person then it's likely not to be credible, but

		if there's several of them it's a bit more trustworthy" (E4: 34-38) "Yeah I think it's easy but sometimes you've got non-reliable sources you have to be aware of" (E8: 61-62) "Yes, erm… my PayPal got hacked and it was from an email that I thought was from PayPal when it wasn't and so I opened it and they got into my account and so now I check where the e-mails come from" (E10: 63-65)

Appendix 8.1: Deception Assessment Real-Time Nexus (DARN)©2015

Deception Assessment Real-Time Nexus (DARN) ©2015

PRESENCE AND RELEVANCE OF RISK FACTORS

Determine the presence of risk factors to and during the most recent pattern of deceptive behaviour (Current vs. Previous), as well as their relevance to the development of future management strategies.

Context of Deception	**Coding**
C1: Context of Deception *This factor reflects the situational context in which deception occurs and how the specific elements of a situation and the motives of the actors involved lead to the form that deception takes.* **Previous:** **Current:**	Presence: Previous ☐ Y ☐ ? ☐ N Presence: Current ☐ Y ☐ ? ☐ N Relevance: Future

Future:	☐ Y ☐ ? ☐ N
C2: ISR Capabilities *This factor reflects UK and friendly skill, experience and capabilities in conducting Intelligence, Surveillance, and Reconnaissance. Risk is measured through ability to conduct ISR, for example, if there are good capabilities then potentially less risk.* **Previous:** **Current:** **Future:**	Presence: Previous ✓ **Y** ☐ ? ☐ N Presence: Current ✓ **Y** ☐ ? ☐ N Relevance: Future ✓ **Y** ☐ ? ☐ N
C3: Usual Behavioural Pattern *This factor reflects usual adversary behaviour, from which a judgement of risk can be made. For example, if the adversary usually conducts deception and/or influence operations then this would be considered high risk.* **Previous:**	Presence: Previous ✓ **Y** ☐ ? ☐ N

Current:

Presence: Current

☐ Y ✓ **?** ☐ N

Future:

Relevance: Future

✓ **Y** ☐ ? ☐ N

C4: Suspicious Behaviour

This factor reflects suspicious behaviour identified in the adversary, and/or changes in usual adversary behaviour that may be deemed as suspicious and may indicate deception and/or influence operations are being conducted. Such behaviour requires further analysis to confirm or disconfirm the presence of deception.

Previous:

Presence: Previous

☐ Y ✓ **?** ☐ N

Current:

Presence: Current

☐ Y ☐ ? ✓ **N**

Future:

Relevance: Future

✓ **Y** ☐ ? ☐ N

C5: Acute Change in Behaviour *This factor reflects acute changes in adversary behaviour compared to their usual behavioural patterns. Such changes in behaviour may be deemed high risk and a full risk assessment should be conducted to ascertain the presence of deception.* **Previous:** **Current:** **Future:**	Presence: Previous ✓ **Y** ☐ ? ☐ N Presence: Current ✓ **Y** ☐ ? ☐ N Relevance: Future ✓ **Y** ☐ ? ☐ N
Evidence and Intelligence developed from ISR	**Coding**
E1: Human Intelligence *This factor reflects information recovered from any human source, whether they are an adversary, friendly or neutral. Intelligence is retrieved through observation and/or direct interaction with individuals or groups. However, care needs to be taken when assessing HUMINT to ensure the credibility of the intelligence.*	Presence: Previous ✓ **Y** ☐ ? ☐ N

Previous:

Current:

Future:

Presence: Current
✓ Y ☐ ? ☐ N

Relevance: Future
✓ Y ☐ ? ☐ N

E2: Open Source Intelligence

This factor reflects any intelligence that can be derived from sources open to the public, for example, public records, online publications and news channels.

Previous:

Current:

Future:

Presence: Previous
✓ Y ☐ ? ☐ N

Presence: Current
✓ Y ☐ ? ☐ N

Relevance: Future
✓ Y ☐ ? ☐ N

E3: Social Media Intelligence

This factor reflects any intelligence that is available through social media, for example, Facebook pages, or Twitter feeds.

Previous:

Presence: Previous
✓ **Y** ☐ ? ☐ N

Current:

Presence: Current
✓ **Y** ☐ ? ☐ N

Future:

Relevance: Future
✓ **Y** ☐ ? ☐ N

E4: Communications Intelligence

This factor reflects and intelligence recovered from electronic communication means and its appearance will reflect the medium selected for communication.

Previous:

Presence: Previous
✓ **Y** ☐ ? ☐ N

Current:

Presence: Current
✓ **Y** ☐ ? ☐ N

Future:

	Relevance: Future ✓ **Y** ☐ ? ☐ N
Situation Expertise	**Coding**
S1: Situation Expertise *This factor reflects the requirement for context-dependent expertise to aid in the interpretation of evidence and to judge the credibility of information available.* **Previous:** **Current:** **Future:**	Presence: Previous ☐ Y ✓ **?** ☐ N Presence: Current ☐ Y ☐ ? ✓ **N** Relevance: Future ☐ Y ✓ **?** ☐ N
Interpretation of Expertise	**Coding**

I1: Consistency of Evidence

This factor reflects the consistency of evidence available for analysis. When evidence is not consistent across multiple sources or lacks consistency when responding to questioning in investigative interviews risk is increased.

Previous:

Presence: Previous
☐ Y ✓ ? ☐ N

Current:

Presence: Current
☐ Y ☐ ? ✓ N

Future:

Relevance: Future
☐ Y ✓ ? ☐ N

I2: Plausibility of Evidence

This factor reflects the plausibility of evidence. Judgements of plausibility may depend upon expert advice about evidence, and may be used to assess the credibility of evidence.

Previous:

Presence: Previous
☐ Y ✓ ? ☐ N

Current:

Presence: Current
☐ Y ☐ ? ✓

Future:	N Relevance: Future ☐ Y ✓ ? ☐ N
I3: Implicit Belief *This factor reflects implicit beliefs and suspicion that adversaries may be conducting deception operations against friendly forces. Scepticism of adversary behaviour will also lead to doubt regarding adversary behaviour and how credible their aims are.* **Previous:** **Current:** **Future:**	Presence: Previous ☐ Y ✓ ? ☐ N Presence: Current ☐ Y ☐ ? ✓ N Relevance: Future ☐ Y ✓ ? ☐ N

Appendix 8.2: Forms of Intelligence

-Acoustic Intelligence: Acoustic Intelligence (ACINT) is defined as 'Intelligence derived from the collection and processing of acoustic phenomena' (AAP-6).

-Human Intelligence: HUMINT is defined as 'A category of intelligence derived from information collected and provided by human sources' (AAP-6).

-Imagery Intelligence: IMINT is defined as 'Intelligence derived from imagery acquired by photographic, radar, electro-optical, infra-red, thermal and multi spectral sensors, which can be ground-based, seaborne or carried by overhead platforms' (AAP-6).

-Measurement and Signature Intelligence: Measurement and Signature Intelligence (MASINT) is defined as 'Scientific and technical intelligence information obtained by quantitative and qualitative analysis of data (metric, spatial, wavelength, time dependence, modulation, plasma and hydro magnetic) derived from specific technical sensors for the purpose of identifying specific features associated with the source, emitter or sender and to facilitate subsequent identification and/or measurement of the sender and to facilitate subsequent identification and/or measurement of the same' (US DoD).

-Open Source Intelligence: Open Source Intelligence (OPSINT) is intelligence based on information collected from sources open to the public, such as the media, radio, television and newspapers, state propaganda, learned journals and technical papers the internet, technical manuals and books, to name but a few.

-Radar Intelligence: Radar Intelligence (RADINT) is intelligence derived from data collected by radar (US DoD).

-Signals Intelligence: Signals Intelligence (SIGINT) is the generic term used to describe all intelligence derived from the Electro-Magnetic Spectrum (EMS). It is divided into:

1. Communications Intelligence: Communications Intelligence (COMINT) is defined as 'Intelligence derived from electro-magnetic communications and communications systems by those who are not the intended recipients of the information' (AAP-6).
2. Electronic Intelligence: Electronic Intelligence (ELINT) is defined as 'Intelligence derived from electro-magnetic non-communication transmissions by those who are not the intended recipients of the information (AAP-6).

-Technical Intelligence: Technical Intelligence is defined as 'Intelligence concerning foreign technological developments and the performance and operational capabilities of foreign material, which have or may eventually have a practical application for military purposes' (AAP-6).

Adapted from Henderson and Pascual (2008)

Appendix 8.3: Deception Risk Assessment Technique©2015

Deception Risk Assessment Technique (DRAT)©2015

PRESENCE AND RELEVANCE OF RISK FACTORS

Determine the presence of risk factors to and during the most recent pattern of deceptive behaviour, as well as their relevance to the development of future management strategies.

Context of Deception *This section examines the situation in which deception occurs, and how situational elements and actors involved leads to deception*	**Coding** 0 = Absent 1 = Possibility/Low Level Presence 2 = Clearly Present
C1: Situation *This factor reflects upon what the current situation is, what has led to this current situation occurring at this moment in time, and what are the distinguishable elements from the situation which are cause for concern.*	
Current:	Presence: Current ✓ **0** ☐ 1 ☐ 2 Relevance: Current

✓ **0** ☐ 1 ☐ 2

C2: Actors

This factor reflects who the actors are in the current situation: can we identify these actors successfully? Are there multiple actors involved? Who are the key actors? Who, if any, are the subsidiary actors? Are the actors involved individuals, groups or larger organisations? In in-real-life interactions identifying actors may prove challenging if they seek to conceal their identity (e.g. removing military insignia – Ukraine). Online interactions are often characterised by anonymity where identifying actors may prove challenging, and discernible behavioural patterns may be overgeneralised to the actor involved, creating a potentially unreliable profile of the actor.

Presence: Current

✓ **0** ☐ 1 ☐ 2

Current:

Relevance: Current

✓ **0** ☐ 1 ☐ 2

C3: Current Threats

This factor reflects what the current threats of the situation are, whether these threats are obvious, concealed or 'ghost' threats designed to waste resources, which area the threat/s is/are emerging from, and which areas of infrastructure these threats are targeting.

Presence: Current

Current:	✓ **0** ☐ 1 ☐ 2 Relevance: Current ✓ **0** ☐ 1 ☐ 2
C4: Communication Medium *This factor reflects the communication medium the deception occurs in. Communication mediums include both online and in-real-life domains. Within the in-real-life domain communication may be verbal, vocal, non-verbal (focussing on body language) and physical acts of deception. Within the online domain communication may be verbal, vocal and non-verbal (focussing on body language) and physical acts of deception, across an array of communication mediums (Instant Messaging, email, blogs, video chats, social media networks and deceptive websites).* **Current:**	Presence: Current ✓ **0** ☐ 1 ☐ 2 Relevance: Current ✓ **0** ☐ 1 ☐ 2
C5: Online Communication Characteristics *This factor reflects the specific characteristics of online communication where interactions may range from a user interacting with online content where there is no reciprocal*	

communication (e.g. a website, or blog), to interactions where there is reciprocal communication (e.g. email, or Twitter). Online communication is characterised by its ability to cost-effectively reach large-scale audiences in a shorter period of time than traditional communication formats. The anonymity of communicating online may also lead to online disinhibition where individuals may be more likely to disclose information that they would not do so in-real-life, presenting an area for exploitation by deceivers.

Current:

Presence: Current

✓ **0** ☐ 1 ☐ 2

Relevance: Current

✓ **0** ☐ 1 ☐ 2

C6: In-Real-Life Communication Characteristics

This factor reflects the specific characteristics of in-real-life communication in interpersonal interactions. These interactions can be within informal or formal settings and context will affect the characteristics of these interactions. First impressions often guide our interpretation of our interactional partner and form our initial judgements of them, we further adapt and respond to the interactional partner during conversation and can be influence by rapport, and the presentation and confidence of the other person.

Current:

Presence: Current

✓ **0** ☐ 1 ☐ 2

Relevance: Current

✓ **0** ☐ 1 ☐ 2

History **Coding**

This section examines previous behaviour and interactions to develop a profile of usual adversary behaviour, enabling the identification of non-normal behaviour which may indicate deception

H1: Previous Behaviour – Non-Deceptive

This factor reflects the previous behaviour of the identified adversaries which is not related to deception. Identifying key goals that the adversary has achieved without using deception enables us to understand the non-deceptive strategies that have been used to achieve these goals. Subsequently developing a baseline of adversary non-deceptive strategic behaviour, enabling us to identify deviations in behaviour that may indicate deception; although it is important to establish that deviations in behaviour do not have another cause.

Current:

Presence: Current

✓ **0** ☐ 1 ☐ 2

Relevance: Current

✓ **0** ☐ 1 ☐ 2

H2: Previous Deceiver Interactions - UK

This factor reflects the past interactions that the deceiver has had with UK individuals, groups, organisations and infrastructure. Identifying and analysing previous known successful and unsuccessful deception attempts towards the UK will enable us to develop an understanding of how the adversary conducts and deploys deception strategies against the UK, enabling us to mitigate the risks of these attempts.

N.B. The deceiver may not use the same strategy multiple times against the UK

Presence: Current

✓ **0** ☐ 1 ☐ 2

Current:

Relevance: Current

✓ **0** ☐ 1 ☐ 2

H3: Previous Deceiver Interactions - Others

This factor reflects the past interactions that the deceiver has had with other individuals, groups, organisations and nations which are not related to the UK. Identifying and analysing previous known deception attempts, whether successful or unsuccessful, by the adversary towards others may enable friendly capabilities to understand how the adversary conducts deception and identify key strategies they have previously used.

N.B. The deceiver may not use the same strategy multiple times across different targets

Current:	Presence: Current ✓ **0** ☐ 1 ☐ 2 Relevance: Current ✓ **0** ☐ 1 ☐ 2
Nature of Deception *This section reflects the different strategies used to deceive others – For further guidance see research by Henderson et al. on Deception Gambits, Vrij (2008), and Whaley (2007)*	**Coding**
N1: Create and Identify Vulnerability and Exploit *This factor reflects strategies used in deception which seek to create and/or identify vulnerabilities in the target and then exploit these vulnerabilities for gain. Strategies include the following:* - *Ruses – This item reflects the intentional exposure of information to the target with the intention of misdirecting them, enabling the deceiver to exploit the adversary whilst their attention is directed towards the ruse (e.g. feeding misinformation to double-agents). Ruses can be conducted by the adversary across multiple levels of communication, whether through in-real-life interactions, through print media, TV, digital media, and other forms of online communication, potentially opening up a*	Presence: Current ✓ **0** ☐ 1 ☐ 2 Relevance: Current ✓ **0** ☐ 1 ☐ 2

wide area for this deception to occur in and requiring a wide-range of resources to target this threat.	Presence: Current ✓ **0** ☐ 1 ☐ 2 Relevance: Current ✓ **0** ☐ 1 ☐ 2
- *Exploitation of target audience fears – This item reflects the deceiver deliberately identifying and targeting target audience fears through deception, meaning the target will be more likely to spend resources responding to this perceived threat, whilst the deceiver then exploits another area.*	Presence: Current ✓ **0** ☐ 1 ☐ 2 Relevance: Current ✓ **0** ☐ 1 ☐ 2
- *Exploitation of target audience hopes – This item reflects the adversary targeting audience and exploiting their hopes as part of their deception operation (e.g. attack when claiming peace).*	Presence: Current ✓ **0** ☐ 1 ☐ 2 Relevance: Current ✓ **0** ☐ 1 ☐ 2
- *Decoys – This item reflects how a deceiver may use a decoy to portray a false target, which the deceiver wants the receiver to believe as credible before they then attack or respond to the dummy, wasting friendly resources and enabling exploitation by the deceiver.*	Presence: Current ✓ **0** ☐ 1 ☐ 2 Relevance: Current ✓ **0** ☐ 1 ☐ 2
- *Feints – This item reflects mock attack or simulation of an attack by an adversary which seeks to create the appearance of an imminent attack, thus tying down friendly resources to countering the implied threat, whilst the adversary may actually perform*	Presence: Current ✓ **0** ☐ 1 ☐ 2 Relevance: Current ✓ **0** ☐ 1 ☐ 2

other behaviour.

- *Demonstrations – This item reflects a real attack by the adversary which seeks to tie down friendly capabilities in active engagement in one situation whilst other adversary capabilities exploit the target in other areas. This strategy may prove costly to adversary resources as well as demonstrations in physical combat often increase number of casualties, however, this may be affect by adversary beliefs (e.g. if a soldier dies in combat he becomes a martyr and goes to heaven).*

Current:

N2: Conditioning the Target

This risk factor reflects strategies which involve conditioning the target into expecting a specific behavioural pattern by the deceiver.

- *Conditioning – This item reflects the deceiver conditioning the adversary into expecting a certain pattern of behaviour over the course of a period time, which then leaves the target open to exploitation when the deceiver performs a different behaviour (e.g. Soviet-Czechoslovakia Campaign 1968 and the Yom Kippur War 1973).*

Presence: Current

✓ **0** ☐ 1 ☐ 2

Relevance: Current

✓ **0** ☐ 1 ☐ 2

Presence: Current

- *Drip-Drip-Feed – Through slowly releasing information to a target, target resources may become focussed on this information, particularly if the adversary feeds truthful information to the target to build trust, before the adversary then presents the target with false information they have worked hard to uncover leading to a less accurate assessment of that information and leaving the target more vulnerable to deception.*

- *Influence increase over time – This item reflects how we are more likely to find an individual credible if we are interacting and developing trust with them over a period of time before they then engage in deception.*

✓ **0** ☐ 1 ☐ 2
Relevance: Current
✓ **0** ☐ 1 ☐ 2

Presence: Current
✓ **0** ☐ 1 ☐ 2
Relevance: Current
✓ **0** ☐ 1 ☐ 2

Current:

N3: Impression Management

This risk factor reflects the strategies that individuals engage in order to convince others that they are telling the truth. Individuals may engage in controlling their verbal behaviour (e.g. through keeping statements short to avoid contradictions) and their non-verbal behaviour (e.g. reducing body movements to avoid appearances of nervousness). Impression management occurs both in-real-life and online domains.

