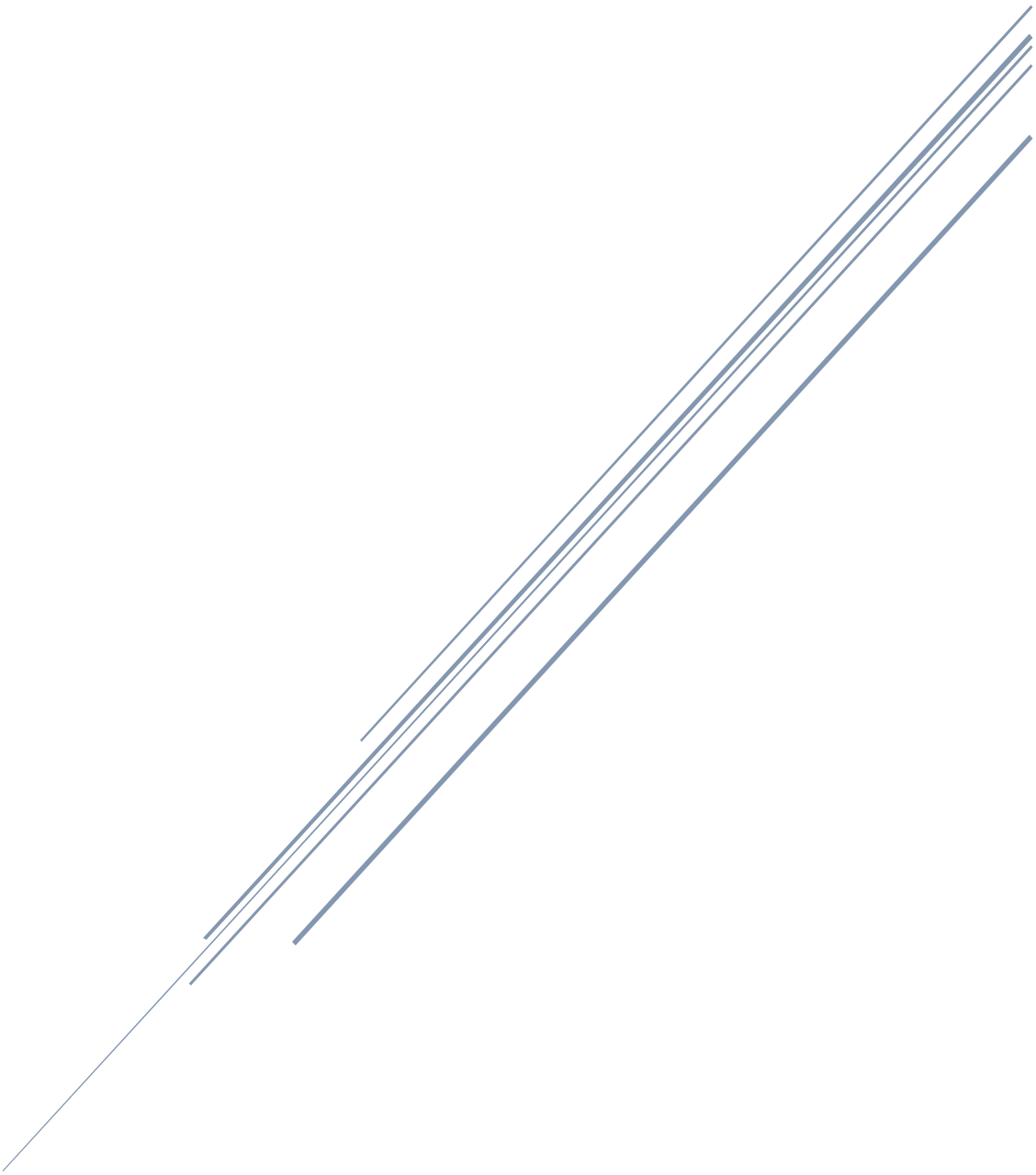
SECURITISING CYBER-CAPABILTY: AN ANALYIS OF NORM CONSTRUCTION METHODS

Alexi Drew



Royal Holloway, University of London
Submitted for the degree of Doctor of Philosophy in Political Science
2018

Declaration of Authorship

I, Alexi Daniella Drew hereby declare that this thesis and the work presented in it entirely my own. Where I have consulted the work of others, this is always clearly stated.

Signed: Alexi Drew

Date: 22/02/2019

Abstract:

Cyber-security as an area of study within international relations has exploded into public view in recent years. Notable and spectacular cyber-attacks directed against states such as Estonia in 2007 and Georgia in 2008, alongside the growing furore over allegations of Russian interference in democratic elections in the United States, the United Kingdom and a number of other states have prompted not only public outcry but a rapid growth in academic literature seeking to further understand the implications of these events.

The aim of this thesis is to seek to understand the means by which these states and other actors have shaped, or more accurately, taken part in the construction of norms regarding cyber-capability that suit their own interests. This approach seeks to circumvent the contested nature of a large portion of cyber-security literature which often struggles to escape the complexities ascribed to it by confusion over the meaning of specific terms.

In order to offer an explanation as to how these norms have been constructed, I will create and propose a set of theoretical concepts that are based out of the combination of norm emergence theory – as proposed Finnemore and Sikkink – and Securitisation theory. I will expand upon both of these theoretical foundations while also combining them to suggest a process of norm securitisation which can be used to explain not only the means by which norms regarding cyber-capability have been constructed.

I will test my new theoretical framework of *norm securitisation* and *operationalised norm construction* upon a series of contemporary case studies that cover cyber-war, cyber-terrorism and cyber-surveillance. The theory I propose will not only be able to explain the means by which norms are constructed around these three cyber-security issues, but can further be employed as a critical tool against a wide range of norm construction processes where there exists a security component.

Acknowledgements…

While the words and ideas, late nights, and caffeine addiction contained within the following pages are my own, the existence of this work depends on so many more. I simply could not have completed such an undertaking without the support and faith placed in me by others. While I cannot mention them all, I wanted to acknowledge and thank my greatest contributors here, at the start of my work.

Firstly, I would like to thank Professor Ben O'Loughlin, my academic supervisor and guide upon this odyssean journey which has finally come to an end. He has been a stalwart mentor and has steered me true despite my own best efforts to stray from the path. Thank you.

Next, my thanks are directed at the various heads of department under which I have worked while at Royal Holloway. To each of you – Nathan Widder, Alistair Miskimmon and Sandra Halperin – I have created more complication and confusion than you deserve. Yet, you met each of my problems and my missteps with surety and compassion. Thank you.

I would like to thank Dr Michelle Bentley. A late arrival to my supervisory team, but a welcome one. On top of this I have had the great pleasure of teaching alongside you for the past five years. The passion and fulfilment that I get from teaching is a result, in no small part, of the trust and genuine camaraderie that you gave me. Thank you.

It would be remiss of me in the extreme not to thank my family alongside these others. Toby, it's been a long time coming and through it all you've had more faith in me than I have, at times, had in myself. Without your steadfastness I would not have been able to complete this work, without you behind me I would never have achieved so much. Thank you, I love you. Mum, Dad: you've pushed, tugged, cajoled, threatened, clothed, fed, loved, cared and so much more for me over so many years. All of these things have made me who I am and enabled me to achieve a potential which I never thought I could. I cannot thank you both enough.

Lastly, I would like to dedicate this work to a man who didn't get to see me finish my odyssey: my grandfather. A man like no other, who called me 'professor' from the day I started my doctorate. I hope I've done you proud and I will do my best to live up to your high standards. This is for you…

Table of Contents

Table of Figures

Chapter 1 – Introduction

A Crisis of Norms

In May 2013 a number of international newspapers including *The Guardian* and *Der Spiegel* began to public articles based upon leaked documents provided by an ex-contractor of the United States' Central Intelligence Agency (CIA) (Borger et al., 2013; Der Spiegel, 2013). The documents provided by Edward Snowden to these news outlets shed light upon the manner in which states, most notably the US and the United Kingdom (UK) employed digital-surveillance techniques to harvest and examine the data produced by the global population's increasing reliance and mass uptake of internet enabled communications and sources of information. The public discourse which followed these released evidenced a rejuvenation of arguments concerning the proper level of power vested in the state, and the balance that must be struck between individual privacy and security (Kettle, 2015). States and the international institutions to which they belonged found themselves increasingly at odds with the manner in which they reacted to these debates. The European Union (EU) began to divest itself of legislative material which justified and provided the framework for surveillance programmes of its member states (Digital Rights Ireland, 2004; Court of Justice of the European Union, 2014; Arthur, 2014). At the same time states such as the UK shored up these same programmes with new legal foundations ('EU data ruling goes against UK government', 2016), even going further and extending these powers in spite of the European Court of Justice's (ECJ) rulings on the illegality of the surveillance methods being empowered. Such stark divergence presents a number of questions. How is it that legislation and powers that appear to be counter to the institutional position held by the EU resist the pressure against them? If these powers and laws are evidence of a dominant normative position what about the nature of this norm has led to its acceptance and continued legitimacy despite the challenge to the narrative presented by Edward Snowden and then taken up by the EU?

In October 2016 the US Office of the Director of National Intelligence (ODNI) and the Department of Homeland Security (DHS) released a joint statement which contained the following:

> The U.S. Intelligence Community (USIC) is confident that the Russian Government directed the recent compromises of e-mails from US persons and institutions, including from US political organizations. The recent disclosures of alleged hacked e-mails on sites like DCLeaks.com and WikiLeaks any by the Gucifer 2.0 online persona are consistent with the methods and motivations of Russian directed efforts. These

> thefts and disclosures are intended to interfere with the US election process. Such activity is not new to Moscow – the Russians have used similar tactics and techniques across Europe and Eurasia, for example, to influence public opinion there. We believe, based on scope and sensitivity of these efforts, that only Russia's senior-most officials could have authorized these activities.
>
> (Department of Homeland Security and Office of the Director of National Intelligence, 2016)

Russian interference in the US Presidential election marks a significant undermining of international norms of non-interference between state actors. When taken in context with other Russian efforts to influence and undermine the democratic systems in a number of European and allied states across several years this suggests not only a weakness in previously dominant international norms of restraint and non-interference, but a process of counter-construction which is potentially successfully supplanting its non-confrontational predecessor. Similarly, the way the United Kingdom resisted the institutional normative shift of the European Union towards digital privacy and human security and instead maintained a normative position that prioritised state security over human security suggests the existence of a more resilient form of norm construction.

As these examples and other provide evidence of state's efforts to expand their cyber-capability towards both domestic security issues and inter-state affairs they also suggest that there is a concurrent shift in previously accepted normative positions. In this thesis I will explain that the resilience of domestic orientated norms regarding digital surveillance in the United Kingdom and the weakness of international norms regarding the development and use of cyber-capability are both related to the means in which these norms are constructed.

This explanation will rest upon two concepts which this thesis will seek to demonstrate through a number of case studies covering three principal topics within cyber-security and capability; cyber-war, cyber-terrorism and cyber-surveillance. These two concepts – operationalised norm construction and Norm Securitisation – provide the theoretical basis for understanding how policy makers and state actors can effectively subvert the presupposed discursive nature of norm construction in order to reach a normative position that best suits that actors interests.

Norm Securitisation draws upon norm emergence theory, as outline by Martha Finnemore and Katherine Sikkink, and Securitisation theory. Norm securitisation is the process by which a norm is constructed or re-constructed to support policy or action which would usually be

outside the realms of what could be considered normal politics. This is achieved by means of constructing a connection between a particular object which is under significant threat and the necessity of the preferred normative position as the most effective way to counter this threat. This process of *securitised norm construction* will be extrapolated and examined through a study of the United Kingdom's cyber-surveillance policy material, particularly regarding events in the aftermath of Edward Snowden's revelations on the activities of the United States National Security Agency (NSA) and the United Kingdom's own signals intelligence division, GCHQ.

Norm securitisation is best understood as an overt process, constituted as it is by open, discourse driven acts by political actors seeking acceptance of their securitised set of norms and thus the ability to enact policy which is now justified despite its normally untenable nature. The second key concept that this thesis extrapolates from the international developments of cyber-security is a far less transparent component of norm construction processes. Operationalised norm construction is, in many ways, a direct opposite in nature to the process and its means that is explored by Finnemore and Sikkink in their explanation of norm emergence theory. Whereas norms are suggested in their text to be predominantly built through negotiation, cooperation and the overt recognition of shared standards *operationalised norm construction* is opaque. The process in which norms are constructed is based upon the active participation in activities that fit within the bounds of the actors preferred normative framework and the success of this active construction is based around whether there is sufficient counter-action taken to discourage this normative from continuing.

The purposes of this thesis, in the chapters which follow, is to examine how the norms regarding cyber-capability development and deployment are being constructed at both the domestic and international level. The study of cyber-security issues – warfare, surveillance, and terrorism – provide a testbed in which the concepts of securitised norm construction and operationalised norm construction can be contextualised. It is the goal of this thesis to formulate a new process for understanding how with regards to international security issues state actors can engage in a manner of norm construction which provides a greater strategic advantage and rapid emergence within the international sphere and a higher resilience within the domestic.

Hypothesis

This thesis will seek to test the following hypotheses, aiming to ascertain the validity of the theoretical concept of securitised norm construction, securitisation and emergence, the nature

and role of securitising norm entrepreneurs, the comparative efficacy of discourse driven versus operationalised methods of norm construction, and the nature of the relationship between the two new proposed forms of norm construction.

1. That governments engage in a process of securitised norm construction when the related policy or capability sought would usually be outside the bounds of normal politics.
2. That securitised norms constructed through operational construction, the physical application of the policy or tools which they enable, allows for a more rapid, effective and resilient formation of the related norms.
3. That operationalised norm construction is the pre-requisite for their being discursive norm construction, securitised or otherwise. Discursive norms are, in effect, reactionary.

With the examination of these hypothesis this thesis will propose an expanded concept of norm construction which builds in specific means for explaining how security-oriented norms can be constructed by states in a manner which can result in significant upset of previously established standards. This framework will not only be able to provide a better means of understanding the implications of cyber-capability building by states and the use of misinformation campaigns by others, but a tool through which other current and future instances of norm construction might be better understood.

These hypotheses seek to situate the two key theoretical components of this thesis, securitised norm construction and operationalised norm construction, within the wider normative framework and simultaneously assess their relationship to each other. Together they support the conclusions that there is an ordinal relationship, in terms of the resilience and comparative ease of uptake, between norms constructed through operationalised means and discourse driven means. This thesis argues that, with regards to cyber-capability oriented norms, states are preferentially engaging in processes of norm construction that are either solely based upon operationalised means or incorporate operationalised components. Further I argue that this decision is made as a result of the implicit understanding that when it comes to constructing norms actions speak louder than words, that significant strategic advantages can be gained through a process of norm construction that subverts and circumvents institutionalised processes that rely upon the diplomatic, discourse driven approach. I suggest that this applies in both and inwards and outwards facing manner.

Methodology: A Case Study and Discourse Analysis Approach

Each analytical chapter of this thesis will consider a cyber-security issue and the processes of normative construction with which that issue is connected. Each of these issues, cyber-war,

cyber-surveillance and cyber-terrorism will be examined through the consideration of case studies which will be examined for their impact upon related norm construction. These case studies will cover both domestic facing and international facing norms and involve, especially in the case of the domestic setting, a discourse analysis of related statements and policy debates.

Cyber-terrorism and Cyber-surveillance: The British Case Study

For the cyber-terrorism and cyber-surveillance cases the centre for my enquiry will focus around the policy discussion and the actions within this space of the United Kingdom. The interrelation of acts of terrorism, cyber or otherwise, and the development, justification and legislating for increased powers of surveillance by the United Kingdom's government of its domestic population provides for an insightful and rewarding case study for analysis.

The normative position of both the United Kingdom and the European Union regarding the necessity for digital surveillance of domestic populaces in order to effectively provide the capability to defend against terrorist and state threat, as evidenced in the EU's Data Retention Bill and the United Kingdom's interconnected and reliant Regulation of Investigatory Powers Act (RIPA), provides an effective window into the interplay between security concerns and the construction or counter-construction of norms. The releases of classified information from Edward Snowden served to make this case study even more attractive as a source for examining the nature of the norm construction process within a security and cyber related setting. With these released detailing the practical implications of the security regimes and capabilities enacted under the dominant normative framework shared by the UK at the domestic level and the EU at the institutional – the position that strategic security should take priority over privacy and human security issues – the EU enacted a volte face while the UK sought to further entrench this position. The language and attached imagery that was employed by the UK to achieve this goal provides a significant resource for testing of this thesis' hypothesis concerning norm securitisation.

The case study provided by the United Kingdom's reaction to the Snowden revelations provides the opportunity to examine the reinforcing, the entrenchment of a norm which had come under threat as a result of a contrary narrative supported by newly emerged factual evidence. This case study then allows for the observation and analysis of how a threatened norm can be strengthened through a securitised process of securitised norm construction. This is not an example of an emergence process, instead this case study examines how security related norms can shrug off the challenge of de-securitising normative pressures through the reiteration of its credentials and the effective use of securitising political acts and speech.

My initial intention regarding the testing of my first hypothesis through this British case study was to first examine the discourse presented in policy debates and documentation and then cross-examine the outputs of this analysis by interviewing the political actors who had contributed to these same debates and documents. This approach was thwarted by the potentially predictable fact that none of the members of parliament that I approached regarding this stage of my research were willing to discuss their potential input into a process of norm securitisation that aimed to provide the space for digital-surveillance policy and powers.

As an alternative source material this thesis, particularly chapters four and six will draw upon Hansard, the collection of recorded debates in the House of Lords and the House of Commons. These debates, gathered across a period covering three different governments, provides a significant body of material with which this thesis can test key hypothesis regarding norm securitisation surrounding digital surveillance and the construction of policy and norms surrounding the countering of cyber-terrorism.

Cyber-war: Russian Disinformation and US Force Multiplication

In 2016 the United Nation's deliberative norm building process towards shared international norms, in the form of the Group of Governmental Experts, collapsed in disarray after the group was unable to reach a consensus regarding its recommendations. This is despite previous meetings of the GGE having successfully reached shared agreements and published its findings and suggestions for future development of the project.

This schism has since seen the emergence of two simultaneous processes within the UN alone. One of these argues for the importance of a clear position that entwines the norms in question with those already expressed in international humanitarian law and enshrines the ability of state actors to defend themselves and likewise to expect punitive responses should Internet Communications Technologies (ICTs) be used to attack another state. The contrasting side of the division in this norm constructive process is summarised by the following statement:

> I must register our serious concern over the pretension of some, reflected in paragraph 34 of the draft final report, to convert cyberspace into a theatre of military operations and to legitimize , in that context, unilateral punitive force actions, including the application of sanctions and even military action by States claiming to be victims of illicit uses of ICTs.
>
> We consider unacceptable the formulations of the draft, aimed to establish equivalence between the malicious use of ICTs and the concept of "armed attack", as

> provided for in Article 51 of the Charter, which attempts to justify the alleged applicability in this context for the right to self-defense.
>
> (Rodriguez, 2017)

This, written by the representative of Cuba to the GGE describes a significant breaking of the normative process within the UN. Notably the GGE had, previous to 2017, managed to meet and to formulate outputs based upon a shared consensus. In the concluding remarks of this statement by the representative of Cuba however it is made clear that a number of parties represented in this group feel that not only can consensus not be achieved at the current moment, but that any progress towards creating a set of norms based upon cooperation and stability now rely upon a reformulation of the process which is open to all members of the General Assembly.