Presence: Current
✓ **0** ☐ 1 ☐ 2
Relevance: Current
✓ **0** ☐ 1 ☐ 2

Current:

N4: Control of Information

This risk factor reflects how information is controlled by the deceiver, where the deceiver may increase or decrease or alter the amount of information the target receives to increase ambiguity and cognitive load in the target. Strategies include the following:

- *Increase Information - An increase in information (also known as white-out) by the deceiver reduces the amount of resources the target needs to accurately assess information increasing the risk of not identifying key threats.*

Presence: Current
✓ **0** ☐ 1 ☐ 2
Relevance: Current
✓ **0** ☐ 1 ☐ 2

- *Decrease Information - A decrease in information (also known as black-out) by the deceiver the amount of resources the target needs to accurately assess information with risk increased through an inability to identify threats.*

Presence: Current
✓ **0** ☐ 1 ☐ 2
Relevance: Current
✓ **0** ☐ 1 ☐ 2

- *Deflection – Through deflecting the target towards information and details irrelevant to the deception operation the adversary increases the amount of resources the target requires to monitor threats, whilst distracting the target from the adversary's real intentions.*

Presence: Current
✓ **0** ☐ 1 ☐ 2
Relevance: Current
✓ **0** ☐ 1 ☐ 2

Presence: Current
✓ **0** ☐ 1 ☐ 2
Relevance: Current

- *Blocking – Through blocking the target's ability to assess information there is an increase in ambiguity about the adversary's actual aims.*	✓ **0** ☐ 1 ☐ 2 Presence: Current ✓ **0** ☐ 1 ☐ 2 Relevance: Current ✓ **0** ☐ 1 ☐ 2
- *Feigning forgetfulness – Through feigning forgetfulness the deceiver reduces the target's ability to uncover information in in-real-life and online encounters reducing the target's ability to detect deception and increasing ambiguity about reality.*	Presence: Current ✓ **0** ☐ 1 ☐ 2 Relevance: Current ✓ **0** ☐ 1 ☐ 2
- *Kernel of Truth – This item refers to the principle of developing deception operations around truthful information creating ambiguity for the target to accurately separate fact from fiction.*	Presence: Current ✓ **0** ☐ 1 ☐ 2 Relevance: Current ✓ **0** ☐ 1 ☐ 2
- *What is not being said – This item reflects examining what the current information does not show, as the deceiver may be stating one thing however their past history may indicate they mean something else.*	Presence: Current ✓ **0** ☐ 1 ☐ 2 Relevance: Current ✓ **0** ☐ 1 ☐ 2
- *Keep the Message Simple – This item reflects a common strategy amongst deceivers of keeping the deceptive message simple, which is harder to examine for inconsistencies.*	Presence: Current ✓ **0** ☐ 1 ☐ 2 Relevance: Current ✓ **0** ☐ 1 ☐ 2

- *Concealment/Camouflage – This item reflects the controlling of information through reducing the target's access to that information through concealing or camouflaging the information, whether this is an in-real-life encounter in combat operations or assessing online material for concealed messages.*

Presence: Current
✓ **0** ☐ 1 ☐ 2
Relevance: Current
✓ **0** ☐ 1 ☐ 2

- *Dazzle – This item reflects a strategy where the deceiver increases ambiguity in the target by overloading their cognitive abilities or sensors with unimportant information or noise.*

Presence: Current
✓ **0** ☐ 1 ☐ 2
Relevance: Current
✓ **0** ☐ 1 ☐ 2

- *Distractors – This item reflects a strategy where the deceiver uses distraction methods to divert the target's attention away from the deception at hand. This can include the deliberate targeting of emotionally salient issues which will focus the target's attention.*

Current:

N5: Credibility Enhancers

This risk factor reflects tactics that the deceiver may use to enhance their own credibility and/or the credibility of the information that they are employing to deceive the target. These strategies include:

- *Fluency – Through ensuring fluency in behaviour the adversary may appear more credible to the target as their no inconsistencies that may indicate deception.*

Presence: Current
✓ **0** ☐ 1 ☐ 2
Relevance: Current
✓ **0** ☐ 1 ☐ 2

- *Positivity – This item reflects that when a deceiver is positive in their behaviour, particularly verbal behaviour, they are more likely to be judged as credible by their target.*

Presence: Current
✓ **0** ☐ 1 ☐ 2
Relevance: Current
✓ **0** ☐ 1 ☐ 2

- *Objectivity – This item reflects that when an individual or organisation shows objectivity and appears neutral in their behaviour they will be more likely viewed as credible by the target, the adversary will then be able to exploit the target.*

Presence: Current
✓ **0** ☐ 1 ☐ 2
Relevance: Current
✓ **0** ☐ 1 ☐ 2

- *Commitment – This item reflects how an individual or organisation is viewed as credible if they are committed to their behaviour. Particularly in verbal behaviour if they are committed in their statement or information they provide and do not appear tentative or hesitant they will be more likely to be viewed as credible, even if this*

Presence: Current

information is false.

✓ **0** ☐ 1 ☐ 2
Relevance: Current
✓ **0** ☐ 1 ☐ 2

- *Convincing – This item reflects how individuals are more likely to believe an individual if they are perceived as appearing convincing, opening up the potential for exploitation by the deceiver.*

Presence: Current
✓ **0** ☐ 1 ☐ 2
Relevance: Current
✓ **0** ☐ 1 ☐ 2

- *Emphasise to influence – This item reflects how deceivers are likely to place emphasis on key points to influence how the target perceives information. Through placing consistent emphasis on particular aspects of behaviour there is a greater chance that the target will focus on these areas enabling exploitation of other areas by the adversary.*

Presence: Current
✓ **0** ☐ 1 ☐ 2
Relevance: Current
✓ **0** ☐ 1 ☐ 2

- *Too good to be true – This item reflects how deceivers may frame information in a manner that the target finds hard to believe, increasing ambiguity for the target and requiring further resources to assess credibility.*

Presence: Current
✓ **0** ☐ 1 ☐ 2
Relevance: Current
✓ **0** ☐ 1 ☐ 2

- *Showing the real as false – This item reflects how the adversary may show the target*

Presence: Current

real information (whether physical or verbal) to add credibility to false information it is hiding, drawing the target's attention away from other information (e.g. Operation Bagration where Soviet forces used real combat planes and aircraft guns to protect dummy equipment drawing the attention of German forces, whilst concealing their true invasion plans).

✓ **0** ☐ 1 ☐ 2

Relevance: Current

✓ **0** ☐ 1 ☐ 2

Presence: Current

✓ **0** ☐ 1 ☐ 2

Relevance: Current

✓ **0** ☐ 1 ☐ 2

- *Subtlety – This item reflects how the subtle presentation of information may manipulate the target into believing information that is false, or to focussing the target towards irrelevant information.*

Presence: Current

✓ **0** ☐ 1 ☐ 2

Relevance: Current

✓ **0** ☐ 1 ☐ 2

- *Mimicry – This item reflects how mimicry aims to make one thing appear as something else, this exploiting the target's erroneous belief. Mimicry can take many forms across the physical, verbal, non-verbal and online domains.*

- *Dummies – This item reflects objects that are used as false representations of reality which seek to affect how the target interprets information and constructs reality.*

Current:

N6: Social Influencers

This risk factor reflects strategies from social influence approaches which are likely to influence the target into accepting the deceiver and/or information as credible. Social influence strategies include:

Presence: Current
✓ **0** ☐ 1 ☐ 2
Relevance: Current
✓ **0** ☐ 1 ☐ 2

- *Higher Authority – Through appealing to a higher authority (e.g. God) a deceiver may enhance their credibility to others. This strategy will be more relevant to in-real-life and online communication. Malign appeals to higher authority can be used as permission giving strategies for justification of action.*

Presence: Current
✓ **0** ☐ 1 ☐ 2
Relevance: Current
✓ **0** ☐ 1 ☐ 2

- *Authority – This item reflects the fact that figures of authority are judged more persuasive and credible by others, potentially increasing the susceptibility to deception from perceived authority figures.*

Presence: Current
✓ **0** ☐ 1 ☐ 2
Relevance: Current
✓ **0** ☐ 1 ☐ 2

- *Referent Power – This item reflects the fact that individuals may be more likely to accept information that has been presented to them by another person they deem credible.*

Presence: Current
✓ **0** ☐ 1 ☐ 2
Relevance: Current

✓ **0** ☐ 1 ☐ 2

- *Attractive – This item reflects that individuals are more likely to find credible people that are attractive.*

Presence: Current
✓ **0** ☐ 1 ☐ 2
Relevance: Current
✓ **0** ☐ 1 ☐ 2

- *Reciprocation – This item reflects that individuals are likely to be influenced when they have been given something, as they then want to give something in return, which may leave the target open to exploitation by the deceiver.*

Presence: Current
✓ **0** ☐ 1 ☐ 2
Relevance: Current
✓ **0** ☐ 1 ☐ 2

- *Social Proof – This item reflects how we deem information correct through how others also judge that information.*

Presence: Current
✓ **0** ☐ 1 ☐ 2
Relevance: Current
✓ **0** ☐ 1 ☐ 2

- *Scarcity – This item reflects that individuals are more likely to be influenced by information that is scarce – potentially as we have had to deploy greater resources to uncover this information.*

Presence: Current
✓ **0** ☐ 1 ☐ 2
Relevance: Current
✓ **0** ☐ 1 ☐ 2

- *Humour – This item reflects that individuals are more likely to be influenced by information that they may find funny. Individuals may use self-denigration or denigration by others as humour to achieve a tactical or strategic advantage.*

Current:	
Deceiver Risk Factors	**Coding**
D1: Deception Doctrine *This risk factor reflects the adversary's deception doctrine, including official and unofficial manuals. Does the adversary have deception as part of their military and intelligence doctrine? Under what conditions does the adversary doctrine allow deception to be conducted?* *This risk factor is focussed towards identifiable groups and organisations that have guidelines for deception operations, individuals and non-state actors may not have cohesive guidelines for using deception, or they may conduct deception tactically rather than strategically, therefore, further monitoring of any suspicious activity is required.* **Current:**	Presence: Current ✓ **0** ☐ 1 ☐ 2 Relevance: Current ✓ **0** ☐ 1 ☐ 2
D2: Gains Vs Losses	Presence: Current ✓ **0** ☐ 1 ☐ 2

This risk factor reflects the stakes of the situation for the deceiver and what they may have to gain through deception or lose if they are caught in their deceit. The possibility of deception may be correlated between the levels of gains versus the level of benefits, for example, if there is potential for large gains and low costs then deception should be anticipated, whilst if there is potential for low gains and high costs then the adversary may not conduct deception. However, this may be mitigated by how the adversary portrays the gains and costs involved and what is deemed excessive.

Relevance: Current
✓ **0** ☐ 1 ☐ 2

Current:

D3: Motivation

This risk factor reflects how motivated the deceiver is to convince others that they are credible. Motivation may affect a deceiver's behaviour in the selection of strategies and length of time spent planning an act of deception. Motivation has also been found to increase the success of deception in online environments, where it is often challenging to assess the credibility of information.

Presence: Current
✓ **0** ☐ 1 ☐ 2
Relevance: Current
✓ **0** ☐ 1 ☐ 2

Current:

D4: Capabilities, Resources and Experience

This risk factor reflects the adversary's capabilities, resources and experience in conducting deception. Adversary capabilities and resources alongside previous experience will affect how credible and convincing the deceiver can be to the target across different communication modes. The deceiver's capabilities, resources and experience will affect their ability to utilise different communication modes and the strategies they use to target and appear credible to others.

Presence: Current
✓ **0** ☐ 1 ☐ 2
Relevance: Current
✓ **0** ☐ 1 ☐ 2

Current:

D5: Deception Spontaneity → Planned

This factor reflects how the deception is constructed, whether the deception is spontaneous or planned and how far along this continuum the deception may be. Spontaneous deception may have different characteristics and associated behaviours to planned and rehearsed acts of deception.

Presence: Current
✓ **0** ☐ 1 ☐ 2
Relevance: Current
✓ **0** ☐ 1 ☐ 2

Current:

D6: Cognitive Performance

This risk factor reflects the deceiver's ability to engage in cognitively challenging behaviours. Deception is argued to be a cognitively demanding task where individual's need to construct a plausible deception and maintain their account whilst controlling their own behaviour and responding to interactions with the target. If the deceiver is not able to engage in multiple demanding cognitive tasks, behavioural cues to deception may become apparent to observers.

Presence: Current
✓ **0** ☐ 1 ☐ 2
Relevance: Current
✓ **0** ☐ 1 ☐ 2

Current:

D7: Language

This risk factor reflects the language which the deceiver uses to communicate in. Language differences may present additional challenges to receivers of information through mistranslation or misunderstanding of challenging information, and proceeding difficulties of interviewing individuals to enhance behavioural cues to deception in interactions.

Presence: Current
✓ **0** ☐ 1 ☐ 2
Relevance: Current
✓ **0** ☐ 1 ☐ 2

Current:

D8: Personality and Individual Differences

This risk factor reflects the effects that personality (normative Vs disordered – the Dark

Tetrad of psychopathy, narcissism, Machiavellianism, and sadism) and individual differences (including demographics) have on an individual's actions in online and real-life environments, the forms of deception in which they may choose to engage in, and their ability to deceive others. - *Normal Personality*	Presence: Current ✓ **0** ☐ 1 ☐ 2 Relevance: Current ✓ **0** ☐ 1 ☐ 2
The Dark Tetrad consists of the following personalities all of which will present additional challenges when seeking to assess credibility. - *Psychopathy is characterised by individuals who lack conscience, are often deceptive and impulsive in their behaviours without regarding the consequences of their actions*	Presence: Current ✓ **0** ☐ 1 ☐ 2 Relevance: Current ✓ **0** ☐ 1 ☐ 2
- *Narcissism is characterised by individuals who seek importance and wish to be viewed this way by others*	Presence: Current ✓ **0** ☐ 1 ☐ 2 Relevance: Current ✓ **0** ☐ 1 ☐ 2
- *Machiavellianism is characterised by individuals who constantly seek to manipulate you for their own gain*	Presence: Current ✓ **0** ☐ 1 ☐ 2 Relevance: Current ✓ **0** ☐ 1 ☐ 2

- *Sadism is characterised by individuals who seek to physically or verbally hurt for their own gain*

Current:

D9: Belief System

This risk factor reflects an individual's or group's belief system including their culture, religion and their political beliefs and allegiances with others. The deceiver's belief system will influence how they interpret the world, their interactions with others and will shape the motive and context from which deception emerges.

Presence: Current
✓ **0** ☐ 1 ☐ 2
Relevance: Current
✓ **0** ☐ 1 ☐ 2

Current:

Target Vulnerability Factors	**Coding**

T1: Who is the target?

This vulnerability factor reflects identifying who the target is – whether the target is an

Presence: Current
✓ **0** ☐ 1 ☐ 2

individual, group, or organisation and whether the target is a decision-maker or the general public. **Current:**	Relevance: Current ✓ **0** ☐ 1 ☐ 2
T2: Stakes *This vulnerability factor reflects the perceived stakes that the target may have in accurately assessing the credibility of information. If the perceived stakes of deception are high this may increase the cognitive load in individual's assigned to assessing credibility and reduce their decision-making abilities.* **Current:**	Presence: Current ✓ **0** ☐ 1 ☐ 2 Relevance: Current ✓ **0** ☐ 1 ☐ 2
T3: Motivation *This vulnerability factor reflects how motivated the target is to detect deception. The motivation impairment effect suggests that when individuals are highly motivated to detect deception their ability to accurately detect deception decreases as they rely upon incorrect decision-making strategies. To overcome this impairment effect it is recommended that practitioners discuss their findings with others to re-evaluate their judgements.*	Presence: Current ✓ **0** ☐ 1 ☐ 2 Relevance: Current ✓ **0** ☐ 1 ☐ 2

Current:

T4: Target Characteristics

This vulnerability factor reflects the culture, individual differences and personality of the target, and how these may affect the target's ability to analyse and assess the credibility of information and intelligence.

Presence: Current

✓ **0** ☐ 1 ☐ 2

Relevance: Current

✓ **0** ☐ 1 ☐ 2

Current:

T5: Mindset - Cognition

This vulnerability factor reflects the cognitive state of the individual or group who are tasked with assessing veracity. As some deception and influence tactics are designed to affect cognitive performance, whether through inundating the target with information increasing cognitive load and reducing ability to accurately assess multiple sources of information, through reducing information leading to individuals and groups requiring more sources to uncover information, or deliberately diverting the target's perception towards other information concealing any deception, highlighting the need for the target to be aware that deception strategies will seek to manipulate target expectation and cognition and reduce

Presence: Current

✓ **0** ☐ 1 ☐ 2

Relevance: Current

✓ **0** ☐ 1 ☐ 2

available resources towards analysing information.

Current:

T6: Mindset - Affect

This vulnerability factor reflects the affective state of the individual or group who are tasked with assessing veracity. As some influence tactics are designed to affect the emotional state of the target to enhance their attempts at deceit, an understanding of our affective state is important when analysing deception.

Presence: Current
✓ **0** ☐ 1 ☐ 2
Relevance: Current
✓ **0** ☐ 1 ☐ 2

Current:

T7: Capabilities – Information, Surveillance, Target Acquisition and Reconnaissance (ISTAR)

This vulnerability factor reflects the targets own capabilities and how they will affect the ability to detect deception. Preparation for and experience of past adversary deception alongside deployment of ISTAR capabilities will enable the gathering of information for credibility assessment. The greater the number of friendly capabilities in ISTAR the more information may be uncovered for subsequent analysis.

Presence: Current
✓ **0** ☐ 1 ☐ 2
Relevance: Current
✓ **0** ☐ 1 ☐ 2

Current:

Risk Scenarios and Management Strategies

The following tables identify the scenarios of future deception acts. The scenarios are summarised below:

RISK SCENARIOS **Identify and describe the most plausible scenarios of future deception**		
Scenario #1	**Scenario #2**	**Scenario #3**
Nature: **Who are the likely targets of the deception?** **What kind of deception is likely to be committed?**		

What kind of strategy will the deceiver deploy to influence the target? **What is the likely motive – that is, what is the deceiver trying to accomplish?**
Severity: **What would be the impact or harm to the target of the deceit?** **What would be the physical harm to the target of the deceit?** **Is there a chance that the deception could**

proliferate across multiple mediums and sources?
Imminence: How soon might the deception occur? **Are there any warning signs that might signal that the risk is increasing or imminent?**
Frequency / Duration Severity: How often might the deception occur – once, several times, frequency? **Is the risk chronic or**

acute (i.e., time limited)?
Likelihood: **In general, how frequent or common is this type of deception?** **Based on the deceiver's history, how likely is it that this type of deception will occur?**
RISK MANAGEMENT STRATEGIES **Recommend strategies for managing deception risk (C/F Henderson & Pascual (2008); JDP 3-80.1 - DCDC (2007))**
Scenario #1 **Scenario #2** **Scenario #3**

Monitoring:
What is the best way to monitor warning signs that the risks posed by the deceiver may be increasing?