In the midst of the legal gap that the GGE was intended to work towards filling there have been a number of notable instances where it would appear that this legal and normative gap has been exploited. The example of Russian interference with the 2016 US presidential elections provides not only further justification for the closing of this legal and normative gap, but an insight in to how this gap can be exploited and entrenched by a competing form of norm construction by state actors.

This thesis in chapter five will use the case study of the United State presidential election campaign as the basis for my analysis of operationalised norm construction and how this form of norm construction provides significant advantage to its users in preferentially shaping norms, destabilising international efforts regarding cooperation and governance, and as an added feature leads to the increased proliferation of the methods this set of norms allow.

This case study further allows for the comparative examination of how two states, Russia and the United States, view and employ cyber-capability as a tool of international politics. These two state's positions regarding the definition and application of cyber-warfare is at significant odds. Much as it will be discussed in this thesis' literature review how the academic concept of cyber is contested the same is certainly true of the strategic concepts held by these two opposing nations. To support this the conclusions of this thesis as to how the relative structural weakness of discourse developed normative processes are being purposefully exploited through an operationalised means of norm construction further examples of Russian interference in opposing states will be drawn upon. These examples include Germany, France and the UK. Together they illustrate that operating alongside the discourse driven norm construction process embodied in the UN GGE – embattled and shriven in two as it is – is an

operationalised process of norm construction enacted by a Russian state seeking to gain strategic advantage over opposing states while simultaneously enthroning norms which support the strategic tool which has provided it with such an advantage.

The US and Russian case studies will also further support this thesis' hypothesis regarding the resilience of norms constructed through operationalised means of construction. In the fifth chapter I will argue that operationalised means of norm construction gain traction when the acts which serve to build these norms are uncontested, contested in insufficient fashion or are countered by actors whose own actions undermine their legitimacy. The US provides case study examples of all of these points. The US response to Russian interference in the Presidential election campaigns, as well as international responses, provide examples of attempt to curtail Russian electoral and social interference at different levels of punitive intensity. The history of the US in its use of complex cyber-attacks against opposing states, operating beneath the same threshold and level of plausible deniability as Russia's campaign of misinformation, supplies an example of undermined legitimacy in counter-normative response.

This chapter on cyber-war, will, through the American and Russian case studies demonstrate how Russian actions within an undefined, opaque normative and legal space has strengthened the normative position constructed through this operationalised means of norm construction. It will demonstrate how, simultaneously, the actions of the US within this same uncertain normative and legal domain of warfare has undermined the ability of the United States to act as an effective norm entrepreneur seeking to counter the Russian position. Well documented examples of cyber-attacks against nation state infrastructure by the US, such as STUXNET, fatally undermine the credibility and thus efficacy of American efforts to counter the Russian norm with an alternative.

Conclusions: The Advantages of a Securitised and Operationalised Approach to Norm Construction

This thesis will use its examination of the above case studies and the methodologies discussed to demonstrate the existence of a process of norm construction that can be purposefully adopted by states, as norm entrepreneurs. This process allows states to construct the basis of public and legislative support for domestic policy which breaches previous normative boundaries. It allows state actors at the international level to gain strategic advantage over their adversaries through the exploitation of limited existing normative or legal constraint. Concurrently this process shapes these same norms and encourages the adoption of the tools

justified by this new position by a broadening array of international actors interested in gaining the same strategic advantage.

In the domestic setting states can draw upon the unintended operationalised norm constructive impact of terrorist actors who engage in acts which can loosely be called cyber-attacks to fuel their internal securitisation of norms concerning digital surveillance. In the international sphere states can gain strategic advantage while simultaneously setting normative values that allow for the maintenance of that advantage. Cyber-attacks carried out against opposing states and misinformation campaigns achieve the strategic goals of destabilisation while simultaneously undermining the developing norms of cyber non-interference and thus creating the opportunity to further employ this methodology both for the originator of this active form of norm construction but for the other state actors who, in seeking similar strategic advantage, begin to take up and employ the same tools, providing for an operationalised version of the move towards norm cascade described by Finnemore and Sikkink (1998, p.895).

It is the goal of this thesis to not only examine the manner in which state and non-state actors have shaped norms concerning cyber-space and its use, but to formulate – through the analysis of this set of security issues – a theory of norm construction which can be used to understand the process of norms construction in a wide variety of instances where their exists a security element. The main focus of this thesis may be the examination of cyber-security related issues and their related processes of norm construction however, the conclusions that I reach regarding the manner in which norms can be securitised and how operationalised methods of construction influence this process are applicable far beyond this specific set of issues. With international politics seemingly becoming more confrontational, with previous animosities reasserting themselves and the resurgence of the language and actions of a Cold War era my additions to our understanding of the construction of norms specifically within a securitised paradigm offers another means of interpreting the actions of policymakers and central actors.

Chapter 2 – Literature Review

A Contested Lexicon

The term cyber-security is as popular the current media and policy discourse as it is contested within the academic one. Cyber as a term has been appended to a vast array of policy issues within the security field alone: cyber-war, cyber-terrorism, cyber-crime, cyber-weapons, cyber-deterrence to name but a few. This has simultaneously resulted in an exponentially increasing body of work seeking to place issues of cyber-security within the broader field of security studies. While some of these efforts have begun to produce notable contributions to our understanding of how networked technologies interact with theories of international relations and security there are still significant gaps in the literature. A great deal of the advancing coverage of cyber-security issues by academic analysis is intended to conclude as to the scale or nature of any changes that might be wrought on existing issues of international security by the development and deployment of the various technologies which rest within this broad and contested concept.

This literature review focus upon these attempts with specific focus upon the three major components of cyber-security to which the rest of this thesis will direct its analysis. I will examine the literature regarding cyber risk and framing which has been so far directed at cyber war, cyber surveillance and cyber terrorism. Within this literature I will cover the broad questions relating to the evolutionary or revolutionary nature of cyber-capability regarding its impact upon warfare and whether cyber war can in fact take place or not. Concluding from this analysis that there is a significant disconnect between the theoretical examination of this concept and the reality which is applied by state actors I will demonstrate a symptomatic problem with the contested nature of security issues upon which cyber has been appended – a tendency for theoretical abstraction which is left behind by the phenomenon itself.

From cyber war I will then consider the literature on cyber-terrorism. The main themes that to draw out form this literature is that cyber terrorism is not only as contested a term as cyber war, but that there is a similar disconnect between conclusions as to actual risk from this phenomenon based upon empirical and theoretical analysis and the perception or at least the apparent perception of key actors.

Finally, it is through the analysis of literature concerning cyber-surveillance and a common strand within this literature that I will draw attention to a gap in the literature that not only ties all three of these issues together with regards to my proposed theoretical framework, but which also demonstrate the gap in existing analysis that my work will seek to fill. A significant

proportion of literature concerning the framing and development of digital surveillance tools probes the problematic relationship between the drive for physical security and the impacts upon central components of human security, such as privacy. This literature effectively avoids the contested nature of the previous two topics through a thorough grounding in case study analysis. This results in an analysis which effectively connects the theoretical concepts involved with the reality of their application and the issues that this creates. It is this methodological and conceptual approach which I will then seek to turn towards cyber war and cyber terrorism as well as the interconnection between the latter and cyber surveillance.

Cyber War

Cyber war has likely enjoyed the most significant and certainly the most long running attention from academics and policymakers out of the three categories that this thesis will consider. Across the academic and policy discussions of this topic there have been a number of common threads with regards to the intersection of existing concepts of war and conflict with emergent networked technologies. The most preeminent of these debates centres around the contested nature of the cyber component mentioned early – will cyber war take place or will it not? The literature around this broad question has recently developed in a more nuanced manner, but at its early stages was heavily binary. Academics such as John Stone argued that cyber war was an inevitable outcome of the militarisation of a technology that has become widespread and offers significant military advantage (Stone, 2003) whereas others such as Thomas Rid have argued that cyber war will not take place, as the conception of cyber war to which we base this analysis is incapable of fulfilling the basic requirements of an act of war: violence (Rid, 2003, p.1).

Here both Rid's and Stone's analysis highlight the problematic nature of the concept of cyber war. That what is intended by the addition of the term cyber in one circumstance is often significantly at odds with what another analyst or policymaker intends to cover by that term. This, unsurprisingly, leads to a contested term which requires careful framing when seeking to engage with it analytically or critically. The confusion created by this definitional obscurity makes the answering of even this seemingly simple predictive quandary regarding the likelihood of cyber war incredibly problematic. What both Stone and Rid miss – in a manner which is synonymous with the academic literature regarding cyber war at this time – is that the route of their distinct and contradictory conclusion could be circumvented through recognition that the actions of actors within this space had already begun to make the question itself defunct. State investment in military programs that were designed to develop the capability for their owners to commit acts of violence and achieve military goals through the use of

cyberspace had already begun , and are now highly developed and often core components of modern military strategy.

Cyber war has likely enjoyed the most significant and certainly the most long running attention from academics and policymakers out of the three categories that this thesis will consider. Across the academic and policy discussions of this topic there have been a number of common threads with regards to the intersection of existing concepts of war and conflict with emergent networked technologies. The most preeminent of these debates centres around the contested nature of the cyber component mentioned early – will cyber war take place or will it not? The literature around this broad question has recently developed in a more nuanced manner, but at its early stages was heavily binary. Academics such as John Stone would argue that cyber war was an inevitable outcome of the militarisation of a technology that has become widespread and offers significant military advantage (Stone, 2003) whereas others such as Thomas Rid have argued that cyber war will not take place as the conception of cyber war to which we base this analysis is incapable of fulfilling the basic requirements of an act of war: violence (Rid,2003).

The definitional quagmire contributed to by Rid and others in an effort to frame what is meant by cyber war has further led to a secondary set of extreme conclusions as to the likely implications of the militarisation of this technology and cyberspace. The extreme nature of these conclusions, suggesting often cataclysmic outcomes as a result of the addition of cyberspace to the list of military domains has further acted to define and ensconce a framing of cyber war as not only being at significant risk in terms of eventuality but in terms of impact as well. A good example of such literature is found in the work of Richard Clarke and Robert Knake. Their introduction to the concept of cyber war and its implications read as follows:

> While it may appear to give America some sort of advantage, in fact cyber war places this country at greater jeopardy than it does any other nation. Nor is this new kind of war a game or a figment of our imaginations. Far from being an alternative to conventional war, cyber war may actually increase the likelihood of the more traditional combat with explosives, bullets and missiles. If we could put this genie back in the bottle, we should, but we can't. Therefore, we need to embark on a complex series of tasks: to understand what cyber war is, to learn how and why it works, to analyse its risk, to prepare for it, and to think about how to control it.
>
> (Clarke and Knake, 2010, pp. xiii)

While the closing sentence of this quotation suggests a perfectly reasonable set of requirements for an academic analysis of what still is a relatively new phenomenon the early segment is more reflective of the general tone of this work and of many other pieces of literature like it. Further examples of a similar tone can be found within work examining technologies such as the Dark Net by Jamie Bartlett (2014) and implications regarding dissolving ethical constraints in future wars as considered by Christopher Coker (2013). The apocalyptic language used in framing a future shaped by cyber war has further been translated into the language employed by military officials and policymakers. References to the potential for a cyber-hiroshima (Hayden in Shinkman, 2013), a cyber Pearl Harbour (Panetta in Ryan, 2011) and most recently cyber Blitzkrieg are clear examples of how the academic framing of cyber war as a revolutionary shift which without fail will lead to extreme scenarios where conflict is not only more likely in general but also more likely to impact civilian populations who will see the technology that they have come to rely on turned against them.

Richard Clarke again provides not only an example of the translation of academic framing of cyber war as existential risk into public and policy debate but a vector. Clarke's appointments in the US government span three presidents: Reagan, Clinton and Bush. Under Clinton he was appointed as chair of the Counter-terrorism Security Group and given a position on the United States National Security Council. During G W Bush's presidency he was made Special Advisor to the President on cybersecurity. It is unsurprising then that the threat picture that he created in his book with Robert Knake was readily adopted by others within government at the time with this position on cybersecurity then becoming quite firmly entrenched within US defence policy and discourse. References to the potential for a cyber pearl harbour came to be synonymous with US military discussions as to the risk posed to critical infrastructure by cyber attacks (Panetta in Ryan, 2011) and has endured from its most notable utterance by Leon Panetta, then US Defence Secretary, in 2012 and been further reinvigorated in far more contextual events in news media sources regarding the WannaCry ransomware attack (Stavridis, 2017).

While all of the examples above can be framed as contributing to the framing and understanding of what cyber-war is by states each and every one of them approaches the issues from what I argue is the wrong direction. The authors and proponents of the arguments examined above start with a concept of what cyber war is and then seek to prove or disprove the existence of their presupposed formation. Not only has this led to the entrenchment of a discourse – in academia, policy and news media – that has leant towards extreme scenarios, but it has also meant that minimal attention has been directed towards a tangential question. How are concepts and norms of cyber war constructed?

The polarised extremes of academic literature regarding cyber war have begun to be drawn closer together. More nuanced analysis has started to fill in the middle ground which had previously been absent moderated examination. The work of Myriam Dunn Cavelty, Andrew Futter and Brandon Valeriano has specifically engaged with the problematic framing of cyber war as well as the contested nature of its lexicon. Brandon Valeriano and Ryan Maness point out the risk of extreme constructions of cyber risk before offering a quantitative means of examining the realities of inter-state cyber conflict:

> The cyber hype perspective would suggest that we are seeing a revolution in military affairs with the advent of new military technologies. The moderate perspective is guided by careful consideration of what the real dangers are, as well as the cost of the overreaction […] Our concern is that fear dominates the international system.
>
> (Valeriano and Maness, 2015, p1)

While these two argue that the hype generated by previous literature in suggesting the likelihood of cyber hiroshimas and pearl harbours are the result of a "process of fear construction [which] continues to shape dialogues in international relations as cyberspace becomes a new are of contestation in international relations" (Valeriano and Maness, 2015, p1) Futter is arguing that the level of obfuscation surrounding the term cyber itself is such that it should be discarded. He states that our "inability to be clear what the concept means, involves and affects has left the word dangerously devoid of meaning, and has obfuscated and complicated the ability to shape suitable responses and policies" (Futter, 2018, p202).

Further filling out the moderate centre ground of cyber war literature are the conclusions of Myriam Dunn Cavelty. Her work specifically focusses on the framing of notably loaded terms such as cyber weapons and the way in which particular attacks have been used to further inflate a perception of cyber risk which lies far above the reality. Dunn Cavlety (2013) argues that "the link between cyberspace and national security is often presented as an unquestionable and uncontested "truth." However, there is nothing natural about this link: It had to be forged, argued and accepted" (p1). With this she not only points to the significant divide between reality and over-hyped perception, she suggests a critical theoretical basis for the reason this discrepancy goes unchallenged.

These three examples begin to dispel the problematic mythos that has been constructed in the academic literature of cyber war and then spread into both policy and media discourse. Valeriano and Maness' efforts to bring quantitative analysis to the examination of inter-state cyber conflict alongside specific framings of what constitutes an attack are an effective

methodological means to counter the factually unsupportable predictions of a coming cyber apocalypse. Simultaneously Futter's declamation of the problematically contested usage of cyber as a concept within security literature and policy sets a precedent regarding the need for clarity and technical literacy in this intersection of technology and security. These lessons and developments in literature all begin to bring clarity through approach, methodology or critical analysis to the examination of cyber war and security in general. In this thesis I will continue this trend and seek to further expand our ability to offer moderation of sensationalised framing as well as offering a greater understanding of the manner and motivations by which key actors seek to influence this same constructive process.

Cyber Terrorism

Cyber terrorism, much like cyber war contains a body of literature which has undergone a significant sensationalising process with more moderate analysis now beginning to bring this in check. The similarity between the two is effectively stated by Dunn Cavelty in the following statement:

> While governments and the media repeatedly distribute information about cyber-threats, real cyber-attacks resulting in deaths and injuries remain largely the stuff of Hollywood movies or conspiracy theory. In fact, menacing scenarios of major disruptive occurrences in the cyber-domain, triggered by malicious actors, have remained just that – scenarios.
>
> (Dunn Cavelty, 2008, p20)

In contrast to the literature on cyber war academic examination of cyber-terrorism has, to a far greater extent, been more moderate and critical of the drift to sensationalism. Despite this the policy and legislative literature as well as the public discourse as shaped through news media has still adopted the framing of cyber-terrorism as an extreme and pressing risk in a manner which all but mirrors the treatment given to cyber-war.

Previous observations by Dunn Cavelty that the academic literature concerning cyber-terrorism has been heavily policy-oriented and has often "uncritically adopted arguments on the nature and scale of cyber-terrorism from official statements or pieces of media coverage" (Dunn Cavelty, 2008, p20) I would argue that the second of these criticisms at least is not longer the predominant feature that it once was. Cyber-terrorism literature is still a heavily policy-focussed body of work. However, this is likely itself a symptom of the easy adoption of that sensationalised framing by policymakers and media and the rapidity in which policy in particular has sought to engage with this perceived risk. The motivation for the increase of

critical analysis of these preconceptions within academic literature similarly is spurred by the temporal. While states were speedily updating anti-terrorism legislative and strategies and media outlets fed this into wider public discourse a notable disconnect between the haste behind these actions and the increasing span of time in which no acts of cyber-terrorism in fact took place.

This fact brought into stark contrast the problematic framing of cyber-terrorism within a significant proportion of academic literature. The contributors to the sensationalised and hyped segment of the literature continue to insist upon the imminence of an attack which will fit definitively within their framing of cyber-terrorism (Arquilla et al., 1999; Schwartau, 2000). At the same time those seeking to moderate this analysis are critically engaging with the components of this suggested imminence and finding them wanting (Lewis, 2002; Barak, 2004; Wilson, 2003).

These moderate voices have, for the most part, maintained a strict and often issue specific focus upon the critique of the concept of cyber terrorism when it is measured against the practical limitations and its lack of empirical manifestation. The literature that this group seek to critically analyse however often employs broad understandings of which issues can be construed as a part of cyber terrorism. One such case is ably demonstrated by Schwartau who, in seeking to fit cyber-terrorism within the concept of Asymmetric warfare makes direct reference to the conundrum of there being no instances of cyber-terrorism to lend credibility to the risk that this phenomenon apparently poses.

> Another skeptic is Martin Libicki, a senior RAND analyst. “If this threat is so dire,” he asks, “why haven’t we seen anything really, really large take place?” But according to that reasoning, we should only worry about disasters after they occur. Such a complacent approach scarcely prevailed during the Cold War, when the dangers of nuclear war were keenly anticipated in advance of some “really, really large” event.
>
> (Schwartau, 2000, p201)

This framing of cyber-terrorism as running parallel to, if not akin to, asymmetric warfare allows Schwartau to make broad declarations regarding the inevitability of acts of cyber-terrorism while drawing in the potential of inter-state conflict within the same analysis. Schwartau does this to the extent of drawing comparisons between the risk of cyber-terrorism in the near future and the risk of nuclear war during the height of the Cold War. Such a connection is based not upon empirical evidence but upon presupposition of what terrorists would like to do without a counter-balancing consideration of whether these desires tally with capabilities and

indeed whether they are ever likely to do so (Kramer, 2003). The pairing of asymmetric warfare and cyber terrorism signifies another literature trend that derives from contested and problematic definitions.