What events, occurrences, or circumstances should trigger a re-assessment of risk?

Supervision:
What surveillance strategies could be implemented to manage the risk posed?

What restrictions on activity, movement, association, or communication are indicated?
Target Inoculation Planning: **What steps could be taken to enhance the protection of potential targets?** **How might the targets' security or vulnerability to deception be improved?**
Other Considerations: **What events,**

occurrences, or circumstances might increase or decrease risk? **What else might be done to manage risk?**

Appendix 8.4: Supporting Evidence for DRAT Risk Factors.

Section and Item of Risk	Supporting Evidence
Context	
C1: Situation	Chapter 6: SME Study Gozna, L. F., & Boon, J. C. W. (2010). Interpersonal deception detection. In J.M. Brown & E.A. Campbell (Eds.). *The Cambridge handbook of forensic psychology.* (pp. 484-491). Cambridge: Cambridge University Press.
C2: Actors	Chen, C., Wu, K., Srinivasan, V., & Zhang, X. (2011). *Battling the Internet Water Army: Detection of Hidden Paid Posters.* CoRR, vol. abs/1111.4297. Donath, J. (1999). Identity and deception in the virtual community. In M.A. Smith & P. Kollock (Eds.). *Communities in cyberspace.* (pp. 29-59). London: Routledge.
C3: Current Threats	Bennett, M., & Waltz, E. (2007). *Counterdeception Principles and Applications for National Security.* London: Artech House.
C4: Communication Medium	Ten Brinke, L., MacDonald, S., Porter, S., & O'Connor, B. (2011). Crocodile tears: Facial, verbal and body language behaviours associated with genuine and fabricated remorse. *Law and Human Behavior*. doi: 10.1007/s10979-011-9265-5. Wright Whelan, C., Wagstaff, G. F., & Wheatcroft, J. M. (2013). High-Stakes Lies: Verbal and nonverbal cues to deception in public appeals for help with missing

	or murdered relatives. *Psychiatry, Psychology and Law*. doi: 10.1080/13218719.2013.839931.
C5: Online Communication Characteristics	Cornish, P., Hughes, R. & Livingstone, D. (2009). *Cyberspace and the national security of the United Kingdom.* London: Chatham House. Hancock, J.T. (2007). Digital deception: The practice of lying in the digital age. In B. Harrington (Ed.). *Deception: From ancient empires to internet dating.* (pp. 109-120). Stanford: Stanford University Press.
C6: In-Real-Life Communication Characteristics	Burgoon, J. K., Buller, D. B., White, C. H., Afifi, W., & Buslig, A. L. S. (1999). The role of conversational involvement in deceptive interpersonal interactions. *Personality and Social Psychology Bulletin.* 25, 669-686. Porter, S., & ten Brinke, L. (2009). Dangerous decisions: A theoretical framework for understanding how judges assess credibility in the courtroom. *Legal and Criminological Psychology,* 14, 119-134. doi: 10.1348/135532508X281520.
History *H1: Previous Behaviour – Non-Deceptive* *H2: Previous Deceiver Interactions – UK* *H3: Previous Deceiver Interactions – Others*	Ewens, S., Vrij, A., Jang, M., & Jo, E. (2014). Drop the small talk when establishing baseline behaviour in interviews. *Journal of Investigative Psychology and Offender Profiling.* doi: 10.1002/jip.1414. Gozna, L. F., & Boon, J. C. W. (2010). Interpersonal deception detection. In J.M.

	Brown & E.A. Campbell (Eds.). *The Cambridge handbook of forensic psychology.* (pp. 484-491). Cambridge: Cambridge University Press. Navarro, J. (2003). A four-domain model of detecting deception. *FBI Law Enforcement Bulletin* (June), 19-24. Vrij, A., & Mann, S. (2001). Telling and detecting lies in a high-stake situation: The case of a convicted murderer. *Applied Cognitive Psychology*, *15*, 187-203.
Nature of Deception	
N1: Create and Identify Vulnerability and Exploit	Henderson, S. (2007). *Deception – A guide to exploiting the psychological basis of deception in military planning.* MIST/06/07/702/21/1.0. Whaley, B. (2007). *Stratagem: Deception and surprise in war.* London: Artech House.
N2: Conditioning the Target	Henderson, S. (2007). *Deception – A guide to exploiting the psychological basis of deception in military planning.* MIST/06/07/702/21/1.0. LeMire, G. A. (2002). *Employing special operations forces to conduct deception in support of shaping and decisive operations.* Fort Leavenworth: School of Advanced Military Studies.
N3: Impression Management	Hartwig, M., Granhag, P. A., Strömwall, L. A., & Doering, N. (2010). Impression and information management: On the strategic self-regulation of innocent and guilty suspects. *The Open Criminology Journal*, 3, 10-16.

	Hines, A., Colwell, K., Hiscock-Anisman, C., Garrett, E., Ansarra, R., & Montalvo, L. (2010). Impression management strategies of deceivers and honest reporters in an investigative interview. *The European Journal of Psychology Applied to Legal Context,* 2, 73-90.
N4: Control of Information	Chapter 6: SME Study Strömwall, L. A., & Willen, R. M. (2011). Inside criminal minds: Offenders' strategies when lying. *Journal of Investigative Psychology and Offender Profiling,* 8, 271-281. doi: 10.1002/jip.148.
N5: Credibility Enhancers	Chapter 6: SME Study Hansen, J. K. (2008). *Military deception and the non-state actor.* Newport: Naval War College.
N7: Social Influencers	Chapter 6: SME Study Cialdini, R. B. (2007). *Influence: The Psychology of Persuasion.* New York: Harper Collins
Deceiver Risk Factors	
D1: Deception Doctrine	Director General Development, Concepts and Doctrine Centre. (2007). *OPSEC, deception and PSYOPS.* Joint Doctrine Publication 3-80.1.

	Whaley, B. (2007). *Stratagem: Deception and surprise in war*. London: Artech House
D2: Gains Vs Losses	Porter, S., & ten Brinke, L. (2010). The truth about lies: What works in detecting high-stakes deception? *Legal and Criminological Psychology*, 15, 57-75. doi: 10.1348/135532509X433151. Ten Brinke, L., MacDonald, S., Porter, S., & O'Connor, B. (2011). Crocodile tears: Facial, verbal and body language behaviours associated with genuine and fabricated remorse. *Law and Human Behavior*. doi: 10.1007/s10979-011-9265-5.
D3: Motivation	Chapter 6: SME Study Woodworth, M., Hancock, J., & Goorha, S. (2005). *The motivational enhancement effect: Implications for our chosen modes of communication in the 21st Century*. Proceedings of International Conference of Systems Science, Hawaii, USA.
D4: Capabilities, Resources and Experience	Chapter 6: SME Study Gozna, L. F., & Boon, J. C. W. (2010). Interpersonal deception detection. In J.M. Brown & E.A. Campbell (Eds.). *The Cambridge handbook of forensic psychology*. (pp. 484-491). Cambridge: Cambridge University Press.
D5: Target Audience Analysis	Director General Development, Concepts and Doctrine Centre. (2007). *OPSEC, deception and PSYOPS*. Joint Doctrine Publication 3-80.1.

	Mackay, A., & Tatham, S. (2011). *Behavioural Conflict: Why understanding people and their motivations will prove decisive in future conflict.* Saffron Walden: Military Studies Press.
D6: Deception Spontaneity > Planned	Chapter 6: SME Study Strömwall, L. A., & Willen, R. M. (2011). Inside criminal minds: Offenders' strategies when lying. *Journal of Investigative Psychology and Offender Profiling*, 8, 271-281. doi: 10.1002/jip.148.
D7: Cognitive Performance	Vrij, A., Granhag, P.A., Mann, S., & Leal, S. (2011a). Outsmarting the liars: Towards a cognitive lie detection approach. *Current Directions in Psychological Science.* 20, 28-32. doi: 10.1177/0963721410391245. Vrij, A., Leal, S., Mann, S., & Fisher, R. (2011). Imposing cognitive load to elicit cues to deceit: Inducing the reverse order technique naturally. *Psychology, Crime & Law*. doi: 10.1080/1068316X.2010.515987.
D8: Language	Cheng, K. H. W., & Broadhurst, R. (2005).The detection of deception: The effects of first and second language on lie detection ability. *Psychiatry, Psychology and Law.* 12, 107-118. Colwell, K., Hiscock-Anisman, C., & Fede, J. (2013). Assessment criteria indicative of deception: An example of the new paradigm of differential recall enhancement. In

	B. S. Cooper, D. Griesel, & M. Ternes (Eds.). *Applied Issues in Investigative Interviewing, Eyewitness Memory, and Credibility Assessment.* (pp. 259-291). London: Springer
D9: Personality and Individual Differences	Paulhus, D. L., & Williams, K. M. (2002). The dark triad of personality: Narcissism, Machiavellianism, and psychopathy. *Journal of Research in Personality,* 36, 556-563. Taylor, R., & Gozna, L. F. (2011). *Deception: A Young Person's Life Skill?* Hove: Psychology Press.
D10: Belief System	Bond, C.F., Jr., & Atoum, A.O. (2000). International deception. *Personality and Social Psychology Bulletin.* 26, 385-395. Lewis, C. C., & George, J. F. (2008). Cross-cultural deception in social networking sites and face-to-face communication. *Computers in Human Behavior, 24,* 2945-2964. doi: 10.1016/j.chb.2008.05.002.
D11: Radicalised?	
Target Vulnerability Factors *T1: Who is the Target?*	This risk factor requires identifying who the target is, to understand the context in which deception may be occurring.

T2: Stakes	Bond, C. F., Jr., & DePaulo, B. M. (2006). Accuracy of deception judgements. *Personality and Social Psychology Review.* 10, 214-234. Chapter 6: SME Study
T3: Motivation	DePaulo, B. M., & Kirkendo, S. E. (1988). The motivational impairment effect in the communication of deception. In J. Yuille (Ed.). *Credibility Assessment.* (pp. 50-69). Belgium: Kluwer Academic Publishers.
T4: Target Characteristics	Baker, A., ten Brinke, L., & Porter, S. (2012). Will get fooled again: Emotionally intelligent people are easily duped by high-stakes deceivers. doi.1111/j.2044-8333.2012.02054.x. Director General Development, Concepts and Doctrine Centre. (2007). *OPSEC, deception and PSYOPS.* Joint Doctrine Publication 3-80.1.
T5: Mindset – Cognition	Henderson, S. (2007). *Deception – A guide to exploiting the psychological basis of deception in military planning.* MIST/06/07/702/21/1.0. Kaina, J., Ceruti, M. G., Liu, K., McGirr, S. C., & Law, J. B. (2011, June). *Deception detection in multicultural coalitions: Foundations for a cognitive model.* Paper presented at the 16th International Command and Control Research and Technology Symposium (ICCTRS), Quebec, Canada.

T6: Mindset – Affect	Forgas, J. P. (2011). Don't worry be sad! On the cognitive, motivational and interpersonal of negative mood. *Current Directions in Psychological Science, 22*, 225-232. doi: 10.1177/0963721412474458. Henderson, S. (2007). *Deception – A guide to exploiting the psychological basis of deception in military planning.* MIST/06/07/702/21/1.0.
T7: Capabilities - ISTAR	Director General Development, Concepts and Doctrine Centre. (2007). *OPSEC, deception and PSYOPS.* Joint Doctrine Publication 3-80.1. Henderson, S. M., & Pascual R. G. (2008). *The psychology of Counter-ISTAR: Concepts and discussion*. QINETIQ/EMEA/TS/CR0801237/1.0.

Appendix 9.1: Article List for Scenario Development

Alic, J. (2013). *Rhetoric increases as Falkland referendum looms.* http://oilprice.com/Geopolitics/International/Rhetoric-Increases-as-Falkland-Referendum-Looms.html

BBC. (2013a). *Argentine President Fernandez renews Falklands claims at UN* http://www.bbc.co.uk/news/world-latin-america-23596312

BBC. (2013b). http://www.bbc.co.uk/news/world-latin-america-18425572

BBC. (2013c). http://www.bbc.co.uk/iplayer/episode/b03kpnjl/Today_09_12_2013/ (From 1:09:42)

BBC. (2014). *China and UK trade at 'record high'.* http://www.bbc.co.uk/news/business-25838655

CPNI. (2013). *CPNI Insider Data Collection Study: Report of Main Findings.* http://www.cpni.gov.uk/Documents/Publications/2013/2013003-insider_data_collection_study.pdf

DCDC. (2010a). *Global Strategic Trends – Out to 2040.* Swindon: DCDC.

DCDC (2010b). *Future Character of Conflict.* Swindon: DCDC.

DCDC (2014). *Global Strategic Trends – Out to 2045.* Swindon: DCDC.

EUROPOL (2013). *EU Serious and Organised Crime Threat Assessment.* Deventer: European Police Office.

FBI. (Unknown). *The Insider Threat: An Introduction to Detecting and Deterring an Insider Spy.* http://www.fbi.gov/about-us/investigate/counterintelligence/insider_threat_brochure

Gibbs, S. (2013). *First metal 3D printed gun is capable of firing 50 shots.* http://www.theguardian.com/technology/2013/nov/08/metal-3d-printed-gun-50-shots

Gilligan, A. (2011). *Police 'covered up' violent campaign to turn London area 'Islamic'.* http://www.telegraph.co.uk/news/uknews/law-and-order/8570506/Police-covered-up-violent-campaign-to-turn-London-area-Islamic.html

Gordon, T., Sharan, Y., & Florescu, E. (2015). Prospects for lone wolf and SIMAD terrorism. *Technological Forecasting and Social Change.* doi: 10.1016/j.techfore.2015.01.013.

Guardian. (2014). http://www.theguardian.com/world/2014/jan/12/argentina-falklands-oil-international-courts

Highfields Community Association. (2010). *Highfields Youth Outreach Project (H-YOP): Project Report – November 2010.* http://www.highfieldscentre.ac.uk/report/H-YOP%20Reportv3.pdf

HM Government. (2013). *Serious and Organised Crime Strategy.* London: Home Office.

Huffington Post. (2013). *'Muslim Patrol' video victim urged to come forward.* http://www.huffingtonpost.co.uk/2013/01/24/muslim-patrol-video-victim-east-london-_n_2541054.html

Jacobson, M. (2010). Terrorist financing and the internet. *Studies in Conflict & Terrorism, 33,* 353-363. doi: 10.1080/10576101003587184.

Jessee, D. D. (2006). Tactical means, strategic ends: Al Qaeda's use of denial and deception. *Terrorism and Political Violence, 18,* 367-388. doi: 10.1080/09546550600751941.

Kagan, F. W., Majidyar, A. K., Pletka, D., & Sullivan M. C. (2012). *Iranian Influence: In the Levant, Egypt, Iraq, and Afghanistan.* http://www.understandingwar.org/sites/default/files/IranianInfluenceLevantEgyptIraqAfghanistan.pdf

Klare (2014, July 15). *Twenty-first century energy wars: how oil and gas are fuelling global conflicts.* Retrieved from http://www.energypost.eu/twenty-first-century-energy-wars-oil-gas-fuelling-global-conflicts/.

Laing, P. (2012). *Albanian crime gangs top list of most feared foreign gangsters.* http://www.deadlinenews.co.uk/2012/01/15/albanian-crime-gangs-top-list-of-most-feared-foreign-gangsters/

Morelle, R. (2013). *Working gun made with 3D printer.* http://www.bbc.co.uk/news/science-environment-22421185

Panda, A. (2013). *India Caves to China on Border Dispute.* http://thediplomat.com/2013/10/india-caves-to-china-on-border-dispute/

Peterson, A., & Barysch, K. (2011). *Russia, China and the Geopolitics of Energy in Central Asia.* London: Centre for European Reform.

Pew Research Center. (2014). *Religious Hostilities Reach Six-Year High.* http://www.pewforum.org/files/2014/01/RestrictionsV-full-report.pdf

Plafke, J. (2013). *NASA successfully tests 3D-printed rocked injector, showcases viability of 3D printing.* http://www.extremetech.com/extreme/165219-nasa-successfully-tests-3d-printed-rocket-injector-showcases-viability-of-3d-printing

Qiao, L., & Wang, X. (1999). *Unrestricted Warfare.* Beijing: PLA Literature and Arts Publishing House.

RAND. (2007). *The Radicalization of Diasporas and Terrorism: A Joint Conference by the RAND Corporation and the Center for Security Studies, ETH Zurich.* Santa Monica: RAND Corporation.

Ruge, T. M. S. (2013). *How the African diaspora is using social media to influence development.* http://www.theguardian.com/global-development-professionals-network/2013/feb/06/african-diaspora-social-media-tms-ruge

Smith, E. (2013). *The Enemy Within: Cyber-Theft Expert Warns of Growing "Insider" Threat.* http://www.ibtimes.co.uk/cyber-theft-gchq-nsa-prism-business-china-485667

Tharoor, I. (2012). *The Sino-Indian War: 50 Years Later, Will India and China Clash Again?* http://world.time.com/2012/10/21/the-sino-indian-war-50-years-later-will-india-and-china-clash-again/

The Economist. (2013). *Britain and India: The odd couple.* http://www.economist.com/news/britain/21586829-two-countries-have-close-financial-ties-trade-between-them-feeble-odd-couple

Thomas, T. L. (2003). Al Qaeda and the internet: The danger of "cyberplanning". *Parameters, 33,* 112-123.

Walker, A. (2012). The United Kingdom and Central Asia. *EUCAM National Policy Series, 3,* 1-5.