Weimann (2004) suggests that a significant cause for the confused and contested status of cyber terrorism literature is as a result of the relative age of the field of cyber security itself and that the related lexicon is still continually and rapidly evolving. This results in exercises seeking to frame the risk and nature of cyber terrorism which approach the same topic with vastly differing understandings of what this phenomenon is. These attempts then seek to ascribe a level of risk, be these on an apocalyptic level or anywhere below, based upon differing and often contradictory conceptualisation of what cyber terrorism actually is.

This approach, which constitutes a large portion of earlier literature, through this broad approach has resulted attempts to comparatively examine cyber terrorism on similar terms to forms of terrorism that have previously undergone similar sensationalised framing within academic literature and media discourses. Examples of this include comparisons with nuclear terrorism and bio terrorism. Furthermore, the consideration of how terrorists might employ the internet or cyber capability has led to further literature examining these connected implications. High amongst these being the potential for terrorists to use the internet to recruit or radicalise individuals.

This facet of cyber terrorism analysis enjoys a distinct absence of over sensationalism or predictive framing based upon inference or comparison to other forms of terrorism. Notably, the study of how terrorists are using the internet and social media in more firmly grounded in the analytical and critical work which predates the inclusion of cyber within the security lexicon. This literature effectively challenges the revolutionary credentials of the internet regarding the existence of cyber terrorism as the concept has become popularly understood. While recognising that there are implications regarding terrorist groups use of networked technologies – particularly with regards to recruitment, communications and training – the existence of cyber terrorism as a distinct and violent form of terrorism in its own right is critically dismissed.

Maura Conway, in a 2011 article which is notably titled ‘Against Cyberterrorism’, sets forwards three reasons for why she categorises herself as belonging in the De-Hyper group as laid out by Dunn Cavelty (2007). She argues that the level of complexity required to carry out a violent online attack is too high a threshold for violent jihadis to meet, that the kind of destruction cyber-attacks might deliver cannot achieve a significant enough spectacle to be appealing to

terrorist actors, and that if these destructive attacks were carried out they could too easily be dismissed as accidental and thus fail to deliver the communicative function that acts of terrorism are intended to provide (Conway, 2011, p28).

Cyber terrorism then appears to be a misnomer, one that has risen to prominence as a result of a rapidly developing popular, technical and academic lexicon of definitions that has led to a polarisation of literature concerning the subject. On the one side are those who suggest that an act of cyber terrorism is not only capable of causing significant damage comparable with previous incidents and that such an attack is imminent. These arguments are supported through a combination of assessments upon the inherent weaknesses of technology coupled with the interconnected and technologically dependent nature of society. The opposing position, Dunn Cavelty's De-Hypers, argue that cyber terrorism is not only an unattractive tool to terrorist actors, but it is also one which comes with a greater cost than is attributed by those from the opposite camp.

The primary and definitive split within this literature, as in that of cyber war, has to do with contradictory framings of what cyber terrorism actually is. Within the cyber terrorism literature as within that of cyber war there are in effect two competing literatures whose main contention lies over the disagreement as to whether the issue in question represents a new and significant threat or not. The definitional quagmire surrounding both cyber terrorism and war present a research question all of their however, one which considers both the means and the motivations for manner in which the hyper sensational framing of both of these concepts in academic literature is adopted and then constructed by policymakers and states.

Again, Dunn Cavelty makes inroads with this approach. She seeks to examine the manner in which the political manifestations of academic efforts to frame cyber terrorism, threat perceptions, are constructed through the application of discourse analysis and a broadened form of securitisation theory. This approach not only ties the examination of cyber security holistically together, across the categorisations that they have thus far been split in to, but it offers insight into the connection between the purposeful construction of extreme representations of threat by policymakers and the specific policies which these representations seek to justify (Dunn Cavelty, 2013, p106).

Cyber Surveillance

Cyber surveillance has avoided the sensational framing of its fellows. In the aftermath of the Snowden revelations regarding state led cyber surveillance there has been significant examination of the topic from a legal and ethical perspective. Alongside this and in concert

with it a growing body of literature seeks to engage with the implications of how the technologies that we use on a daily basis are increasingly being gathered for the purposes of providing security. Conflict arises between the security-driven policy desire to decrease perceived insecurity at any cost and an increasing awareness in the public and institutional space of the ways that this could significantly infringe on human security issues – such as privacy.

Much as Dunn Cavelty argued that the study of cyber terrorism has been largely engaged upon in a granular and policy-centric manner the literature regarding surveillance suffers from a similar trend. With the framing from policy makers, especially in the aftermath of Snowden's revelations, seeking to justify cyber surveillance capability as necessary as a result of terrorist usage of the internet the preponderance of academic study being directed at the potential efficacy of such capability is somewhat understandable. Analysis of this kind often either fully discounts the operability and utility of the mass collection regimes exposed by Snowden or suggests that these could be rendered more effective should they be supplemented with counter-communication efforts (Palasinski and Bowman-Grieve, 2017).

The framing of cyber surveillance within academic literature is considered with regards to the impacts of surveillance policies upon both state security and issues of civil liberties. There is undeniably a pressing need for such scholarship and the fact that arguments made within this body of work have been taken up by lobbying groups, NGOs and media outlets is encouraging. Legal scholarship has examined the intersection of the adoption of digital surveillance with existing legal standards as well as those which have been specifically developed in order to create a legal framework upon which digital surveillance can be carried out (Lipton, 2010). Most strikingly there are legal examinations of rulings which later removed or curtailed these powers in light of the Snowden's releases (Fabbrini, 2019). All of these studies however focus their examination upon policy and are, for the most part reactive to narrow instances or examples of the specific successes or failures of digital surveillance methods with regards to their provision of security or damage to civil liberties.

A significant body of scholarship exists which examines the evolving nature of what privacy means within a changing landscape of how we create and use data. Nissenbaum's arguments concerning what she terms contextual integrity, the manner in which personal data and the norms which govern its use and ownership are linked to certain social contexts which determine the nature and level of privacy expected (Nissenbaum, 2004). Efforts to consider how privacy and our use of digital technologies and the production of mass data have led to the suggests risk to individual privacy through the structurally inevitable production of a

"surveillance-industrial complex" (Ball and Snider, 2013) where business and government interests overlap.

With the basis for much of this research being the dramatic unveiling of the realities of cyber surveillance regimes as operated by the US and the UK the analysis of surveillance and its framing has been significantly shaped by media narratives as opposed to academic. In effect the sensational nature of Edward Snowden's release of classified material and the amplifying of this due to the means and manner of its release through media outlets has meant that academic and policy debates have been forced to confront the issues raised by Snowden specifically or risk being regarded as out of touch. What is required to fully understand these implications is a broader examination of the means and methods by which the concept of cyber surveillance, as an acceptable and necessary means of providing security to the state, was constructed and so firmly situated.

Critical and comparative examinations of the impact of Snowden's intelligence leak have been undertaken but much of this work examines the impacts of this updated information on public perceptions within various domestic settings. This work has extended beyond the US and UK centric boundaries of where the majority of Snowden's material was situated (Zavrsnik and Levicnik, 2015), and as such presents an effective body of work upon which a comparative analysis of public perceptions regarding surveillance across regions and states may be conducted. However, once again there is limited efforts within these studies to examine the means by which cyber surveillance is framed as a necessity, or how these acts of construction interconnect with wider theoretical concerns. It is my intention, in part, to go beyond the critique of hyper sensationalising framing of cyber surveillance as a critical requirement for security seeking states and to examine the means by which this concept is constructed. Beyond that I further intend to explore how these methods are themselves acts of norm construction which provide further evidence of an interconnected process of security framing that is not unique to cyber surveillance or cyber security.

Conclusions and Contributions

Across the three bodies of literature discussed above there are distinct similarities which have themselves arisen out of the manner in which all three of these issues have been thrust into the spotlight, both in academic and public consideration. The rapidity of cyber's emplacement within the critical topics of policymakers and security focussed academics has resulted in a tendency towards polarisation and confusion. The former evidenced by the continuing arguments concerning the risks posed by cyber war, terrorism and surveillance – in terms of

immediacy and relative harm – and the latter by the care required in defining highly contested and central terms in any work that seeks to engage with this debate.

Both of these issues have undergone redress, with the doomsday scenarios generated through the automatic adoption and limited critique of various framings of the risks posed by cyber terrorism, war and surveillance now being challenged with moderating literature that engages with the lack of empirical evidence and problematic transposition of concepts from dubiously connected fields.

This thesis however intends to advance this approach further. Already the growing body of work which supports a moderation of sensational over exaggerations of cyber-security issues is drawing attention to the fact that the concepts of cyber-war, terrorism or surveillance upon which these problematic and predictive analyses are based do not accurately reflect reality. They are not conclusions based upon deductions made from empirical observation. From this position I believe there is a further question, or questions, that must be asked. Firstly, how is it that these various forms of cyber-security risk have been sensationalised to such a level within academic, policy and public discourse? Secondly, if – as I believe to be the case – that these framings of risk are purposefully constructed, what are the implications of this for our understanding of how the process of norm construction operates with regards to security centric issues.

Myriam Dunn Cavelty provides the beginnings of this approach with her critical theoretical approach and the application of securitisation theory to the very question that I have posed above. When laying out the approach that she intends to take she notes significant issues with the classical conceptualisation of securitisation as proposed by Buzan et al (1998). Arguing that its focus upon elite actors and speech acts delivered by this typological group is overly simplistic as a model and fails to effectively model the reality of how issues are in fact constructed within security discourse through the efforts of actors that do not all fit within this category (Dunn Cavelty, 2013, p106).

While my approach again intends to employ securitisation as one theoretical component, I also find it self-limiting in the way it conceptualises both actors and securitising acts. Much as Dunn Cavelty argues that limiting the search for securitising discursive speech acts to elite actors is a restrictive and unrealistic facet of traditional securitisation theory I suggest that the focus upon discursive acts is itself unreflective of how the basis for domestic and international security policy is constructed by all actors involved. Action has as much a role in the securitising of a concept and thus policy relating to it as the discursive element, if not more so.

Thus I argue the various categories of cyber security addressed above and in the following chapters of this thesis can be best understood through a form of securitisation theory that seeks to examine the relationship of active and discursive means of construction across a range of actor typologies.

My intention is to address what I consider to be a significant gap in the literature, one which if properly addressed can provide not only useful insight regarding cyber security issues specifically, but also have wider implications for the any other issue wherein policy decisions and security overlap. Quite simply I view the argument that a hyper sensational threat representation of issues such as cyber war and terrorism, which in turn justifies cyber surveillance, that is based upon the suggestion that if state actors are themselves framing these issues as significant risks there must in fact be such a risk. This approach fails to consider the possibility that the risk framing is itself a means and not an end, the fact that states are not the only actors with a hand in influencing risk perception, or finally, that actions are just as capable of forming the basis of a perceived threat as discursive statements.

In the following chapter I will outline in greater detail the theoretical framework that I propose to make the basis of this thesis. As suggested above I will continue upon the course laid out by Dunn Cavelty with regards to the adaption and expansion of securitisation as proposed by the Copenhagen School. Further to this I will combine this expanded formulation of securitisation theory to combine elements of normative theory, in particular norm emergence theory. The critical analysis conducted so far within cyber security literature has suggested that all the component categories contained within which pertain to policy creation are subject to a sensationalised framing which various state actors have sought to either adopt of further emphasise. Cyber war and terrorism are, in terms of their perceptions at the public and to some extent international institutional levels, what states want them to be. The aim of this thesis and the theoretical framework that I will set out in the next chapter is to offer an explanation as to how states have achieved such successful acts of securitisation.

Chapter 3 – Theoretical Framework

The Foundations

Cyber security is a field which has so far suffered in critical academic terms thanks to the speed of its arrival and rapid rise to prominence within academic and political debates. The contested framing of the various categories of cyber security issue, of which there appear to be more of on a near daily basis, has arrested much needed critical analysis of the field. My intention with this thesis is to begin to engage with this critical analysis by examining the how these issues have been framed by state actors for the purposes of either gaining strategic advantage at the international level or to gain support for the extension of power at the domestic.

In order to engage with how actors have framed issues of cyber security and related capability and not get further drawn in to the debate surrounding the accuracy of these, often contradictory, positions I seek to take a theoretical approach. My proposal, which is a combination of two existent theoretical frameworks, takes securitisation theory and combines it with norm emergence theory. It is my belief that, through expanding the concepts of both of these beyond their traditional framing, I can cement components of both these two frameworks which already enjoy significant overlaps and so create a single set of theoretical principles with significant utility in answering both my specific, cyber oriented questions and others with similar components.

This theoretical framework will begin by outlining these two theories – norm construction and securitisation – in isolation and demonstrating their relevancy to the cyber capability and framing that is the main basis of this thesis. I will then discuss the overlaps that these two theories have with each other within this context which suggests their potential for connection into a single, unified framework that can be used to examine the means by which states shape and employ particular framings of cyber security issues.

Finally, I will lay out the key concepts within the new theoretical principles that this thesis seeks to demonstrate: *Norm Securitisation* and *Operationalised Norm Construction*. Once these two have been explored and defined I will show how they interrelate in a manner which explains the process by which states construct normative positions and framings of cyber-security issues that provide for strategic advantage and legitimacy for domestic security policy.

<u>Norm Construction</u>

Norms are, as explained by Finnemore and Sikkink (1998), understood to be a “standard of appropriate behaviour for actors with a given identity” (p.891). To go against internalised norms is to break with expected standards which often the attract stigma or even punitive

responses whereas to conform to these expected standards promotes at the least an apathetic response, but at the best active praise as a result of conformity of action. Norms have in effect a prescriptive power in that they encapsulate what is currently perceived, within the applicable group of actors, what is believed to be right way of operating. This is not state that the nature of any internalised norm, which enjoys acceptance by the majority of actors, is by this nature unequivocally good. Norms are, in this sense prescriptive in that they are responsible for defining the current accepted concept of good with regards to certain actions or sets of actions by a set group of actors. At a point in history norms suggested that slavery was good in exactly the same manner in which norms today categorically refute this statement. It is this prescriptive nature which suggests that a norm based analysis of how state and institutional actors have framed concepts of capability within cyberspace at the domestic and inter-state level could be effective. If actors are constructing specific framings of cyber-capability development or deployment as good, necessary or acceptable then they are seeking to contribute to prescriptive norms.

In attempting to shape the norm these states or institutions are acting as norm entrepreneurs. In explaining the interconnection between domestic and international norms Finnemore and Sikkink once more offer an effective explanation of this term. Norms being non-dichotomous – varying in strength and levels of acceptance – between one setting and the next the theory suggests that it is common for norms initially arising in a domestic setting to then be exported to an international one. Finnemore and Sikkink use the example of Women's suffrage as a case study to present the connections between domestic and international norms as this normative process "began as a demand for domestic change within a handful of countries and eventually became an international norm" (Finnemore and Sikkink, 1998, p.893). Such an example effectively demonstrates the non-dichotomous nature of international norms that begin at the domestic level: women's suffrage while enjoying wide acceptance and internalisation at the international level is still not accepted by all state actors equally. Even within those states that do ascribe to this normative position the manner in which they domestically translate this norm into policy and action is influenced by the domestic setting of that same state. Norm entrepreneurs then are best understood as actors who wish to transplant an existing normative position with their own, or to create a new norm with regards to an issue which currently has none. They themselves are likely to be members of the group identity to which this normative position applies or, at the least, they will represent a group with influence or shared positionality with relation to the norm in question. In this respect norm entrepreneurs

in a domestic setting could be a political party, a charity group, a business, a religious group, or in some cases an individual citizen.

At the international stage we tend to think of norm entrepreneurs as states within which the domestic version of this norm has arisen and become the accepted, dominant normative position and which is now in the process of being in a way, exported on to the international arena. However, in recognition of the more nuance means by which prescriptive values are shaped in international affairs it is suggested that international forms of the domestic array of norm entrepreneurs are just as valid members of this theoretical grouping; international NGOs, faith groups, alliance organisations and others are just as likely to take on the role of norm entrepreneurs over issues which connect with their areas of interests.

"We can only have indirect evidence of norms just as we can only have indirect evidence of most other motivations for political action" (Finnemore and Sikkink, 1998, p.892). Norms, when they are fully established present little sign of their existence as a result of the apathy commonly generated by the adherence to them by those who have accepted their legitimacy. The evidence of the means of norm construction or attempts to contest existent norms however is, according to these same authors, generated in significant quantity by dint of the necessity for justification of actor's diversion from agreed standards. In order to supplant an existent norm with one which prescribes a new concept of what is right norm entrepreneurs must justify this shift. They do so through discursive acts whereupon they seek to convince others who adhere to the previously preferred normative position that the new version that they represent is better and that they too should accept its prescriptions as to what is right. Norm construction then, through the necessity of explicit contestation with existing standards amongst norm entrepreneurs is an open and discursive process which creates significant evidence of its occurrence in political statements.

The aim of the norm entrepreneur is to successfully convince enough of those that fit within the same actors within its relative group to accept and thereby internalise the new norm that they propose. Through discursive acts which seek to justify the actions contained within the new standard that they propose these norm entrepreneurs leave behind the evidence of the constructive process in their attempts to export their position on to their peers. Various factors can influence the success of this normative bargaining process. The nature and legitimacy of the norm entrepreneur might either provided added force to their attempts or, in some cases the norm entrepreneurs might suffer from perceived illegitimacy with regards to the norm which they are attempting to promulgate and thus find achieving a wider uptake more difficult. A state with a poor human rights record, for example, seeking to disseminate a

new norm regarding the international response to human rights abuses would find it harder to justify and thus spread the acceptance of this normative position as a result of its own prior record. Finnemore and Sikkink suggest that, in this process of norm emergence, those norms which successfully gain wide acceptance and internalisation are those whose norm entrepreneurs can garner enough support to reach a state of what they describe as "norm cascade".

Norm cascade is, in effect, the point whereupon the number of actors who have been convinced to accept and themselves become norm entrepreneurs for the newly proposed prescriptive form reaches a tipping point. Where the momentum gathered by the effective justifications for this new concept of what constitutes right has reached the point where opposition cannot counter it and is eventually overcome to the point that the incoming norm is now the dominant version (Finnemore and Sikkink, 1998, p.895). This would see those actors that still refuse to accept the justifications for the shift now being considered as those worthy of stigma or even punitive action as a result of not aligning with the new norm.

Norm cascade, along with norm emergence and internalisation together form what Finnermore and Sikkink term the Norm Life Cycle (Finnemore and Sikkink, 1998, p.895). The theoretical framework that this chapter seeks to outline and which this thesis hopes to demonstrate with regards to the norm life cycle of cyber-capability is built upon the foundations of this framework, as outlined by Sikkink and Finnemore and explained above. Upon this foundation I will suggest further conceptual additions which draw upon the Copenhagen School's securitisation theory. My intent being to demonstrate the manner by which some norms can be constructed through a securitising lens and how the successful drive to norm cascade and eventual internalisation by securitising norm entrepreneurs can be influenced through an active, operationalised process of norm construction as opposed to a purely discourse driven one.

Securitisation

Securitisation is the process by which an issue is framed as an existential threat and therefore requiring specific and, often by existent standards, extreme response in terms of resourcing of policy expansion to counter the threat posed. Like the stages of the norm life cycle explained above this process is often described as performative (Dunn Cavelty, 2013, p.106). The attempts to justify this shift of politics from the normal to the exceptional (Buzan et al., 1998) are embarked upon by political actors by means of "politically salient speech acts" which attempt to convince the audience, most commonly interpreted as the general public, to accept this shift (Husymans, 2011, p.371).