Appendix 9.2: Scenarios of Future Threats

Scenario 1: CBRN weapon capabilities

The proliferation of new technological innovations globally has the potential to put pressure on the capacity of non-Western nations and as such will likely result in a broader requirement to present a capability of claimed technological innovations regardless of associated credibility. Deception regarding weapons capabilities has been observed in recent, on-going and potential conflicts involving Iraq, Afghanistan, Syria and Iran respectively. As Iran seeks to increase influence in the Middle East and surrounding regions, it is possible that uranium enrichment capabilities will be increased (despite any international diplomatic agreements to the contrary) to ensure energy supply for the population, alongside a potential for nuclear weapon development to appear as a strong nation. The interpretation of such nuclear capabilities in Iran will likely be viewed by the West now and in the future as being for malign military intent. Following challenges in post-hoc justifications for the invasion of Iraq in 2003 and the present Chilcott Inquiry in the UK, it is likely that there will be an increased requirement in the future to determine the credibility of any future claims of CBRN capabilities. Although the present focus has been on the threat of potential nuclear warfare, broader future challenges involve consideration not only of nation state capabilities, but of individual and group development of asymmetric weapons. Hence the challenges within this arena of future CBRN weapon threats require broader consideration than at a high level political focus. The detection of risk in regard of any CBRN threat will likely be identified through monitoring across ISR procedures and therefore the focus on deception or concealment of such activity will be online and through broader behavioural actions.

Likely deception methods –

- Context (interpersonal and mediated communication)
- Control of Information (increase information related to non-CBRN intentions; block and deny information regarding CBRN intentions)
- Influencers (wide range of potential influence tactics aiming to appear positive, credible, objective in claims)
- Replicating Genuine Behaviour (state representatives, diplomats, negotiators will all aim to appear credible through appearances of normality, basing deceptions around some elements of the truth)

Scenario 2: Competition for energy resources

In order to ensure the future security of the UK energy infrastructure and respond to reduced offshore energy production there will be a requirement for imported oil and gas. The energy transit routes to the European Union traverse Turkey from the Middle East, the Caucasus and Central Asia. Although the importation of energy resources from these other regions reduces reliance upon energy resources imported from Russia, there will be concerns from conducting business with authoritarian regimes in these areas, alongside growing fundamentalist groups operating in these countries. These issues will be further exacerbated by the Russian annexation of Crimea and on-going military actions in Ukraine alongside the exertion of Russian influence throughout the Caucasus and former USSR states. Russian-backed proxy groups may be likely to target UK interests in this region, and if these groups seek to target energy infrastructure then UK interests may be harmed in the short-term for isolated incidents, however, if a protracted conflict develops in these regions then long-term issues may develop for the UK energy infrastructure. In order to be successful in furthering their aims these groups will need to engage in deception to conceal their initial operational planning, and during operations themselves to conceal their identities before attacking targets. Furthermore, public facing elements of Russian diplomacy will also have to conceal and deny knowledge of links to these groups to avoid political embarrassment or repercussion.

Likely deception methods –

- Context (interpersonal and mediated communication)
- Control of Information (increase information related to proxy groups to make them appear credible, whilst concealing information related to Russian involvement, planning and target selection and of the individuals engaged in such tasks)
- Influencers (emphasise objectivity, convincing, committed, use of distractors)
- Replicating Genuine Behaviour (speech control and mimicking by diplomats and members of proxy groups as they seek to appear credible)

Scenario 3: Radicalisation/Diaspora

The UK has become and continues to be a diverse, multi-cultural society, with an increase in nationalities from EU member states, Commonwealth members, and increases in asylum seekers and refugees from areas of conflict including Syria, Afghanistan, Iraq, Sudan and Libya. Following recent large scale population movements by migrants fleeing conflict zones in the Middle East, Central Asia and North Africa these diaspora groups will increase in population size within the UK and will present an increasing influence on social, political and cultural events in the UK. Religious affiliation and identity will continue amongst elements of these diaspora groups and some individuals and groups will place more importance upon their religious than national identity, alongside perceived grievances against the host nation will open up possibilities for radicalisation, and further acts of terrorism within the UK (DCDC, 2010). Further difficulties will be faced in verifying recent asylum seekers to ensure they are credible refugees fleeing conflict zones rather than members of extremist groups, for example, the 'Islamic State' seeking to infiltrate and then conduct terror campaigns in Europe (Giglio & al-Awad, 2015). In seeking to prepare an act of terrorism an individual or group is required to act on a covert level, so that they do not come to the attention of security and intelligence agencies, particularly if they are entering the UK illegally. In seeking to prepare an act of terror, individuals and groups will be required to purchase specific chemicals from a range of retailers, including both online purchases and face-to-face retail purchases. Individuals will be required to present themselves as genuine purchasers who will be using these chemicals for plausible reasons, highlighting the challenges involved in detecting these individuals. Alongside purchasing materials, extremist individuals and organisations require targets where there will be large media exposure highlighting their cause, and these individuals may survey targets to ensure that their plans are effective. This form of deception in concealing preparing acts of terrorism presents challenges in detecting them, as there may be less evidence with which to detect these individuals and groups.

Likely deception methods –

- Context (primarily interpersonal deception, but with some mediated deception in securing components for explosives)
- Control of information (information will be increased to aid appearance as a genuine asylum seeker, whilst decreased and concealed surrounding links to their real identity and operational planning of acts of terrorism)

- Influencers (appeals to higher authority, commitment, subtlety, distraction from truth – particularly relevant for false asylum seekers)
- Replicating Genuine Behaviour (mimicking real behaviours when surveying targets, speech control during interviews for asylum claims)

Scenario 4: Insider Threat

One of the most vulnerable points in UK organisations comes from 'insider threat' where individuals or groups pose a threat to an organisation through theft of data, revelation of information, physical and IT sabotage, or through input of false data potentially effecting an organisation's ability to function (CPNI, 2013). It is anticipated that as developed and developing nations and non-governmental organisations seek to expand their research and development capabilities to enhance their economies, there will be a greater risk of threats to commercial property from commercial and state-backed espionage (FBI, unknown; Smith, 2013). Scientific and engineering innovations will be at particular risk of exploitation by such organisations as they seek to develop these capabilities (FBI, unknown; Smith, 2013). Although a number of insider threats are self-initiated there are still opportunities for infiltration by individuals and groups seeking strategic advantage (CPNI, 2013). An individual working in an organisation who is seeking to remove commercial property is required to hide their motives for working for that organisation from their employers and this may be difficult to detect if the individual works as a trusted employee before removing commercial property (CPNI, 2013). With the development of data storage it can be a simple procedure for an individual to download information onto a USB stick and pass that information onto a third-party. These threats may be concealed for a period of time, during which a large amount of information may be stolen (CPNI, 2013).

Likely deception methods –

- Context (Primarily interpersonal and/or written communication as the insider justifies access to information systems)
- Control of information (increase information related to non-relevant areas to try and provide justification for actions; decrease or deny and conceal information related to malign intent)

- Influencers (Emphasise honest behaviour, appeals to authority, convincing, authority, referent power, distraction).
- Replicating Genuine Behaviour (Appear normal, try and base deception around truth to provide justification for access to information, control verbal behaviour during interactions)

Scenario 5: Territory and Resource Disputes

Contemporary and future territory conflicts will affect UK overseas territories including, the Falkland Islands, South Shetland, and the South Georgia and South Sandwich Islands which have led to conflict between the UK and Argentina in the past, and there are current disputed claims as to the sovereignty of these islands (BBC, 2013b). In recent years Argentina has increased the political rhetoric regarding these disputed territories claiming these territories for Argentina against the wishes of the inhabitants, for example, President Fernandez has recently renewed Argentina's claims to the Falkland Islands at the United Nations (BBC, 2013a). The conflict surrounding these islands will be exacerbated due to the potential resources that may be uncovered in these areas, including oil and gas, and access to mineral resources in Antarctica, which will provide strong financial gains (Alic, 2013; Guardian, 2014). Argentina may seek to assert sovereignty over these territories through a combination of diplomatic and military means, both of which will involve aspects of deception. If diplomatic means fail to resolve the territorial dispute Argentina may resort to military means, which will require elements of surprise to ensure their success. It is anticipated that Argentine military capabilities are not as developed as UK military capabilities therefore there will be a need for deception through concealing any operational planning from UK intelligence, alongside deception in military engagements to divert UK attention.

Likely deception methods –

- Context (both interpersonal and mediated communication will be used for deception)
- Control of information (increase of rhetoric surrounding justifications for control of Falkland Islands as a potential distraction, whilst other information regarding planning activities is concealed)

- Influencers (Emphasis, appeals to higher authority, attractive, concealing, commitment, distractors)
- Replicating Genuine Behaviour (Primarily focussed around maintaining normal behaviour whilst concealing any military ambitions)

Scenario 6: Internal Intercultural Conflict

As the UK becomes an increasingly multi-cultural society with an international diaspora from EU and non-EU, developed and developing nations there is an increasing mix of diverse groups from differing ethnic, religious and cultural backgrounds. Some of these groups may integrate well with mainstream British culture others may not. With the lack of integration between established and immigrant communities in urban environments, for example, Tower Hamlets in London (Gilligan, 2011; Huffington Post, 2013) and Highfields in Leicester, potential conflict will occur. Within these environments there may be a perceived threat from the immigrant community towards the established community, as the established community may not understand the customs and traditions of the immigrant community. Simultaneously the immigrant community may perceive the established as a threat as they too do not understand the customs and traditions of the established community. Stereotypical accounts of racism towards immigrant communities by established communities and the perceived lack of opportunities by young adults from immigrant communities may increase resentment by immigrant communities towards the mainstream. Established communities may perceive the immigrant communities in stereotypical ways of using up resources that should be reserved for established communities. Once this resentment has built between these different cultures there may be a triggering incident which results in open conflict between these two groups, for example, there was a recent conflict in Highfields in Leicester between the Jamaican and Somali émigré communities, resulting in a number of Jamaican families leaving the area. The triggering incident may be difficult to accurately predict, however, there may be specific groups involved that will seek to hide their motives for these actions and have organised themselves for any incidents occurring for them to exploit, whether that be enacting grudges against members of other communities or to take advantage of conflicts for financial gain, in a similar manner to the widespread looting seen in the London riots.

Likely deception methods –

- Context (both interpersonal and mediated communication)
- Control of Information (Most likely to involve reducing information through denial, blocking and other concealing attempts)
- Influencers (Emphasise their points to provide justification for actions, appearance as authority figures to appear more credible, referent power, attractive, committed, use of distraction tactics)
- Replicating Genuine Behaviour (Speech control to appear more credible, base deceptions around truths, mimic normal behaviour)

Scenario 7: Religious Conflict

Religion and extremist beliefs are currently and will be a major source of conflict in multiple parts of the world (DCDC, 2010). Overt violent conflicts are currently on-going in Africa, the Middle East and Asia with more isolated incidents occurring in Europe and North America (DCDC, 2010). These conflicts are often portrayed as being ostensibly Christian versus Muslim in nature, however, multiple actors are involved and current conflicts include different branches of Muslims, Muslims and Buddhists, Christians and Muslims and different branches of Christianity, it is anticipated that a large majority of these conflicts will continue (DCDC, 2010). Although conflicts may appear to be about religious and cultural differences between groups over a number of issues a wider array of motives appear. Furthermore, some conflicts will be conducted ostensibly under the guise of religion as a method for individuals to justify their actions and gain wider support for their ambitions. UK interests in conflict parts of Africa, the Middle East and Asia will be affected as Western nations will be seen as legitimate targets in religious conflict. There will be threats to UK businesses, embassies and consulates in these regions from spontaneous and organised groups, for example, repeated Al-Shabaab attacks in Kenya conducted in retaliation for Kenyan support for the legitimate government of Somalia and in providing troops to fight Al-Shabaab. Spontaneous conflicts may be harder to predict, however, organised groups will need to engage in deception to ensure that their activities are covert and do not come to the attention of Western security and intelligence agencies. Furthermore, cultural differences in norms of conflict will change what other actors may see as legitimate targets providing a need

to understand how these groups will operate and the spectrum of threats that they will pose.

Likely deception methods –

- Context (Interpersonal and mediated communication – limited by access to technology)
- Control of Information (Potential to increase flow of information as a diversion strategy, alongside concealment and denial of motives and objectives)
- Influencers (appeals to authority, authority, referent power, committed)
- Replicating Genuine Behaviour (Mimicking normal behaviour)

Scenario 8: Intelligence-Gathering

In seeking to uncover adversary operations and planning various intelligence and information gathering approaches have been developed by security agencies that monitor the online activities of a large number of people across society. These intelligence gathering approaches seek to monitor and uncover the digital trails that potential adversary individuals and networks may leave in the online domain in order to prevent acts of terrorism or other threats (BBC, 2013c), where individuals identified online can be brought in for questioning. Terrorists and other adversaries are not naïve and use all technology that can be available to them to achieve their aims whether to spread influence and misinformation (Jessee, 2006), plan operations (Thomas, 2003) or to raise finances (Jacobson, 2010). However, following revelations of these intelligence-gathering approaches by whistle-blowers adversaries may change their tactics to becoming more covert to reduce their chances of being detected (BBC, 2013c). A possible backlash against state intelligence-gathering approaches may also occur where the state is seen as infringing upon individual liberties potentially leading to a reduction in intelligence-gathering increasing the potential for online exploitation by adversaries (BBC, 2013c). Adversary knowledge of information-gathering approaches also opens up possibilities for the spread of deception where adversaries may deliberately leave an online footprint to influence security agencies to an incorrect response. Furthermore, adversaries may seek to upload misinformation that security agencies may accept as genuine intelligence again influencing them to an incorrect response.

Likely deception methods –

- Context (deception will occur across both interpersonal and mediated environments)
- Control of Information (Increase information as a distraction from aims and waste target resources; conceal and deny true aims and motives)
- Influencers (Emphasise to influence, objective, referent power, attractive, committed, confidence)
- Replicating Genuine Behaviour (Mimicking, kernel of truth, controlled behaviour)

Scenario 9: UK Organised Crime

Organised Crime Groups (OCGs) are increasingly multinational in their infrastructure, although core groups are often based around a shared ethnic identity from which a bond and trust are developed, OCGs incorporate a wide range of actors according to their aims and criminal activities (EUROPOL, 2013). There are approximately 1500 OCGs targeting the UK with groups involved in drug trafficking, people trafficking, fraud, counterfeit goods and cybercrime (HM Government, 2013), and a number of OCGs engage in multiple criminal activities, including links to terrorism (HM Government, 2013), to increase their share of the illicit economy and this his become increasingly possible with the advancement of the Schengen Zone and free movement within the EU (EUROPOL, 2013). OCGs are estimated to cost the UK at least £24 billion per year alongside loss of life, security and prosperity and the effects of corruption and intimidation that OCGs have on communities (HM Government, 2013). The global financial crisis has increased the scope of these groups as more consumers are turning towards illicit markets to meet this increased demand (EUROPOL, 2013). Internet growth has enabled OCGs to reach a larger number of potential victims, the potential to hide their illicit activities and the ability to commit a greater number of crimes in a reduced time period (EUROPOL, 2013). Albanian OCGs are argued to be involved in drug, arms and people trafficking and operate in large cities within the UK. These groups operate across illegitimate and legitimate businesses with OCGS also running bars, clubs and restaurants to appear legitimate, whilst also running brothels and involvement with associate OCGs in drug trade (Wikipedia, 2013b). OCGs are required to operate at a covert level in order to hide their illegitimate activities from authorities and they may achieve this through a variety of methods including running legitimate businesses

and maintaining Operational Security (OPSEC), posing challenges to investigating agencies seeking to confront these OCGs.

Likely deception methods –

- Context (interpersonal communication in face-to-face encounters whilst investigating and using informants amongst the OCG; mediated communication where OCG members are in different locations)
- Control of Information (Increase information related to legitimate and front businesses; decrease through denial and concealment of illicit activities)
- Influencers (authority, referent power, fluency, influence increases over time)
- Replicating Genuine Behaviour (mimicking normal behaviour, use of decoys, base deception around truth)

Scenario 10: 3D Printers

Increasing technological developments in the world of manufacturing and printing technologies has led to the construction of 3D printers. 3D printers can build objects from multiple layers of plastic or metals opening a wide-range of applications for these technologies. Although 3D printers are currently costly, these costs will reduce as the technology becomes more widespread opening up the potential for usage by a wide range of individuals and groups. Recent media attention has highlighted one potential threat from 3D printers in the shape of both plastic and metal guns created by 3D printers (Gibbs, 2013; Morelle, 2013). As the cost of 3D printers reduces groups with malign intent may be able to access the technologies to start producing weapons from 3D printers, especially where designs can be shared online increasing access to these technologies. Beyond creating 3D printed firearms there is the potential for adversary groups to 3D print rocket parts (Plafke, 2013) which open up possibilities for adversaries to construct weapons that may be capable of inflicting mass casualties. If adversaries can 3D print missile components they may be able to target specific structures through transporting missile components from multiple locations to try and conceal the overall aim, and make the connections between individuals less obvious before assembling components at a location close to the target.

Likely deception methods –

- Context (Interpersonal and mediated communication between group members, may be hard to identify communication if a lone wolf)
- Control of Information (Reduce and conceal information related to malign activities)
- Influencers (Appeals to higher authority, authority, referent power, committed)
- Replicating Genuine Behaviour (Mimicking real behaviour, use of decoys to distract authorities)

Appendix 9.3: Radicalisation and Terrorism in Diaspora Groups Risk Assessment

Deception Risk Assessment Technique (DRAT)©2015

PRESENCE AND RELEVANCE OF RISK FACTORS

Determine the presence of risk factors to and during the most recent pattern of deceptive behaviour, as well as their relevance to the development of future management strategies.

Context of Deception *This section examines the situation in which deception occurs, and how situational elements and actors involved leads to deception*	**Coding** 0 = Absent 1 = Possibility/Low Level Presence 2 = Clearly Present
C1: Situation *This factor reflects upon what the current situation is, what has led to this current situation occurring at this moment in time, and what are the distinguishable elements from the situation which are cause for concern.*	

Current:

Potential for acts of terrorism by diaspora groups within the UK instigated by groups from their home nations. This will involve online communication between the actors which will require monitoring and detection. Identifying potential locations where actors may purchase compounds used to make explosives is required and where actors may assemble explosive devices. Actors may also begin target selection therefore there is a requirement to identify potential targets and increase their resilience.