To successfully securitise an issue is to reach a point where the audience in question, commonly the general public as first-generational securitisation theory is largely domestic focussed, that the issue at hand poses an existential threat. If the audience is convinced, then political acts that relate to this issue suffer less restraint with regards to balancing concerns over connected issues such as civil or human rights. Within this thesis a successful example securitisation can be found in the chapter four with the empowerment of the British government to create policy and legal frameworks regarding the digital surveillance of the population. In this instance successive British governments managed to maintain public acceptance of the securitisation of digital surveillance with the infringement of individual privacy balanced out by the desire to be safe from harm. This is an example of a successful shift from normal politics to securitised politics by a securitising agent.

In first-generation securitisation theory securitising agents are those with the positionality, by dint of their role within politics, to have the necessary reach to directly shape the public perceptions of an issue and convince this same public of the existential nature of the threat it poses. Thus, first-generational securitisation theory is a largely elite-centric concept through the belief that in order to have this form of reach and power an individual must either by the head of state or someone of significant seniority within the political structure at hand. Alongside the head of states securitising agents with sufficient performative power to successfully persuade the public of a threat against them might be “senior civil servants, high ranked military, [or] heads of international institutions” (Hansen, 2006, p.64). Elite actors such as these do not hold a monopoly on shaping public perception, nor do they operate within a vacuum in which there are no preparatory or amplificatory efforts made regarding attempts to securitise an issue by other non-elite actors (Huysymans, 2006, p.72). As such the foundation of securitisation, as laid down by Buzan and others of the Copenhagen school has been expanded and specifically used as a critical tool with regards to the examination of framing with cyber-capability issues (Dunn Cavelty, 2008, 2013; Bendrath 2001, 2003; Eriksson, 2001; Nissenbaum, 2009). While this thesis predominantly examines securitising acts carried out by elite actors which best conform with first-generation securitisation theory it is my belief that further research would certainly conform with the expanded range of potential securitising agents.

As a performative role securitising agents seek convince their respective publics to accept and internalise the reality of the threat posed to them by means of speech acts. These politicised utterances can take the shape of vocalised narratives or written ones and can be presented to the audience either directly or through indirect means such as news broadcast or another

media source. The speech act is therefore the central focus of securitisation as it is upon the effectiveness of this statement that securitisation is either a success of a failure. While the nature of the individual agent that is the source of the speech act may further influence the likelihood of a successful or unsuccessful act of securitisation it is the speech act itself which is the lynch pin of the process. A carefully framed speech act that effectively draws upon existent fears within a given target audience with regards to referent objects such as children might succeed in convincing that specific audience. However, the same components that led to success with that audience may, with regards to an audience with different political or ideological predilections, lead to failure – a fact which the Copenhagen School fails to account for.

A more granular analysis of what makes an effective speech act is offered by Balzacq who injects a number of contextual components. In critiquing the Copenhagen School's original concept as being simplistic in the manner which it imagines successful securitisation to be based solely upon the conjoined factors of a securitising agent's "linguistic competence" and holding of a position supportive of the act being made (Balzacq, 2005, p.172)**.** This approach however, according to Balzacq is as limiting as the manner in which it reduces those capable of carrying out securitising acts to elite actors. Balzacq argues that this universal pragmatic approach fails to properly take into account the necessity for contextualisation of the linguistic action made by the securitising agent with regards to the audience to which it is targeted. He argues that the language used as part of a speech act "has an intrinsic force that rests with the audience's scrutiny of truth claims, with regards to a threat, being made by the speaker" (Balzacq, 2005, p.173). Meaning that certain uses of language, certain securitising agents, and indeed certain combinations of these two are going to undergo greater or lesser scrutiny by certain audiences with this in turn resulting in the necessity of contextualisation when formulating securitising speech acts and selecting the agents to carry them out.

The final component of securitisation that requires attention is itself a component of an effective speech act. Referent objects, as proposed by the initial proponents of securitisation theory, the Copenhagen School, are the things which speech acts seek to frame as under threat. These things can have significant impact upon the potentially efficacy of a speech act, both under the universal pragmatic approach of the Copenhagen school and the contextually literate formulation suggested by Balzacq. A referent object to which an audience has limited attachment is going to have similarly limited persuasive force when it comes to convincing that audience of the necessity of a securitised shift beyond the realm of normal politics. A referent object which is carefully chosen as possessing a particularly powerful emotive or structural

connection to the audience being targeted by the securitising agent however may significantly increase the potential for a successful act of securitisation. Finally, the injection of a greater level of contextualised analysis with regards to both referent objects and the recognition of a wider pool of actions which can influence these constructive acts allows this next-generational mode of securitisation theory to incorporate and answer the realities of domestic variation that have previously been easy avenues of critique.

Examining the Overlaps

The key principles of norm emergence theory and securitisation theory as described above posses a significant number of overlaps. It is these overlaps that contributed to convincing me that a theoretical framework which combined these two into a single entity would not only be possible but potentially offer significant utility when it comes to understanding the processes undergoing within the framing of cyber-security issues as well as the policy positions that generate from these constructed entities.

The first of instance of compatibility between securitisation and norm emergence is perhaps the most telling. When a norm entrepreneur successfully supplants an existent norm with a new form which matches their own preferences, convincing their peers of the legitimacy of this new version to the point of a dominant level of acceptance and internalisation this is akin to a successful act of securitisation. Within the framework of normative theory, the audience simply happens to be actors who are the peers of the norm entrepreneur as opposed to the accepted nature of securitisation wherein the audience is commonly understood to be the general public. This suggests that a conjoined framework of securitisation and normative theory would state that while not all acts of norm construction are securitised that all acts of securitisation are acts of norm construction.

From this point it is equally possible to conceptualise that norm entrepreneurs and securitising agents are terms which can be applied in this region of overlap. When an emerging norm is being constructed through a securitised lens then the norm entrepreneur/s responsible for its emergence and its trajectory through the norm life cycle to cascade and eventual internalisation are akin to securitising agents. Likewise, the point at the end of the norm life cycle, acceptance or internalisation is all but indecipherable from that of a successful act of securitisation where the target audience has accepted the securitised framing of a referent object. In this status actions or policies that enact this new normative position, one which has traversed the full spectrum of the suggested cycle and been accepted in its legitimacy, will not result in a negative reaction or the attachment of stigma from the audience that has accepted

this act of securitisation. Therefore, not every act of successful norm construction is a successful act of securitisation, but every successful instance of securitisation comes as a result of the successful transit of the norm life cycle via a securitised framing.

Finally, the means by which successful acts of securitisation are achieved and norms are progressed from emergence through cascade and to eventual internalisation share distinct similarities which further support the combination of the two conceptual frameworks. In the same manner that Finnemore and Sikkink argue that the evidence for the process of norm construction is everywhere, contained within the attempted justifications of action and political speeches of politicians, military agents and representatives of institutions so too is the evidence of the attempts to securitise. The speech acts enacted by securitising agents are indistinguishable from the justifications of those attempts to bolster the support for a norm by norm entrepreneurs aside from their security-centric framing. Both securitisation and norm construction is achieved through a purposeful series of discursive acts by determined actors with vested interest. Both theories of norm construction and securitisation can be understood to have, in their first-generational and uncontested forms, a reliance upon elite led discursive action. This limitation having been covered earlier in this examination of the theoretical basis for this thesis. As much as it was found to be unrealistic and self-limiting with regards to an understanding of securitisation I would suggest that it is similarly unnecessary and unjustifiable to consider that norm construction is an act only embarked upon and contributed to by elite actors. What this leads me to conclude is that both norm construction and securitisation are seemingly reliant upon discursive acts of construction. Irrespective of whether an emergent norm is to undergo a securitised progression through its life cycle or not the consensus that appears to be arrived at through the conjoining of theories of norm construction and securitisation is that the means of its progression will be discursive in nature. In my proposed combined concept of norm securitisation I further suggest that this shared reliance upon discursive acts of construction is insufficient. To counter this and to further strengthen the theory that I propose I argue that both acts of norm construction and securitisation rest heavily upon active means as much as discursive. To this ends this thesis will put forward not only a theory of norm securitisation but the establishment of the role of operationalised, or active norm construction.

Norm Securitisation and Operationalised Norm Construction

This thesis seeks to propose a complimentary set of theoretical frameworks which it will use to examine the means by which norms regarding cyber-capability are constructed in international and domestic politics. The first of these is based upon the combination of the two overlapping

concepts described above; norm construction and securitisation. Taking versions of these two that have both been expanded beyond their initial representations to be more contextual and reflective of both actor input and audience variation. Secondly, I will forward an alternative mode of norm construction which I argue corrects a failing present in both securitisation theory and norm construction as it is currently understood. I will argue that while significant attention and impetus is attached to discourse with regards to its role in both the construction of norms and of successful acts of securitisation that insufficient consideration is given to the manner in which norm entrepreneurs or securitising agents can employ a more active approach to norm construction. I will therefore propose not only the concept of norm securitisation, but that within this process norm entrepreneurs that embark upon a securitised route of norm construction can imbue their preferred norm with a greater chance of success and resilience to contestation through an operationalised means of norm construction.

As discussed in the section above when examining overlaps and parallels between norm construction theory and securitisation the concept of norm securitisation exists at the nexus point between these two frameworks. Norm securitisation concerns a process of construction in the same manner as norm construction does, however it is concerned with norms wherein the norm entrepreneurs involved in driving that process are seeking to do so through the use of referent objects and acts of securitisation. An act of norm construction can be described as attempting to interpose a new prescriptive shape of accepted behaviour upon a group of actors with a given identity norm: a concept of what is right or good. Norm securitisation however infer upon its audience a prescription of what is necessary. This necessity both suggests the nature of the behaviours that arise from the norm at hand and infer a greater level of urgency and a greater ordinal value than one which doesn't possess securitised features.