Presence: Current

☐ 0 ✓1 ☐ 2

Relevance: Current

☐ 0 ✓1 ☐ 2

C2: Actors

This factor reflects who the actors are in the current situation: can we identify these actors successfully? Are there multiple actors involved? Who are the key actors? Who, if any, are the subsidiary actors? Are the actors involved individuals, groups or larger organisations? In in-real-life interactions identifying actors may prove challenging if they seek to conceal their identity (e.g. removing military insignia – Ukraine). Online interactions are often characterised by anonymity where identifying actors may prove challenging, and discernible behavioural patterns may be overgeneralised to the actor involved, creating a potentially unreliable profile of the actor.

Current:

The actors are from a diaspora group in the UK, with links to further actors in their nations of origin. However, it may be harder to successfully identify these actors due to associated anonymity of online communication. Actors from diaspora groups are attempting to conceal their actions from authorities.

Presence: Current

☐ 0 ✓ 1 ☐ 2

Relevance: Current

☐ 0 ☐ 1 ✓ 2

C3: Current Threats

This factor reflects what the current threats of the situation are, whether these threats are obvious, concealed or 'ghost' threats designed to waste resources, which area the threat/s is/are emerging from, and which areas of infrastructure these threats are targeting.

Presence: Current

☐ 0 ☐ 1 ✓ 2

Current:

Current situational threat is focussed on the potential for developing IEDs, the threat may be concealed to attempt surprise in targeting. Actors may target public areas with potential for mass casualties – therefore risk management should focus on transport hubs, sporting events, cultural and economic areas.

Relevance: Current

☐0 ☐ 1 ✓2

C4: Communication Medium

This factor reflects the communication medium the deception occurs in. Communication mediums include both online and in-real-life domains. Within the in-real-life domain

communication may be verbal, vocal, non-verbal (focussing on body language) and physical acts of deception. Within the online domain communication may be verbal, vocal and non-verbal (focussing on body language) and physical acts of deception, across an array of communication mediums (Instant Messaging, email, blogs, video chats, social media networks and deceptive websites).

Presence: Current

☐ 0 ☐ 1 ✓2

Current:

Relevance: Current

☐ 0 ☐ 1 ✓ 2

Deception will be conducted when the actors are seeking to conceal their communications, and across in-real-life and online domains, depending on where chemicals are bought from to create IEDs.

C5: Online Communication Characteristics

This factor reflects the specific characteristics of online communication where interactions may range from a user interacting with online content where there is no reciprocal communication (e.g. a website, or blog), to interactions where there is reciprocal communication (e.g. email, or Twitter). Online communication is characterised by its ability to cost-effectively reach large-scale audiences in a shorter period of time than traditional communication formats. The anonymity of communicating online may also lead to online disinhibition where individuals may be more likely to disclose information that they would not do so in-real-life, presenting an area for exploitation by deceivers.

Presence: Current

✓0 ☐ 1 ☐ 2

Current:

Online communication only used to discuss strategy and tactics between host nation actors and nation of origin actors, no real attempts at influence and deception to large audiences

Relevance: Current

✓ 0 ☐ 1 ☐ 2

C6: In-Real-Life Communication Characteristics

This factor reflects the specific characteristics of in-real-life communication in interpersonal interactions. These interactions can be within informal or formal settings and context will affect the characteristics of these interactions. First impressions often guide our interpretation of our interactional partner and form our initial judgements of them, we further adapt and respond to the interactional partner during conversation and can be influence by rapport, and the presentation and confidence of the other person.

Current:

Actors are required to make in-real-life communication when sourcing components for IEDs where they are required to create a favourable impression towards product sellers and to appear as credible buyers to them.

Presence: Current

☐ 0 ☐ 1 ✓2

Relevance: Current

☐0 ✓ 1 ☐ 2

History *This section examines previous behaviour and interactions to develop a profile of usual adversary behaviour, enabling the identification of non-normal behaviour which may indicate deception*	Coding
H1: Previous Behaviour – Non-Deceptive *This factor reflects the previous behaviour of the identified adversaries which is not related to deception. Identifying key goals that the adversary has achieved without using deception enables us to understand the non-deceptive strategies that have been used to achieve these goals. Subsequently developing a baseline of adversary non-deceptive strategic behaviour, enabling us to identify deviations in behaviour that may indicate deception; although it is important to establish that deviations in behaviour do not have another cause.*	
Current: Adversaries already have established contacts with actors in nations of origin, who may pose a threat to UK interests.	Presence: Current ☐ 0 ✓ 1 ☐ 2 Relevance: Current ☐0 ✓1 ☐ 2
Adversaries have been radicalised, which will increase the likelihood of them using deception to conceal their behaviour.	

H2: Previous Deceiver Interactions - UK

This factor reflects the past interactions that the deceiver has had with UK individuals, groups, organisations and infrastructure. Identifying and analysing previous known successful and unsuccessful deception attempts towards the UK will enable us to develop an understanding of how the adversary conducts and deploys deception strategies against the UK, enabling us to mitigate the risks of these attempts.

N.B. The deceiver may not use the same strategy multiple times against the UK

Presence: Current

✓ 0 ☐ 1 ☐ 2

Current:

No known previous deceptive interactions with the UK

Relevance: Current

✓ 0 ☐ 1 ☐ 2

H3: Previous Deceiver Interactions - Others

This factor reflects the past interactions that the deceiver has had with other individuals, groups, organisations and nations which are not related to the UK. Identifying and analysing previous known deception attempts, whether successful or unsuccessful, by the adversary towards others may enable friendly capabilities to understand how the adversary conducts deception and identify key strategies they have previously used.

N.B. The deceiver may not use the same strategy multiple times across different targets

Current: No known previous deception interactions with others	Presence: Current ✓ 0 ☐ 1 ☐ 2 Relevance: Current ✓0 ☐ 1 ☐ 2
Nature of Deception *This section reflects the different strategies used to deceive others – For further guidance see research by Henderson et al. on Deception Gambits, Vrij (2008), Whaley (2007)*	Coding
N1: Create and Identify Vulnerability and Exploit *This factor reflects strategies used in deception which seek to create and/or identify vulnerabilities in the target and then exploit these vulnerabilities for gain. Strategies include the following:* - *Ruses – This item reflects the intentional exposure of information to the target with the intention of misdirecting them, enabling the deceiver to exploit the adversary whilst their attention is directed towards the ruse (e.g. feeding misinformation to double-agents). Ruses can be conducted by the adversary across multiple levels of communication, whether through in-real-life interactions, through print media, TV, digital media, and other forms of online communication, potentially opening up a wide area for this deception to occur in and requiring a wide-range of resources to target this threat.*	Presence: Current ✓0 ☐ 1 ☐ 2 Relevance: Current ☐0 ✓ 1 ☐ 2 Presence: Current

✓0 ☐ 1 ☐ 2

- *Exploitation of target audience fears – This item reflects the deceiver deliberately identifying and targeting target audience fears through deception, meaning the target will be more likely to spend resources responding to this perceived threat, whilst the deceiver then exploits another area.*

Relevance: Current
☐ 0 ✓1 ☐ 2

Presence: Current
✓0 ☐ 1 ☐ 2

- *Exploitation of target audience hopes – This item reflects the adversary targeting audience and exploiting their hopes as part of their deception operation (e.g. attack when claiming peace).*

Relevance: Current
☐0 ✓1 ☐ 2

Presence: Current
✓0 ☐ 1 ☐ 2

- *Decoys – This item reflects how a deceiver may use a decoy to portray a false target, which the deceiver wants the receiver to believe as credible before they then attack or respond to the dummy, wasting friendly resources and enabling exploitation by the deceiver.*

Relevance: Current
☐ 0 ✓1 ☐ 2

Presence: Current
✓0 ☐ 1 ☐ 2

Relevance: Current
☐0 ✓1 ☐ 2

- *Feints – This item reflects mock attack or simulation of an attack by an adversary which seeks to create the appearance of an imminent attack, thus tying down friendly resources to countering the implied threat, whilst the adversary may actually perform other behaviour.*

Presence: Current
✓0 ☐ 1 ☐ 2

Relevance: Current
☐0 ✓ 1 ☐ 2

- *Demonstrations – This item reflects a real attack by the adversary which seeks to tie down friendly capabilities in active engagement in one situation whilst other adversary capabilities exploit the target in other areas. This strategy may prove costly to adversary resources as well as demonstrations in physical combat often increase number of casualties, however, this may be affect by adversary beliefs (e.g. if a soldier dies in combat he becomes a martyr and goes to heaven).*

Current:

There is a low chance that the adversary is seeking to create and then exploit a perceived vulnerability – actors have not been identified focussing their deception towards this approach, however, adversary behaviour may change to exploit this area.

N2: Conditioning the Target

This risk factor reflects strategies which involve conditioning the target into expecting a specific behavioural pattern by the deceiver.

- *Conditioning – This item reflects the deceiver conditioning the adversary into expecting a certain pattern of behaviour over the course of a period time, which then leaves the target open to exploitation when the deceiver performs a different behaviour (e.g. Soviet-Czechoslovakia Campaign 1968 and the Yom Kippur War 1973).*

Presence: Current

☐ 0 ☐ 1 ✓ 2

Relevance: Current

☐ 0 ☐ 1 ✓ 2

- *Drip-Drip-Feed – Through slowly releasing information to a target, target resources may become focussed on this information, particularly if the adversary feeds truthful information to the target to build trust, before the adversary then presents the target with false information they have worked hard to uncover leading to a less accurate assessment of that information and leaving the target more vulnerable to deception.*

Presence: Current
☐0 ✓1 ☐ 2
Relevance: Current
☐0 ✓1 ☐ 2

- *Influence increase over time – This item reflects how we are more likely to find an individual credible if we are interacting and developing trust with them over a period of time before they then engage in deception.*

Presence: Current
☐0 ☐ 1 ✓2
Relevance: Current
☐0 ☐ 1 ✓2

Current:

Adversaries will seek to condition the companies they are buying materials from so that they appear credible rather than seeking to use the materials for malign purposes.

Adversaries will also need to condition the target in their target reconnaissance efforts so that they are not identified and/or appear as credible.

N3: Impression Management

This risk factor reflects the strategies that individuals engage in order to convince others that they are telling the truth. Individuals may engage in controlling their verbal behaviour (e.g. through keeping statements short to avoid contradictions) and their non-verbal behaviour (e.g. reducing body movements to avoid appearances of nervousness). Impression management occurs both in-real-life and online domains.

Presence: Current

☐ 0 ☐ 1 ✓ 2

Relevance: Current

☐0 ☐ 1 ✓ 2

Current:

The actors will be required to engage in impression management strategies to control their non-verbal and verbal behaviour whilst they are engaged in real-life business transactions in being the necessary materials to make an IED and also in online interactions when buying materials.

N4: Control of Information

This risk factor reflects how information is controlled by the deceiver, where the deceiver may increase or decrease or alter the amount of information the target receives to increase ambiguity and cognitive load in the target. Strategies include the following:

- *Increase Information - An increase in information (also known as white-out) by the deceiver reduces the amount of resources the target needs to accurately assess information increasing the risk of not identifying key threats.*

Presence: Current

✓0 ☐ 1 ☐ 2

Relevance: Current

☐0 ✓ 1 ☐ 2

- *Decrease Information - A decrease in information (also known as black-out) by the deceiver the amount of resources the target needs to accurately assess information with risk increased through an inability to identify threats.*

Presence: Current
☐0 ☐ 1 ✓ 2
Relevance: Current
☐0 ☐ 1 ✓ 2

- *Deflection – Through deflecting the target towards information and details irrelevant to the deception operation the adversary increases the amount of resources the target requires to monitor threats, whilst distracting the target from the adversary's real intentions.*

Presence: Current
☐ 0 ✓1 ☐ 2
Relevance: Current
☐0 ✓1 ☐ 2

- *Blocking – Through blocking the target's ability to assess information there is an increase in ambiguity about the adversary's actual aims.*

Presence: Current
☐0 ☐ 1 ✓2
Relevance: Current
☐0 ☐ 1 ✓2

- *Feigning forgetfulness – Through feigning forgetfulness the deceiver reduces the target's ability to uncover information in in-real-life and online encounters reducing the target's ability to detect deception and increasing ambiguity about reality.*

Presence: Current
✓0 ☐ 1 ☐ 2
Relevance: Current
✓0 ☐ 1 ☐ 2

- *Kernel of Truth – This item refers to the principle of developing deception operations around truthful information creating ambiguity for the target to accurately separate fact from fiction.*

Presence: Current
☐0 ✓1 ☐2
Relevance: Current
☐0 ✓1 ☐2

- *What is not being said – This item reflects examining what the current information does not show, as the deceiver may be stating one thing however their past history may indicate they mean something else.*

Presence: Current
☐0 ✓1 ☐2
Relevance: Current
☐0 ✓1 ☐2

- *Keep the Message Simple – This item reflects a common strategy amongst deceivers of keeping the deceptive message simple, which is harder to examine for inconsistencies.*

Presence: Current
☐ 0 ✓1 ☐2
Relevance: Current
☐0 ✓1 ☐2

- *Concealment/Camouflage – This item reflects the controlling of information through reducing the target's access to that information through concealing or camouflaging the information, whether this is an in-real-life encounter in combat operations or assessing online material for concealed messages.*

Presence: Current
☐0 ☐1 ✓2
Relevance: Current
☐0 ☐1 ✓2

- *Dazzle – This item reflects a strategy where the deceiver increases ambiguity in the target by overloading their cognitive abilities or sensors with unimportant information or noise.*

Presence: Current
☐0 ✓1 ☐ 2
Relevance: Current
☐0 ✓1 ☐ 2

- *Distractors – This item reflects a strategy where the deceiver uses distraction methods to divert the target's attention away from the deception at hand. This can include the deliberate targeting of emotionally salient issues which will focus the target's attention.*

Presence: Current
✓0 ☐ 1 ☐ 2
Relevance: Current
✓0 ☐ 1 ☐ 2

Current:

In controlling information the actors are mainly concerned with reducing target access to information through blocking and concealing target access to the actors behaviour, potentially increasing difficulties in assessing information for threats.

N5: Credibility Enhancers

This risk factor reflects tactics that the deceiver may use to enhance their own credibility and/or the credibility of the information that they are employing to deceive the target. These strategies include:

- *Fluency – Through ensuring fluency in behaviour the adversary may appear more credible to the target as their no inconsistencies that may indicate deception.*	Presence: Current ✓ 0 ☐ 1 ☐ 2 Relevance: Current ☐ 0 ✓ 1 ☐ 2
- *Positivity – This item reflects that when a deceiver is positive in their behaviour, particularly verbal behaviour, they are more likely to be judged as credible by their target.*	Presence: Current ☐ 0 ✓ 1 ☐ 2 Relevance: Current ☐ 0 ✓ 1 ☐ 2
- *Objectivity – This item reflects that when an individual or organisation shows objectivity and appears neutral in their behaviour they will be more likely viewed as credible by the target, the adversary will then be able to exploit the target.*	Presence: Current ✓ 0 ☐ 1 ☐ 2 Relevance: Current ☐ 0 ✓ 1 ☐ 2
- *Commitment – This item reflects how an individual or organisation is viewed as credible if they are committed to their behaviour. Particularly in verbal behaviour if they are committed in their statement or information they provide and do not appear tentative or hesitant they will be more likely to be viewed as credible, even if this information is false.*	Presence: Current ☐ 0 ✓ 1 ☐ 2 Relevance: Current ☐ 0 ✓ 1 ☐ 2

- *Convincing – This item reflects how individuals are more likely to believe an individual if they are perceived as appearing convincing, opening up the potential for exploitation by the deceiver.*

Presence: Current
✓0 ☐ 1 ☐ 2
Relevance: Current
☐0 ✓1 ☐ 2

- *Emphasise to influence – This item reflects how deceivers are likely to place emphasis on key points to influence how the target perceives information. Through placing consistent emphasis on particular aspects of behaviour there is a greater chance that the target will focus on these areas enabling exploitation of other areas by the adversary.*

Presence: Current
✓0 ☐ 1 ☐ 2
Relevance: Current
✓0 ☐ 1 ☐ 2

- *Too good to be true – This item reflects how deceivers may frame information in a manner that the target finds hard to believe, increasing ambiguity for the target and requiring further resources to assess credibility.*

Presence: Current
✓0 ☐ 1 ☐ 2
Relevance: Current
✓0 ☐ 1 ☐ 2

- *Showing the real as false – This item reflects how the adversary may show the target real information (whether physical or verbal) to add credibility to false information it is hiding, drawing the target's attention away from other information (e.g. Operation Bagration where Soviet forces used real combat planes and aircraft guns to protect dummy equipment drawing the attention of German forces, whilst concealing their true invasion plans).*

Presence: Current
☐0 ✓1 ☐ 2
Relevance: Current
☐0 ✓1 ☐ 2

- *Subtlety – This item reflects how the subtle presentation of information may manipulate the target into believing information that is false, or to focussing the target towards irrelevant information.*

Presence: Current
☐0 ✓1 ☐ 2
Relevance: Current
☐0 ✓1 ☐ 2

- *Mimicry – This item reflects how mimicry aims to make one thing appear as something else, this exploiting the target's erroneous belief. Mimicry can take many forms across the physical, verbal, non-verbal and online domains.*

Presence: Current
✓0 ☐ 1 ☐ 2
Relevance: Current
✓0 ☐ 1 ☐ 2

- *Dummies – This item reflects objects that are used as false representations of reality which seek to affect how the target interprets information and constructs reality.*

Current:

Actors will be required to be positive, committed, convincing and subtle in their behaviour whilst buying materials or conducting reconnaissance to ensure that they are credible to others, further in conversation with others they will also need to engage in behavioural mimicry as this reflected normal behaviour in interaction.

N6: Social Influencers

This risk factor reflects strategies from social influence approaches which are likely to influence the target into accepting the deceiver and/or information as credible. Social influence strategies include:

Presence: Current
☐0 ✓1 ☐2
Relevance: Current
☐0 ✓1 ☐2

- *Higher Authority – Through appealing to a higher authority (e.g. God) a deceiver may enhance their credibility to others. This strategy will be more relevant to in-real-life and online communication. Malign appeals to higher authority can be used as permission giving strategies for justification of action.*

Presence: Current
☐0 ✓1 ☐2
Relevance: Current
☐0 ✓1 ☐2

- *Authority – This item reflects the fact that figures of authority are judged more persuasive and credible by others, potentially increasing the susceptibility to deception from perceived authority figures.*

Presence: Current
✓0 ☐1 ☐2

- *Referent Power – This item reflects the fact that individuals may be more likely to accept information that has been presented to them by another person they deem credible.*

Relevance: Current
✓0 ☐ 1 ☐ 2

Presence: Current
☐0 ✓1 ☐ 2

Relevance: Current
☐0 ✓1 ☐ 2

- *Attractive – This item reflects that individuals are more likely to find credible people that are attractive.*

Presence: Current
✓0 ☐ 1 ☐ 2

Relevance: Current
✓0 ☐ 1 ☐ 2

- *Reciprocation – This item reflects that individuals are likely to be influenced when they have been given something, as they then want to give something in return, which may leave the target open to exploitation by the deceiver.*

Presence: Current
☐ 0 ✓ 1 ☐ 2

Relevance: Current
☐0 ✓1 ☐ 2

- *Social Proof – This item reflects how we deem information correct through how others also judge that information.*

Presence: Current
✓0 ☐ 1 ☐ 2

Relevance: Current
☐0 ✓ 1 ☐ 2

- *Scarcity – This item reflects that individuals are more likely to be influenced by information that is scarce – potentially as we have had to deploy greater resources to uncover this information.*

Presence: Current
✓0 ☐ 1 ☐ 2

Relevance: Current

✓0 ☐1 ☐2

- *Humour – This item reflects that individuals are more likely to be influenced by information that they may find funny. Individuals may use self-denigration or denigration by others as humour to achieve a tactical or strategic advantage.*

Current:

Actors may use a variety of influence strategies to appear credible to others in purchasing materials for IEDs and conducting reconnaissance on targets. Actors may conduct appeals to higher authority as permission-granting for their behaviour, when interacting with others, actors may appear will aim to appear authoritative and attractive to increase credibility to those who they are purchasing materials from, and social proof will affect how actors are perceived as credible if they are interacting with multiple people from a group when they are purchasing materials.

Deceiver Risk Factors	Coding

D1: Deception Doctrine

Presence: Current

☐ 0 ✓ 1 ☐ 2

Relevance: Current

☐ 0 ✓ 1 ☐ 2

This risk factor reflects the adversary's deception doctrine, including official and unofficial manuals. Does the adversary have deception as part of their military and intelligence doctrine? Under what conditions does the adversary doctrine allow deception to be conducted?

This risk factor is focussed towards identifiable groups and organisations that have guidelines for deception operations, individuals and non-state actors may not have cohesive guidelines for using deception, or they may conduct deception tactically rather than strategically, therefore, further monitoring of any suspicious activity is required.

Current:

Islamic extremists are known to have flexible deception doctrine from manuals and ideas developed by leaders. The actors' deception may be guided by such manuals, careful monitoring is required to examine links between manuals and the actors strategy and tactics.

D2: Gains Vs Losses

Presence: Current

☐ 0 ☐ 1 ✓ 2

Relevance: Current

☐0 ☐ 1 ✓ 2

This risk factor reflects the stakes of the situation for the deceiver and what they may have to gain through deception or lose if they are caught in their deceit. The possibility of deception may be correlated between the levels of gains versus the level of benefits, for example, if there is potential for large gains and low costs then deception should be anticipated, whilst if there is potential for low gains and high costs then the adversary may not conduct deception. However, this may be mitigated by how the adversary portrays the gains and costs involved and what is deemed excessive.

Current:

Deception should be anticipated as there are high gains for the adversaries in concealing their behaviour and there are comparatively low costs if they are caught before their plans are completed.

D3: Motivation

Presence: Current

☐0 ☐ 1 ✓2

Relevance: Current

☐0 ☐ 1 ✓2

This risk factor reflects how motivated the deceiver is to convince others that they are credible. Motivation may affect a deceiver's behaviour in the selection of strategies and length of time spent planning an act of deception. Motivation has also been found to increase the success of deception in online environments, where it is often challenging to assess the credibility of information.

Current:

Actors will be motivated and this will reflect the amount of time they place into sourcing and constructing IEDs and conducting target selection.

D4: Capabilities, Resources and Experience

This risk factor reflects the adversary's capabilities, resources and experience in conducting deception. Adversary capabilities and resources alongside previous experience will affect how credible and convincing the deceiver can be to the target across different communication modes. The deceiver's capabilities, resources and experience will affect their ability to utilise different communication modes and the strategies they use to target and appear credible to others.

Presence: Current

☐0 ✓1 ☐2

Relevance: Current

☐0 ☐1 ✓2

Current:

Prior to identification of individual actors is hard to know what capabilities, resources and experience are available to the group, however, through knowledge of terrorist training manuals and instructions from extremist clerics on deception in operations some capabilities, resources and experience in concealing activities may be anticipated.

D5: Deception Spontaneity → Planned

This factor reflects how the deception is constructed, whether the deception is spontaneous or planned and how far along this continuum the deception may be. Spontaneous deception may have different characteristics and associated behaviours to planned and rehearsed acts of deception.

Presence: Current

☐0 ☐ 1 ✓ 2

Relevance: Current

☐0 ☐ 1 ✓ 2

Current:

The deception will have been planned by the actors as they are required to assemble the materials needed for an IED over a period of time to reduce chance of detection. Target selection may vary depending on context and aims of the group, although this too will require some reconnaissance.

D6: Cognitive Performance

This risk factor reflects the deceiver's ability to engage in cognitively challenging behaviours. Deception is argued to be a cognitively demanding task where individual's need to construct a plausible deception and maintain their account whilst controlling their own behaviour and responding to interactions with the target. If the deceiver is not able to engage in multiple demanding cognitive tasks, behavioural cues to deception may become apparent to observers.

Presence: Current

☐ 0 ✓ 1 ☐ 2

Relevance: Current

☐ 0 ✓ 1 ☐ 2

Current:

The actors will be required to conceal their activities from others, however, unless they are directly challenged about their behaviour, actors should not have trouble in appearing credible to others.

D7: Language

This risk factor reflects the language which the deceiver uses to communicate in. Language differences may present additional challenges to receivers of information through mistranslation or misunderstanding of challenging information, and proceeding difficulties of interviewing individuals to enhance behavioural cues to deception in interactions.

Presence: Current

✓0 ☐ 1 ☐ 2

Relevance: Current

☐0 ✓ 1 ☐ 2

Current:

Language may not play a large role in the concealment of the illegal activities as there may not be direct contact with credibility assessors until actors have been apprehended.

D8: Personality and Individual Differences

This risk factor reflects the effects that personality (normative Vs disordered – the Dark Tetrad of psychopathy, narcissism, Machiavellianism, and sadism) and individual differences (including demographics) have on an individual's actions in online and real-life

Presence: Current

☐ 0 ✓ 1 ☐ 2

environments, the forms of deception in which they may choose to engage in, and their ability to deceive others.

- *Normal Personality*

Relevance: Current
☐0 ✓1 ☐2

The Dark Tetrad consists of the following personalities all of which will present additional challenges when seeking to assess credibility.

Presence: Current
✓0 ☐1 ☐2
Relevance: Current
☐0 ✓1 ☐2

- *Psychopathy is characterised by individuals who lack conscience, are often deceptive and impulsive in their behaviours without regarding the consequences of their actions*

Presence: Current
✓0 ☐1 ☐2
Relevance: Current
☐0 ✓1 ☐2

- *Narcissism is characterised by individuals who seek importance and wish to be viewed this way by others*

Presence: Current
✓0 ☐1 ☐2
Relevance: Current
☐0 ✓1 ☐2

- *Machiavellianism is characterised by individuals who constantly seek to manipulate you for their own gain*

Presence: Current
☐0 ✓1 ☐2
Relevance: Current
☐0 ✓1 ☐2

- *Sadism is characterised by individuals who seek to physically or verbally hurt for their own gain*

Current:

It is anticipated that elements of normative personality and the dark tetrad will be present in groups of actors conducting deception related to acts of terrorism, however, it may be hard to ascertain presence of such factors outside of interactive contexts.

D9: Belief System

This risk factor reflects an individual's or group's belief system including their culture, religion and their political beliefs and allegiances with others. The deceiver's belief system will influence how they interpret the world, their interactions with others and will shape the motive and context from which deception emerges.

Presence: Current

☐ 0 ☐ 1 ✓2

Relevance: Current

☐0 ☐ 1 ✓ 2

Current:

The actors have been radicalised and this will affect the way in which they view the world and their motives for deception, choice of tactics and strategies and their target selection.

Target Vulnerability Factors	Coding
T1: Who is the target? *This vulnerability factor reflects identifying who the target is – whether the target is an individual, group, or organisation and whether the target is a decision-maker or the general public.* **Current:** The target will be the general public and decision-makers.	Presence: Current ☐0 ☐ 1 ✓ 2 Relevance: Current ☐0 ☐ 1 ✓ 2
T2: Stakes *This vulnerability factor reflects the perceived stakes that the target may have in accurately assessing the credibility of information. If the perceived stakes of deception are high this may increase the cognitive load in individual's assigned to assessing credibility and reduce their decision-making abilities.*	Presence: Current ☐0 ☐ 1 ✓2 Relevance: Current ☐0 ☐ 1 ✓2

Current:

The stakes are very high in accurately detecting the actor's concealed behaviour and intent due to the potential for large casualties – this has the potential to affect decision-making abilities and analysts should be aware of this.

T3: Motivation

This vulnerability factor reflects how motivated the target is to detect deception. The motivation impairment effect suggests that when individuals are highly motivated to detect deception their ability to accurately detect deception decreases as they rely upon incorrect decision-making strategies. To overcome this impairment effect it is recommended that practitioners discuss their findings with others to re-evaluate their judgements.

Presence: Current

☐ 0 ☐ 1 ✓2

Relevance: Current

☐0 ☐ 1 ✓ 2

Current:

Analysts are highly motivated to uncover concealment of malign activities; however, judgements should be discussed with others to reduce potential biases.

T4: Target Characteristics

This vulnerability factor reflects the culture, individual differences and personality of the target, and how these may affect the target's ability to analyse and assess the credibility of information and intelligence.

Presence: Current
☐0 ☐ 1 ✓ 2
Relevance: Current
☐0 ☐ 1 ✓2

Current:

Background history will affect individuals seeking to uncover deception due to previous experience of terrorist attacks and the casualties they may inflict influencing judgements.

T5: Mindset - Cognition

This vulnerability factor reflects the cognitive state of the individual or group who are tasked with assessing veracity. As some deception and influence tactics are designed to affect cognitive performance, whether through inundating the target with information increasing cognitive load and reducing ability to accurately assess multiple sources of information, through reducing information leading to individuals and groups requiring more sources to uncover information, or deliberately diverting the target's perception towards other information concealing any deception, highlighting the need for the target to be aware that deception strategies will seek to manipulate target expectation and cognition and reduce available resources towards analysing information.

Presence: Current
☐ 0 ☐ 1 ✓ 2
Relevance: Current
☐0 ☐ 1 ✓2

Current:

Analysts will require greater sources of information to detect concealment of malign activities, potentially reducing resources available for other areas of interest.

T6: Mindset - Affect

This vulnerability factor reflects the affective state of the individual or group who are tasked with assessing veracity. As some influence tactics are designed to affect the emotional state of the target to enhance their attempts at deceit, an understanding of our affective state is important when analysing deception.

Presence: Current
✓0 ☐ 1 ☐ 2
Relevance: Current
☐0 ✓1 ☐ 2

Current:

There are no detected strategies seeking to manipulate emotional state in the information analyst.

T7: Capabilities – Information, Surveillance, Target Acquisition and Reconnaissance (ISTAR)

This vulnerability factor reflects the targets own capabilities and how they will affect the ability to detect deception. Preparation for and experience of past adversary deception alongside deployment of ISTAR capabilities will enable the gathering of information for

Presence: Current
☐0 ☐ 1 ✓ 2
Relevance: Current
☐0 ☐ 1 ✓2

credibility assessment. The greater the number of friendly capabilities in ISTAR the more information may be uncovered for subsequent analysis.

Current:

There are a large number of capabilities to monitor the actors' behaviour across in-real-life and online domains.

Risk Scenarios and Management Strategies

The following tables identify the scenarios of future deception acts. The scenarios are summarised below:

RISK SCENARIOS Identify and describe the most plausible scenarios of future deception			
	Scenario #1	**Scenario #2**	**Scenario #3**
Nature:			
Who are the likely targets of the deception?	General Public and intelligence agencies	General Public and intelligence agencies	General Public and intelligence agencies
What kind of deception is likely to be committed?	Concealment of activities by extremist groups. Deception in-real-life and online interactions with companies from which materials are sourced for IEDs. Potential for in-real-life deception when conducting reconnaissance on target depending on interactions with general public at target.		

What kind of strategy will the deceiver deploy to influence the target?	The deceiver will be using multiple strategies to influence the targets including: conditioning the target; verbal and non-verbal impression management in purchasing materials in-real-life and online domains; controlling information through reducing target access to information (blocking and concealing); increasing credibility by appearing positive, committed, convincing and subtle and engaging in behavioural mimicry during interactions; and social influencers will be used to justify behaviour (Appeals to higher authority), and appearing authoritative, attractive and having social proof when interacting with others.

What is the likely motive – that is, what is the deceiver trying to accomplish?	The motive for the deceivers' behaviour is to successfully detonate an IED causing terror amongst the general public for an ideological and political purpose.
Severity:	
What would be the impact or harm to the target of the deceit?	There would be a large impact to the target potentially through casualties and fatalities amongst the general public, alongside damage to infrastructure and a loss of confidence in security service effectiveness.
What would be the physical harm to the target of the deceit?	The physical harm to the target may be civilian casualties and fatalities and damage to infrastructure.

Is there a chance that the deception could proliferate across multiple mediums and sources?	There is a strong chance that the deception will be conducted across multiple mediums and sources, however, this will not spread outside of the group of actor planning acts of terror.
Imminence: How soon might the deception occur?	It is anticipated that such deception will occur as soon as the group begins developing plans towards conducting acts of terror.
Are there any warning signs that might signal that the risk is increasing or imminent?	Warning signs of increased risk may be linked to actors beginning to attempt to buy materials for IEDs, conducting reconnaissance and moving IEDs to the target location.

Frequency / Duration	
Severity:	
How often might the deception occur – once, several times, frequency?	Deception will occur often during the course of the actors behaviour as they require concealment of information to increase the success of their plans.
Is the risk chronic or acute (i.e., time limited)?	The risk is acute as the actors timeline increases there will be a greater chance of a terrorist act.
Likelihood:	
In general, how frequent or common is this type of deception?	This type of deception is relatively common with acts of terrorist preparation uncovered throughout the year; such acts will dependence on local and global context.

Based on the deceiver's history, how likely is it that this type of deception will occur?	This type of deception around concealment of information and maintaining a credible appearance to others whilst planning an act of terror will occur when groups are planning acts of terrorism.		
RISK MANAGEMENT STRATEGIES **Recommend strategies for managing deception risk (C/F SME Model; Henderson & Pascual (2008); JDP 3-80.1 - DCDC (2007))**			
	Scenario #1	**Scenario #2**	**Scenario #3**
Monitoring: **What is the best way to monitor warning signs that the risks posed by the deceiver may be increasing?**	Monitor changes in deceiver behaviour to identify when they are approaching in-real-life and online retailers of materials that can be used in IEDs – as this will require actors to engage with others rather than		

	focus on information concealment.
What events, occurrences, or circumstances should trigger a re-assessment of risk?	Identify suspicious activity at locations that may be attractive for terrorist attacks. Identification of further actors that may be involved with the terrorist plot, especially if such individuals are known extremists or have links to known extremists. Changes in domestic and foreign affairs that have an effect on the actors' ideological and ethnic community.
Supervision: **What surveillance strategies could be implemented to manage the risk posed?**	Surveillance from human intelligence, image intelligence (photographs of actors conducting reconnaissance of potential targets and buying materials needed) and signals intelligence (monitoring of

	phone conversations and online activity) is required to monitor actors' behaviour for indications they are developing IEDs and/or are about to conduct the attack.
What restrictions on activity, movement, association, or communication are indicated?	Activity should not be restricted until the actors' are in the final stages of planning the attack in an attempt to uncover further actors or contacts and ensure enough evidence for eventual prosecution.
Target Inoculation Planning:	
What steps could be taken to enhance the protection of potential targets?	Increase awareness amongst analysts that deception may be occurring through concealment of information rather than misinformation.

	Companies selling materials that can be used to make IEDs should be aware of potentially deceptive buyers and systems developed to record who buyers are, and why they are buying materials.
How might the targets' security or vulnerability to deception be improved?	Requirements for ID when buying materials that can potentially be used in IEDs – this may act a source of verification of who individuals are and make them more easily identifiable. CCTV surveillance may also improve vulnerability to deception as potential deceivers may be identified faster. Whether this is surveillance in companies selling potentially hazardous materials or at locations which may be attractive to terrorists.

Other Considerations:	
What events, occurrences, or circumstances might increase or decrease risk?	Chances in domestic and global affairs may increase or decrease risk depending on actors perceptions of the justification of their actions.
What else might be done to manage risk?	Conduct social network analysis to identify further actors with extremist beliefs which post a threat to UK or Allied interests.

Appendix 9.4: Detecting Adversaries and Their Intelligence-Gathering Risk Assessment

Deception Risk Assessment Technique (DRAT)©2015

PRESENCE AND RELEVANCE OF RISK FACTORS

Determine the presence of risk factors to and during the most recent pattern of deceptive behaviour, as well as their relevance to the development of future management strategies.

Context of Deception *This section examines the situation in which deception occurs, and how situational elements and actors involved leads to deception*	**Coding** 0 = Absent 1 = Possibility/Low Level Presence 2 = Clearly Present
C1: Situation *This factor reflects upon what the current situation is, what has led to this current situation occurring at this moment in time, and what are the distinguishable elements from the situation which are cause for concern.*	
Current: The current situation reflects on-going adversary intelligence gathering efforts effecting UK capabilities and interests, with particular cause for concern regarding the spreading of	Presence: Current ☐ 0 ☐1 ✓2 Relevance: Current ☐ 0 ☐1 ✓2

misinformation and potential for stealing information whether through social engineering or insiders and the resultant damage this can cause to UK interests and image.

C2: Actors

This factor reflects who the actors are in the current situation: can we identify these actors successfully? Are there multiple actors involved? Who are the key actors? Who, if any, are the subsidiary actors? Are the actors involved individuals, groups or larger organisations? In in-real-life interactions identifying actors may prove challenging if they seek to conceal their identity (e.g. removing military insignia – Ukraine). Online interactions are often characterised by anonymity where identifying actors may prove challenging, and discernible behavioural patterns may be overgeneralised to the actor involved, creating a potentially unreliable profile of the actor.

Presence: Current

☐ 0 ✓ 1 ☐ 2

Relevance: Current

☐ 0 ☐ 1 ✓ 2

Current:

There is potential to identify some of the multiple actors involved through their involvement in groups and known organisations, although some actors may have concealed their identity and adopted false ones. However, actors may prove more difficult to identify in online environments.

C3: Current Threats

This factor reflects what the current threats of the situation are, whether these threats are obvious, concealed or 'ghost' threats designed to waste resources, which area the threat/s is/are emerging from, and which areas of infrastructure these threats are targeting.

Presence: Current

☐ 0 ☐ 1 ✓ 2

Current:

Threats may be concealed or obvious/'ghost' threats designed to waste friendly resources. Threats are emerging from nations seeking to increase their strategic position globally, whether this is through financial or military presence and such threats will target infrastructure related to politics, security and economic interests.

Relevance: Current

☐0 ☐ 1 ✓2

C4: Communication Medium

This factor reflects the communication medium the deception occurs in. Communication mediums include both online and in-real-life domains. Within the in-real-life domain communication may be verbal, vocal, non-verbal (focussing on body language) and physical acts of deception. Within the online domain communication may be verbal, vocal and non-verbal (focussing on body language) and physical acts of deception, across an array of communication mediums (Instant Messaging, email, blogs, video chats, social media networks and deceptive websites).

Presence: Current

☐ 0 ☐ 1 ✓2

Current:

Relevance: Current

☐ 0 ☐ 1 ✓ 2

Deception will occur across multiple communication mediums involving verbal, non-verbal and physical forms of deception.

C5: Online Communication Characteristics

This factor reflects the specific characteristics of online communication where interactions may range from a user interacting with online content where there is no reciprocal communication (e.g. a website, or blog), to interactions where there is reciprocal communication (e.g. email, or Twitter). Online communication is characterised by its ability to cost-effectively reach large-scale audiences in a shorter period of time than traditional communication formats. The anonymity of communicating online may also lead to online disinhibition where individuals may be more likely to disclose information that they would not do so in-real-life, presenting an area for exploitation by deceivers.

Presence: Current

☐0 ☐ 1 ✓ 2

Current:

Adversary agents may seek to conduct deception through the deliberate uploading of misinformation onto online domains, and the potential for social engineering through phone and online messaging domains – such techniques may present challenges in detecting deceit.

Relevance: Current

☐ 0 ✓1 ☐ 2

C6: In-Real-Life Communication Characteristics

This factor reflects the specific characteristics of in-real-life communication in interpersonal interactions. These interactions can be within informal or formal settings and context will affect the characteristics of these interactions. First impressions often guide our interpretation of our interactional partner and form our initial judgements of them, we further adapt and respond to the interactional partner during conversation and can be influence by rapport, and the presentation and confidence of the other person.

Current:

Adversaries may deliberately seek to uncover information or spread misinformation through in-real-life interactions where targets may be easily influenced by a credible persona.

Presence: Current

☐ 0 ✓1 ☐2

Relevance: Current

☐0 ✓ 1 ☐ 2

History

This section examines previous behaviour and interactions to develop a profile of usual adversary behaviour, enabling the identification of non-normal behaviour which may indicate deception

Coding

H1: Previous Behaviour – Non-Deceptive

This factor reflects the previous behaviour of the identified adversaries which is not related to deception. Identifying key goals that the adversary has achieved without using deception enables us to understand the non-deceptive strategies that have been used to achieve these

goals. Subsequently developing a baseline of adversary non-deceptive strategic behaviour, enabling us to identify deviations in behaviour that may indicate deception; although it is important to establish that deviations in behaviour do not have another cause.

Current:

There has been a large amount of non-deceptive previous behaviour with the adversary enabling us to understand how they have achieved key goals without deception in the past.

Presence: Current

☐ 0 ☐ 1 ✓ 2

Relevance: Current

☐ 0 ☐ 1 ✓ 2

H2: Previous Deceiver Interactions - UK

This factor reflects the past interactions that the deceiver has had with UK individuals, groups, organisations and infrastructure. Identifying and analysing previous known successful and unsuccessful deception attempts towards the UK will enable us to develop an understanding of how the adversary conducts and deploys deception strategies against the UK, enabling us to mitigate the risks of these attempts.

N.B. The deceiver may not use the same strategy multiple times against the UK

Presence: Current

☐ 0 ☐ 1 ✓ 2

Current:

The adversary has a history of deceptive interactions with the UK across a long period of time and across varying communication modes, enabling a profile of usual adversary behaviour to be developed.

Relevance: Current

☐ 0 ☐ 1 ✓ 2

H3: Previous Deceiver Interactions - Others

This factor reflects the past interactions that the deceiver has had with other individuals, groups, organisations and nations which are not related to the UK. Identifying and analysing previous known deception attempts, whether successful or unsuccessful, by the adversary towards others may enable friendly capabilities to understand how the adversary conducts deception and identify key strategies they have previously used.

N.B. The deceiver may not use the same strategy multiple times across different targets

Current:

The adversary has a long history of deception towards other nations not linked to the UK enabling a profile of these behaviours to be developed, although they may not deploy the same strategies with the UK due to contextual factors.

Presence: Current

☐ 0 ☐ 1 ✓ 2

Relevance: Current

☐ 0 ☐ 1 ✓2

Nature of Deception Coding

This section reflects the different strategies used to deceive others – For further guidance see research by Henderson et al. on Deception Gambits, Vrij (2008), Whaley (2007)

N1: Create and Identify Vulnerability and Exploit

This factor reflects strategies used in deception which seek to create and/or identify vulnerabilities in the target and then exploit these vulnerabilities for gain. Strategies include

the following:

- *Ruses – This item reflects the intentional exposure of information to the target with the intention of misdirecting them, enabling the deceiver to exploit the adversary whilst their attention is directed towards the ruse (e.g. feeding misinformation to double-agents). Ruses can be conducted by the adversary across multiple levels of communication, whether through in-real-life interactions, through print media, TV, digital media, and other forms of online communication, potentially opening up a wide area for this deception to occur in and requiring a wide-range of resources to target this threat.*

Presence: Current
☐0 ☐ 1 ✓2

Relevance: Current
☐0 ☐ 1 ✓ 2

- *Exploitation of target audience fears – This item reflects the deceiver deliberately identifying and targeting target audience fears through deception, meaning the target will be more likely to spend resources responding to this perceived threat, whilst the deceiver then exploits another area.*

Presence: Current
☐0 ☐ 1 ✓ 2

Relevance: Current
☐ 0 ☐ 1 ✓ 2

- *Exploitation of target audience hopes – This item reflects the adversary targeting audience and exploiting their hopes as part of their deception operation (e.g. attack when claiming peace).*

Presence: Current
☐0 ☐ 1 ✓2

Relevance: Current
☐0 ☐ 1 ✓2

- *Decoys – This item reflects how a deceiver may use a decoy to portray a false target, which the deceiver wants the receiver to believe as credible before they then attack*

Presence: Current
✓0 ☐ 1 ☐ 2

Relevance: Current
✓0 ☐ 1 ☐ 2

or respond to the dummy, wasting friendly resources and enabling exploitation by the deceiver.

- *Feints – This item reflects mock attack or simulation of an attack by an adversary which seeks to create the appearance of an imminent attack, thus tying down friendly resources to countering the implied threat, whilst the adversary may actually perform other behaviour.*

Presence: Current
✓0 ☐ 1 ☐ 2
Relevance: Current
✓0 ☐ 1 ☐ 2

- *Demonstrations – This item reflects a real attack by the adversary which seeks to tie down friendly capabilities in active engagement in one situation whilst other adversary capabilities exploit the target in other areas. This strategy may prove costly to adversary resources as well as demonstrations in physical combat often increase number of casualties, however, this may be affect by adversary beliefs (e.g. if a soldier dies in combat he becomes a martyr and goes to heaven).*

Presence: Current
✓0 ☐1 ☐ 2
Relevance: Current
✓0 ☐1 ☐ 2

Current:

Deception will seek to exploit target audience hopes and fears, and ruses in particular will be used to feed misinformation to the target to direct their attention and resources to one area whilst the deceiver exploits another.

N2: Conditioning the Target

This risk factor reflects strategies which involve conditioning the target into expecting a specific behavioural pattern by the deceiver.

- *Conditioning – This item reflects the deceiver conditioning the adversary into expecting a certain pattern of behaviour over the course of a period time, which then leaves the target open to exploitation when the deceiver performs a different behaviour (e.g. Soviet-Czechoslovakia Campaign 1968 and the Yom Kippur War 1973).*

Presence: Current
☐ 0 ☐ 1 ✓ 2
Relevance: Current
☐0 ☐ 1 ✓ 2

- *Drip-Drip-Feed – Through slowly releasing information to a target, target resources may become focussed on this information, particularly if the adversary feeds truthful information to the target to build trust, before the adversary then presents the target with false information they have worked hard to uncover leading to a less accurate assessment of that information and leaving the target more vulnerable to deception.*

Presence: Current
☐0 ☐ 1 ✓2
Relevance: Current
☐0 ☐ 1 ✓2

- *Influence increase over time – This item reflects how we are more likely to find an individual credible if we are interacting and developing trust with them over a period of time before they then engage in deception.*

Presence: Current
☐0 ☐ 1 ✓2
Relevance: Current
☐0 ☐ 1 ✓2

Current:

Adversary actors will seek to deceive the target over a period of time through conditioning the target to expect certain behaviour whilst feeding the target information over a period of time before false information is given to the target. The target will be further influenced by the deceiver as trust develops over a period of time enabling the deceiver to appear more credible than they actually are.

N3: Impression Management

This risk factor reflects the strategies that individuals engage in order to convince others that they are telling the truth. Individuals may engage in controlling their verbal behaviour (e.g. through keeping statements short to avoid contradictions) and their non-verbal behaviour (e.g. reducing body movements to avoid appearances of nervousness). Impression management occurs both in-real-life and online domains.

Presence: Current
☐ 0 ☐ 1 ✓ 2
Relevance: Current
☐0 ☐ 1 ✓2

Current:

Adversary actors will engage in verbal and non-verbal impression management across in-real-life and online interactions with others, and covert actors in particular will be highly skilled at such behaviour.

N4: Control of Information

This risk factor reflects how information is controlled by the deceiver, where the deceiver may increase or decrease or alter the amount of information the target receives to increase ambiguity and cognitive load in the target. Strategies include the following:

- *Increase Information - An increase in information (also known as white-out) by the deceiver reduces the amount of resources the target needs to accurately assess information increasing the risk of not identifying key threats.*

Presence: Current
✓0 ☐ 1 ☐ 2
Relevance: Current
☐0 ✓ 1 ☐ 2

- *Decrease Information - A decrease in information (also known as black-out) by the deceiver the amount of resources the target needs to accurately assess information with risk increased through an inability to identify threats.*

Presence: Current
☐0 ✓1 ☐ 2
Relevance: Current
☐0 ✓ 1 ☐ 2

- *Deflection – Through deflecting the target towards information and details irrelevant to the deception operation the adversary increases the amount of resources the target requires to monitor threats, whilst distracting the target from the adversary's real intentions.*

Presence: Current
☐ 0 ✓ 1 ☐ 2
Relevance: Current
☐0 ✓1 ☐ 2

- *Blocking – Through blocking the target's ability to assess information there is an increase in ambiguity about the adversary's actual aims.*

Presence: Current
☐0 ✓1 ☐ 2
Relevance: Current
☐0 ✓1 ☐ 2

Presence: Current
✓0 ☐ 1 ☐ 2

- *Feigning forgetfulness – Through feigning forgetfulness the deceiver reduces the target's ability to uncover information in in-real-life and online encounters reducing the target's ability to detect deception and increasing ambiguity about reality.*

Relevance: Current
✓0 ☐ 1 ☐ 2

- *Kernel of Truth – This item refers to the principle of developing deception operations around truthful information creating ambiguity for the target to accurately separate fact from fiction.*

Presence: Current
☐0 ✓1 ☐ 2
Relevance: Current
☐0 ✓1 ☐ 2

- *What is not being said – This item reflects examining what the current information does not show, as the deceiver may be stating one thing however their past history may indicate they mean something else.*

Presence: Current
☐0 ✓ 1 ☐ 2
Relevance: Current
☐0 ✓1 ☐ 2

- *Keep the Message Simple – This item reflects a common strategy amongst deceivers of keeping the deceptive message simple, which is harder to examine for inconsistencies.*

Presence: Current
☐ 0 ✓1 ☐ 2
Relevance: Current
☐0 ✓1 ☐ 2

- *Concealment/Camouflage – This item reflects the controlling of information through reducing the target's access to that information through concealing or camouflaging*

Presence: Current
☐0 ☐ 1 ✓ 2
Relevance: Current
☐0 ✓1 ☐ 2

Presence: Current
✓0 ☐ 1 ☐ 2
Relevance: Current

the information, whether this is an in-real-life encounter in combat operations or assessing online material for concealed messages.

☐0 ✓1 ☐2

Presence: Current

✓0 ☐1 ☐2

Relevance: Current

☐0 ✓1 ☐2

- *Dazzle – This item reflects a strategy where the deceiver increases ambiguity in the target by overloading their cognitive abilities or sensors with unimportant information or noise.*

- *Distractors – This item reflects a strategy where the deceiver uses distraction methods to divert the target's attention away from the deception at hand. This can include the deliberate targeting of emotionally salient issues which will focus the target's attention.*

Current:

Adversary may engage in a range of techniques in controlling information to deceive others and the relevance of tactics will affect the context. Adversaries may decrease, deflect and block the target from information whilst basing information they choose to reveal around partial truth and keeping any narratives simple to avoid inconsistencies.

N5: Credibility Enhancers

This risk factor reflects tactics that the deceiver may use to enhance their own credibility and/or the credibility of the information that they are employing to deceive the target. These strategies include:

- *Fluency – Through ensuring fluency in behaviour the adversary may appear more credible to the target as their no inconsistencies that may indicate deception.*

Presence: Current
☐ 0 ☐ 1 ✓2
Relevance: Current
☐0 ☐ 1 ✓2

- *Positivity – This item reflects that when a deceiver is positive in their behaviour, particularly verbal behaviour, they are more likely to be judged as credible by their target.*

Presence: Current
☐0 ☐ 1 ✓ 2
Relevance: Current
☐0 ☐ 1 ✓2

- *Objectivity – This item reflects that when an individual or organisation shows objectivity and appears neutral in their behaviour they will be more likely viewed as credible by the target, the adversary will then be able to exploit the target.*

Presence: Current
☐0 ☐ 1 ✓2
Relevance: Current
☐0 ☐ 1 ✓ 2

- *Commitment – This item reflects how an individual or organisation is viewed as credible if they are committed to their behaviour. Particularly in verbal behaviour if they are committed in their statement or information they provide and do not appear tentative or hesitant they will be more likely to be viewed as credible, even if this*

Presence: Current
☐ 0 ☐ 1 ✓ 2

information is false.

Relevance: Current
☐ 0 ☐ 1 ✓2

- *Convincing – This item reflects how individuals are more likely to believe an individual if they are perceived as appearing convincing, opening up the potential for exploitation by the deceiver.*

Presence: Current
☐0 ✓ 1 ☐ 2
Relevance: Current
☐0 ✓1 ☐ 2

- *Emphasise to influence – This item reflects how deceivers are likely to place emphasis on key points to influence how the target perceives information. Through placing consistent emphasis on particular aspects of behaviour there is a greater chance that the target will focus on these areas enabling exploitation of other areas by the adversary.*

Presence: Current
✓0 ☐ 1 ☐ 2
Relevance: Current
✓0 ☐ 1 ☐ 2

- *Too good to be true – This item reflects how deceivers may frame information in a manner that the target finds hard to believe, increasing ambiguity for the target and requiring further resources to assess credibility.*

Presence: Current
☐0 ☐ 1 ✓2
Relevance: Current
☐0 ☐ 1 ✓2

- *Showing the real as false – This item reflects how the adversary may show the target*

Presence: Current
☐0 ☐ 1 ✓ 2

real information (whether physical or verbal) to add credibility to false information it is hiding, drawing the target's attention away from other information (e.g. Operation Bagration where Soviet forces used real combat planes and aircraft guns to protect dummy equipment drawing the attention of German forces, whilst concealing their true invasion plans).

Relevance: Current
☐0 ✓1 ☐ 2

Presence: Current
☐0 ✓1 ☐ 2

Relevance: Current
☐0 ✓1 ☐ 2

- *Subtlety – This item reflects how the subtle presentation of information may manipulate the target into believing information that is false, or to focussing the target towards irrelevant information.*

Presence: Current
✓0 ☐ 1 ☐ 2

Relevance: Current
✓0 ☐ 1 ☐ 2

- *Mimicry – This item reflects how mimicry aims to make one thing appear as something else, this exploiting the target's erroneous belief. Mimicry can take many forms across the physical, verbal, non-verbal and online domains.*

- *Dummies – This item reflects objects that are used as false representations of reality which seek to affect how the target interprets information and constructs reality.*

Current:

Adversary actors will engage in a number of tactics to appear credible to others including fluency, positivity, objectivity, subtlety, committed and convincing in their interactions with others, whilst offering real information to the target to make false information seem credible. Actors may also choose to emphasise certain areas of information to direct target attention away from other areas and will also need to mimic behavioural norms to appear credible to the target.

N6: Social Influencers

This risk factor reflects strategies from social influence approaches which are likely to influence the target into accepting the deceiver and/or information as credible. Social influence strategies include:

- *Higher Authority – Through appealing to a higher authority (e.g. God) a deceiver may enhance their credibility to others. This strategy will be more relevant to in-real-life and online communication. Malign appeals to higher authority can be used as permission giving strategies for justification of action.*

Presence: Current
✓0 ☐ 1 ☐ 2
Relevance: Current
✓0 ☐ 1 ☐ 2

- *Authority – This item reflects the fact that figures of authority are judged more persuasive and credible by others, potentially increasing the susceptibility to deception from perceived authority figures.*

Presence: Current
✓0 ☐ 1 ☐ 2
Relevance: Current
☐0 ✓1 ☐ 2

Presence: Current

☐0 ✓1 ☐ 2

Relevance: Current

☐0 ✓1 ☐ 2

- *Referent Power – This item reflects the fact that individuals may be more likely to accept information that has been presented to them by another person they deem credible.*

Presence: Current

☐0 ✓1 ☐ 2

Relevance: Current

☐0 ✓1 ☐ 2

- *Attractive – This item reflects that individuals are more likely to find credible people that are attractive.*

Presence: Current

☐0 ✓1 ☐ 2

Relevance: Current

☐0 ✓1 ☐ 2

- *Reciprocation – This item reflects that individuals are likely to be influenced when they have been given something, as they then want to give something in return, which may leave the target open to exploitation by the deceiver.*

Presence: Current

☐ 0 ✓ 1 ☐ 2

Relevance: Current

☐0 ✓1 ☐ 2

- *Social Proof – This item reflects how we deem information correct through how others also judge that information.*

Presence: Current

☐0 ✓1 ☐ 2

Relevance: Current

☐0 ✓1 ☐ 2

- *Scarcity – This item reflects that individuals are more likely to be influenced by information that is scarce – potentially as we have had to deploy greater resources to*

Presence: Current

✓0 ☐ 1 ☐ 2

uncover this information. - *Humour – This item reflects that individuals are more likely to be influenced by information that they may find funny. Individuals may use self-denigration or denigration by others as humour to achieve a tactical or strategic advantage.* **Current:** Adversary actors have the potential to use a variety of influence tactics to appear credible to others including referent power, being attractive, reciprocating behaviour, social proof and presenting scarce information to the target.	Relevance: Current ☐0 ✓1 ☐2
Deceiver Risk Factors	Coding
D1: Deception Doctrine *This risk factor reflects the adversary's deception doctrine, including official and unofficial manuals. Does the adversary have deception as part of their military and intelligence doctrine? Under what conditions does the adversary doctrine allow deception to be conducted?*	Presence: Current ☐ 0 ☐ 1 ✓ 2 Relevance: Current ☐0 ☐ 1 ✓ 2

This risk factor is focussed towards identifiable groups and organisations that have guidelines for deception operations, individuals and non-state actors may not have cohesive guidelines for using deception, or they may conduct deception tactically rather than strategically, therefore, further monitoring of any suspicious activity is required.

Current:

The adversary has widespread deception doctrine for a large range of contexts and deception is often used in interactions with other nations.

D2: Gains Vs Losses

Presence: Current

☐ 0 ☐ 1 ✓ 2

Relevance: Current

☐ 0 ☐ 1 ✓ 2

This risk factor reflects the stakes of the situation for the deceiver and what they may have to gain through deception or lose if they are caught in their deceit. The possibility of deception may be correlated between the levels of gains versus the level of benefits, for example, if there is potential for large gains and low costs then deception should be anticipated, whilst if there is potential for low gains and high costs then the adversary may not conduct deception. However, this may be mitigated by how the adversary portrays the gains and costs involved and what is deemed excessive.

Current:

There are large gains for adversary actors through planting misinformation as it may direct the target's attention and resources away from other areas which the adversary may then exploit.

D3: Motivation

This risk factor reflects how motivated the deceiver is to convince others that they are credible. Motivation may affect a deceiver's behaviour in the selection of strategies and length of time spent planning an act of deception. Motivation has also been found to increase the success of deception in online environments, where it is often challenging to assess the credibility of information.

Presence: Current
☐0 ☐ 1 ✓2
Relevance: Current
☐0 ☐ 1 ✓ 2

Current:

Actors will be highly motivated to convince others that they and the information they present is credible and this will reflect their selection of deception strategies as they seek to use the ones they perceive as most effective to deceive others across multiple channels.

D4: Capabilities, Resources and Experience

This risk factor reflects the adversary's capabilities, resources and experience in conducting deception. Adversary capabilities and resources alongside previous experience will affect

Presence: Current
☐0 ☐ 1 ✓ 2
Relevance: Current

how credible and convincing the deceiver can be to the target across different communication modes. The deceiver's capabilities, resources and experience will affect their ability to utilise different communication modes and the strategies they use to target and appear credible to others.

☐0 ☐ 1 ✓ 2

Current:

Adversaries have a large range of collective, resources and experience in conducting intelligence gathering and deception operations against the UK and this may be reflected at an individual level in selected experienced or extensively trained operatives as intelligence gatherers.

D5: Deception Spontaneity → Planned

This factor reflects how the deception is constructed, whether the deception is spontaneous or planned and how far along this continuum the deception may be. Spontaneous deception may have different characteristics and associated behaviours to planned and rehearsed acts of deception.

Presence: Current

☐0 ☐ 1 ✓2

Relevance: Current

☐0 ☐ 1 ✓ 2

Current:

The deception will be planned so that adversary actors conceal their intelligence gathering activities and carefully construct misinformation to be used to influence others. However, it

should be anticipated that spontaneous deception will occur according to the contexts that actors find themselves in and what rules there are governing their use of deception.

D6: Cognitive Performance

This risk factor reflects the deceiver's ability to engage in cognitively challenging behaviours. Deception is argued to be a cognitively demanding task where individual's need to construct a plausible deception and maintain their account whilst controlling their own behaviour and responding to interactions with the target. If the deceiver is not able to engage in multiple demanding cognitive tasks, behavioural cues to deception may become apparent to observers.

Presence: Current
☐ 0 ☐ 1 ✓ 2
Relevance: Current
☐ 0 ☐ 1 ✓2

Current:

Actors will have strong cognitive performance ability and may have been selected for such operations due to abilities to present a credible appearance whilst deceiving others.

D7: Language

This risk factor reflects the language which the deceiver uses to communicate in. Language differences may present additional challenges to receivers of information through mistranslation or misunderstanding of challenging information, and proceeding difficulties

Presence: Current
☐0 ✓1 ☐ 2
Relevance: Current

of interviewing individuals to enhance behavioural cues to deception in interactions.

☐0 ✓1 ☐2

Current:

Actors conducting intelligence gathering and misinformation campaigns within the UK will have strong language skills which will enable them to appear more convincing to others. Language difficulties in interviews may only emerge if actors are apprehended and present challenging behaviour during subsequent interviewing.

D8: Personality and Individual Differences

This risk factor reflects the effects that personality (normative Vs disordered – the Dark Tetrad of psychopathy, narcissism, Machiavellianism, and sadism) and individual differences (including demographics) have on an individual's actions in online and real-life environments, the forms of deception in which they may choose to engage in, and their ability to deceive others.

- *Normal Personality*

Presence: Current
☐ 0 ☐ 1 ✓2
Relevance: Current
☐0 ☐ 1 ✓ 2

The Dark Tetrad consists of the following personalities all of which will present additional challenges when seeking to assess credibility.

- *Psychopathy is characterised by individuals who lack conscience, are often deceptive and impulsive in their behaviours without regarding the consequences of their*

Presence: Current
☐0 ✓1 ☐2
Relevance: Current
☐0 ☐1 ✓2

actions

- *Narcissism is characterised by individuals who seek importance and wish to be viewed this way by others*

- *Machiavellianism is characterised by individuals who constantly seek to manipulate you for their own gain*

- *Sadism is characterised by individuals who seek to physically or verbally hurt for their own gain*

Presence: Current
✓ 0 ☐ 1 ☐ 2
Relevance: Current
✓0 ☐ 1 ☐ 2

Presence: Current
☐ 0 ✓1 ☐ 2
Relevance: Current
☐0 ✓1 ☐ 2

Presence: Current
☐0 ✓1 ☐ 2
Relevance: Current
☐0 ✓1 ☐ 2

Current:

Actors will mainly have normal personality types, however, some actors may have Machiavellian tendencies and enjoy deceiving others with little thought of the consequences of such actions. Impulsive behaviour may not common amongst actors as they may have unintended consequences effecting their strategic aims.

D9: Belief System

This risk factor reflects an individual's or group's belief system including their culture, religion and their political beliefs and allegiances with others. The deceiver's belief system will influence how they interpret the world, their interactions with others and will shape the motive and context from which deception emerges.

Presence: Current
☐ 0 ☐ 1 ✓2
Relevance: Current
☐0 ☐ 1 ✓ 2

Current:

Actors belief system will shape their behaviour in concealing information-gathering and misinformation campaigns. Use of deception is widely accepted within the cultural belief system highlighting the ease with which actors may use this as a solution to any issues they face.

Target Vulnerability Factors	Coding

T1: Who is the target?

This vulnerability factor reflects identifying who the target is – whether the target is an individual, group, or organisation and whether the target is a decision-maker or the general public.

Presence: Current
☐0 ☐ 1 ✓ 2
Relevance: Current
☐0 ☐ 1 ✓ 2

Current:

The target is the UK general public, individuals related to adversary intelligence-gathering aims and decision-makers within UK organisations.

T2: Stakes

This vulnerability factor reflects the perceived stakes that the target may have in accurately assessing the credibility of information. If the perceived stakes of deception are high this may increase the cognitive load in individual's assigned to assessing credibility and reduce their decision-making abilities.

Presence: Current

☐0 ✓1 ☐ 2

Relevance: Current

☐0 ✓1 ☐ 2

Current:

In detecting adversary intelligence-gathering and misinformation there are important stakes in identifying and protecting areas of exploitation, although this may not impair judgement and decision-making.

T3: Motivation

This vulnerability factor reflects how motivated the target is to detect deception. The motivation impairment effect suggests that when individuals are highly motivated to detect deception their ability to accurately detect deception decreases as they rely upon incorrect

Presence: Current

☐ 0 ✓ 1 ☐ 2

Relevance: Current

decision-making strategies. To overcome this impairment effect it is recommended that practitioners discuss their findings with others to re-evaluate their judgements.

☐0 ✓1 ☐2

Current:

The target will be motivated to detect deception, however, any impair in judgement will be mitigated by training analysts to focus on validated cues to deception.

T4: Target Characteristics

This vulnerability factor reflects the culture, individual differences and personality of the target, and how these may affect the target's ability to analyse and assess the credibility of information and intelligence.

Presence: Current

☐0 ✓1 ☐2

Relevance: Current

☐0 ☐1 ✓2

Current:

Adversary misinformation may be found more plausible by lay individuals who are more likely to trust others or lack knowledge of how deception appears credible in some communication channels, although analysts seeking to detect adversaries may be more aware of such biases in information interpretation.

T5: Mindset - Cognition

This vulnerability factor reflects the cognitive state of the individual or group who are tasked

with assessing veracity. As some deception and influence tactics are designed to affect cognitive performance, whether through inundating the target with information increasing cognitive load and reducing ability to accurately assess multiple sources of information, through reducing information leading to individuals and groups requiring more sources to uncover information, or deliberately diverting the target's perception towards other information concealing any deception, highlighting the need for the target to be aware that deception strategies will seek to manipulate target expectation and cognition and reduce available resources towards analysing information.

Presence: Current
☐ 0 ☐ 1 ✓2
Relevance: Current
☐0 ☐ 1 ✓2

Current:

Actors will seek to conceal their information-gathering activities through a combination of denying information to the target and directing their attention to other areas of concern. Misinformation will seek to influence the general public who may not be as aware of such attempts at influence, whilst target analysts will require greater resources to uncover attempts at misinformation and misdirection.

T6: Mindset - Affect

This vulnerability factor reflects the affective state of the individual or group who are tasked with assessing veracity. As some influence tactics are designed to affect the emotional state of the target to enhance their attempts at deceit, an understanding of our affective state is

Presence: Current
☐0 ☐ 1 ✓ 2
Relevance: Current

important when analysing deception.

☐0 ☐ 1 ✓ 2

Current:

Attempts at misdirection and misinformation by the adversary will seek to exploit the emotional state of the target and this may be particularly effective with deceiving the general public but may be more easily identified by analysts.

T7: Capabilities – Information, Surveillance, Target Acquisition and Reconnaissance (ISTAR)

Presence: Current

☐0 ☐ 1 ✓2

Relevance: Current

☐0 ☐ 1 ✓ 2

This vulnerability factor reflects the targets own capabilities and how they will affect the ability to detect deception. Preparation for and experience of past adversary deception alongside deployment of ISTAR capabilities will enable the gathering of information for credibility assessment. The greater the number of friendly capabilities in ISTAR the more information may be uncovered for subsequent analysis.

Current:

There are a large number of analysis and surveillance techniques open to friendly analysts in uncovering adversary intelligence-gathering and misinformation and these should be regularly monitored for deception. However, the general public may not have these techniques or knowledge available and be influenced by adversary misinformation.

Risk Scenarios and Management Strategies

The following tables identify the scenarios of future deception acts. The scenarios are summarised below:

RISK SCENARIOS Identify and describe the most plausible scenarios of future deception			
	Scenario #1	**Scenario #2**	**Scenario #3**
Nature: **Who are the likely targets of the deception?**	Concealment of intelligence-gathering will be targeted towards intelligence analysts and decision-makers. Misinformation will target the general public, intelligence agencies and decision-makers.		
What kind of deception is likely to be committed?	The deceiver is likely to conceal their activities and identity, whilst portraying a credible persona and		

	using misinformation to divert the target's attention and resources.
What kind of strategy will the deceiver deploy to influence the target?	The deceiver will seek to exploit audience hopes and fears, whilst using ruses to feed misinformation to the target to divert attention before exploiting another area. The target will be conditioned before preventing them with false information and this will be further effected by the development of trust and rapport by the target towards the deceiver. Actors will engage in verbal and non-verbal impression management to portray a credible persona to others. A variety of tactics will be used to

control information including decreasing available information, and deflecting and blocking attempts to uncover intelligence-gathering activities. Information portrayed to others will be based around partial truths and have a simple narrative to avoid inconsistencies.

The adversary will need to appear fluent, positive, objective, subtle, committed and convincing when interacting with others. They may also offer real information to make false information seem more credible, emphasise some areas to divert attention from others and mimic behavioural norms to appear credible.

Adversaries may influence others

	through referent power, attractiveness, reciprocating behaviour with the target, social proof and presenting scare information to others.
What is the likely motive – that is, what is the deceiver trying to accomplish?	The deceiver is seeking to conceal their intelligence-gathering activities from others whilst also taking available opportunities to spread misinformation to the target.
Severity:	
What would be the impact or harm to the target of the deceit?	If the adversary is undetected then they may be able to gain information on new technologies, sensitive information and cause economic harm.
What would be the physical harm to the target of the deceit?	The target may waste resources and finances developing technology that the adversary is now aware of, and

	there is potential for security implications if the adversary is able to uncover sensitive information.
Is there a chance that the deception could proliferate across multiple mediums and sources?	There is a chance that the deception could proliferate across multiple mediums and sources and this will reflect adversary attempts to develop credible persona and the spread of misinformation may occur in both in-real-life and online environments.
Imminence: **How soon might the deception occur?**	This deception is potentially already occurring.

Are there any warning signs that might signal that the risk is increasing or imminent?	Actors may be identified as building contacts with areas of key interest – which may indicate target selection for intelligence-gathering.
Frequency / Duration Severity: **How often might the deception occur – once, several times, frequency?**	This deception will be on-going and may only stop once actors have been identified and expelled from the UK, however, there may be actors not identified.
Is the risk chronic or acute (i.e., time limited)?	The risk should be considered chronic as it reflects long-term adversary strategy. Times of acute risk may emerge

	during international conflicts and such risks will reflect contexts.
Likelihood:	
In general, how frequent or common is this type of deception?	Adversary concealment of intelligence-gathering is a frequent behaviour – and misinformation may often be used to divert attention away from other strategic aims.
Based on the deceiver's history, how likely is it that this type of deception will occur?	The deceiver's history and culture highlight frequent use of deception as part of policy and in working towards strategic aims, suggesting it is highly likely this type of deception will occur.

RISK MANAGEMENT STRATEGIES Recommend strategies for managing deception risk (C/F Henderson & Pascual (2008); JDP 3-80.1 - DCDC (2007))			
	Scenario #1	**Scenario #2**	**Scenario #3**
Monitoring:			
What is the best way to monitor warning signs that the risks posed by the deceiver may be increasing?	If the adversary is attempting to build up relationships with companies with links to the UK it may suggest that adversary intelligence-gathering is about to start or is already underway. If the adversary nation becomes involved in conflict then there will be more risk from misinformation or even outright deception towards the UK general public and decision-makers.		
What events, occurrences, or	Re-assessment of risk should be		

circumstances should trigger a re-assessment of risk?	conducted if the adversary nation has sudden changes in its foreign affairs, especially if the nation becomes involved in a conflict. If there is a large increase in the number if identified adversary actors operating in the UK then a re-assessment of risk will be required to identify their motives and reasons for their presence.
Supervision: **What surveillance strategies could be implemented to manage the risk posed?**	Key industries that might be targeted by adversary information-gathering should be monitored to detect any attempt at exploitation. Identified actors should be made subjects of surveillance to monitor who they are interacting with, to identify potentially further adversary

	actors.
What restrictions on activity, movement, association, or communication are indicated?	Only if serious threat is posed by identified adversary actors then they should have their movement's restricted – if the threat they pose is not large then they should be monitored to identify further actors and this will also enable them to be fed with misinformation to send back to the adversary.
Target Inoculation Planning: **What steps could be taken to enhance the protection of potential targets?**	Companies need to be sure that individuals approaching their business are verified across a range of sources to ensure that they are credible – particularly if these companies are working in areas of technological development and/or

	have links to government agencies or interests.
How might the targets' security or vulnerability to deception be improved?	Informing such companies of the potential for deception to occur – companies are already aware of the potential for cyber-attacks however cognitive hacking needs to be addressed in companies security policies.
Other Considerations:	
What events, occurrences, or circumstances might increase or decrease risk?	Changes in international affairs may increase or decrease risk – if the adversary's nation is involved in conflict they may deploy misinformation strategies or seek to direct the target's attention towards other areas.

What else might be done to manage risk?	Use counter-intelligence assets to feed misinformation to adversaries in their intelligence-gathering, which will enable the adversary to then develop an incorrect profile affecting their strategy.