The success of norm securitisation once again rests upon whether the prescribed necessity, as justified by the securitising norm entrepreneurs, is accepted by the intended audience. This is true both with norms which are being constructed at the domestic or the international level. Any norm can potentially undergo a process of securitisation, as long as the norm entrepreneurs driving this process can successfully employ referent objects, language and action to justify this shift. Securitised norm emergence may then represent an entirely new set of norms which is being constructed to designate its necessity through the securitising lens. It may also represent an attempt by a norm entrepreneur or entrepreneurs, to redefine an existing norm in a new, securitised manner. The basis of this thesis, the examination of cyber-capability, primarily concerns the former of these two. However, in reference to the

evolutionary implications of concepts of cyber-war and cyber-terrorism there are instances of the pre-existent norms undergoing a new round of the norm life cycle, this time with a securitised framing.

Securitised norm emergence can be understood therefore as the alternative first stage of the norm life cycle where the norm being constructed is intended to result in a securitised state. The norm entrepreneur in this instance may sincerely believe in the necessity that the intended securitised state of this norm prescribes or they may be selecting a securitising approach in recognition that a securitised means of norm construction that seeks to progress an emerging norm on to cascade and finally internalisation has a greater inherent power and thus chance of success than a constructive process which lacks this securitising element.

Operationalised norm construction is a concept which I use to describe an active contribution to any attempted norm construction, securitised or otherwise. This means of construction is achieved through the norm entrepreneur/s carrying out activities which are within the prescribed bounds of acceptable behaviour of the norm which they are seeking to see adopted. A state seeking to legitimise and spread a norm that suggests for the removal of landmines for example might actively engage in the physical removal of these weapons as opposed to engage in a discourse driven method of construction. Operationalised norm construction is a method of framing which does not necessarily supplant or replace a discourse driven approach. The use of operationalised norm construction might be employed alongside discursive action, with the discourse component further amplifying the impact of the physicalised component. To draw on the landmine example again a state might either simply remove landmines without making a discursive statement, it might also only engage in discursive statements aimed at supporting its preferred normative position. However, that state might also embark on a policy of landmine removal, employing this operationalised context created by this active engagement with the normative position, to further reinforce the efficacy of discursive acts of norm construction.

It is one of the aims of this thesis to argue, through the example of cyber-capability, that this behaviour-based means of norm construction is the basis of the majority of effective securitised norm construction. I will further argue that norms constructed through a combination of operationalised, behaviour driven means of construction and the amplification of these actions through discursive means of construction accelerates an emergent securitised norm through to cascade and acceptance, increases the likelihood of eventual acceptance by the target audience, and grants a significant level of resilience to the securitised norm created with regards to attempts of contestation.

Both operationalised norm construction and the discursive norm construction associated with it do not have to be conducted by the same norm entrepreneur. A behaviour carried out by another actor can be co-opted by a securitising norm entrepreneur who then can either engage in both that same behaviour, committing further operationalised acts of norm construction, or simply use the acts carried out by the other agent to act as the basis for their discursive efforts to build support for that norm. This further suggests that operationalised norm construction is both the basis of effective discursive norm construction efforts and reliant upon perception rather than reality. An act of operationalised construction, much as a referent object, need only be believed to have occurred by the intended audience for it to be an effective means of construction.

Towards a Realistic and Contextual Model

To conclude, the theoretical framework that I propose seeks to take securitisation theory as initially proposed by the Copenhagen School and later refined to be more contextually applicable and reflective of a realistic range of actors and combine it with the theoretical concept of the norm life cycle as proposed by Finnemore and Sikkink. The motivations for this conceptual meeting are based on both the significant overlaps that the ideas contained with these two theories already enjoy coupled with the belief that a further expansion of these leads to the creation of a theoretical framework with significant utility and ability to be applied in a wide array of contexts. The efforts to expand upon the groundwork of Buzan et al. by both Dunn Cavelty and Balzacq are driven further in a manner which not only combines securitisation theory and norm emergence, but concurrently offers a means by which a more complete picture of norm construction in general can be formulated. The inclusion of operationalised norm construction, taking into account the behaviour of actors and how this influences the process of norm construction from initial emergence, securitised or otherwise, through to cascade and acceptance presents a more contextual and grounded theoretical basis for understanding norm construction which I hope can be useful beyond the cyber-focussed analysis of this thesis.

Chapter 4 – Contested norm securitisation: digital privacy versus individual and state security

Introduction: the framework for successful norm securitisation

The purpose of this chapter is to examine the nature of norm development with regards to the digital surveillance of individuals by their states. Rather than attempting to pronounce a moral judgement upon the direction in which these norms are progressing across certain states, I will instead seek to offer an explanation as to how these norms have been shaped, or, more accurately, how the particular shape that they have taken has been justified and supported through the strategic construction of conditions of fear, necessity, and legitimacy. In order to narrow this study to a more accessible context, this chapter will draw specifically upon the digital surveillance-orientated norms of the UK and the European Union (EU); the former offering a state-level vector of assessment and the latter that of an international organisation. Both of these areas also, importantly, have overlapping interests with regards to the policy implications of these surveillance norms.

Within the overarching aims of this thesis this chapter will examine and explain how securitised norms hold a particular relative position of strength and resilience over norms that lack the securitising component. This chapter will analyse how the UK government employed acts of securitisation to successfully construct a normative basis for the creation, extension, and justification of a level of digital surveillance which would, in other circumstances, be considered an unacceptable breach of civil liberties. I will conclude that securitised norms, when constructed effectively through selective use of emotive referent objects of security, facilitating conditions, and piggybacking on the legitimacy offered by international institutions, enjoy a level of natural dominance over contrary processes of norm construction. I will further demonstrate that this pre-eminence of securitisation is, at the very least, a tacitly understood fact by potential norm entrepreneurs. This will be done by showing that the particular traits of acts of securitised norm construction are evident in every ruling political party in the UK, with the language and apparent policy-based intentions of these acts being exchanged at the point where a party moves from opposition into government.

With regards to the further hypothesis of this thesis, regarding operationalised norms, this chapter intends to offer evidence that, within the sphere of domestic politics, discourse-driven norms are still the standard tactic. To prove this conclusion, I will undertake a broad analysis of the nature of normative construction within cyber-security, ensuring that the analysis of this

thesis includes an examination of both domestic and international norms. This analysis will be employed in the final chapter of this thesis – regarding cyber-terrorism – as support for conclusions regarding the potentially policy-centric utility of securitisation, alongside its mistaken application with regards to cyber-terrorism in particular.

This chapter will draw upon politicised actions and securitising acts from both of these points of origin. The chapter draws upon debates in the House of Commons and House of Lords, Acts of Parliament, policy documents, and speeches from the UK and their parallels in the EU, including statements from the European Court of Justice. Particular attention will be given to the debates and policy shifts surrounding the Data Retention Directive issued by the European Parliament and its subsequent dismissal in 2014 and to the Investigatory Powers Act passed by the UK Parliament in November 2016 and its precursory articles the Regulation of Investigatory Powers Act 2000 (RIPA) and the Data Retention and Investigatory Powers Act 2014 (DRIP), with which this Directive had a particularly close relationship.

This chapter will conclude that the UK's normative position with regards to the digital surveillance of its populous has been founded upon a purposeful construction of a state of abnormal politics: a state of fear. Alongside this will be demonstrated how the EU and the UK have entered a period of non-cooperation with regards to digital surveillance. Particular events have resulted in the rejection of the previously accepted and internalised securitised state on the part of the EU, whereas the government of the UK has instead reacted to the same events and circumstances by reiterating and reconstructing the justifications for its previous, securitised position. In examining the act of construction underpinning this reaffirmation of norms of digital surveillance within the UK alongside the concurrent deconstruction of the same norms within the institutional EU, I will bring together the concepts of norm development and securitisation as forwarded by the Copenhagen School and, most notably, Barry Buzan. This amalgamation – norm securitisation as I term it – will be examined and employed across a series of episodic shifts in the development, employment, and construction of the norms of surveillance described above. Analysis of these episodes, arranged in this chapter in chronological order, will seek to demonstrate two things. Firstly, how the deployment of emotive language, imagery, and personal legitimacy can be and has been used to construct support for a norm that under other circumstances, and perhaps without such directed effort, may have failed to become the accepted standard; and secondly, that securitised norms by their very nature enjoy even greater resilience to being undermined by contrary information or efforts to replace them than norms that are without the securitised component. This chapter will demonstrate this relative resilience and ease of norm

construction through the analysis of attempts (such as moves by the opposition parties in the House of Lords and the House of Commons) to counteract the construction of the securitised position held by government and evidenced by the moves towards gaining or extending digital surveillance powers for the state.

Constructing surveillance as a necessity

The first period that this chapter will seek to address through the lens of securitised norms is a time of relatively turbulent political transition within the UK; it will cover from early 2000 and the Labour government of Tony Blair, through the brief office of Gordon Brown, and into the Coalition government of David Cameron paired with the Liberal Democrats under Nick Clegg. This period is bounded by the introduction of the RIPA Bill before the House of Commons in February 2000 and the publication of previously secret documents, provided by ex-CIA employee Edward Snowden, in June 2013 by the *Guardian* newspaper.

Such a transitory period provides the opportunity to address one particular question with regards to the nature of the norms of state cyber-surveillance, that of the impact of partisan positions upon the norm's continued position of influence. It might seem obvious to make the claim that parties in opposition are more likely to be the source of norm contestation, fulfilling the role which is indicative of their position. This period of political change, with regards to the governing party, allows us to test the manner in which the contradictory positions held during periods of opposition are transplanted into actual shifts in dominant norms when that same opposition takes the reins of power.

This section will conclude that political parties in the UK during this period operated along the lines ascribed to them by their positions in government; that the opposition assumes by dint of their role the part of norm contestation, and the party in power seeks to continue to support, strengthen, or justify the norms of cyber-surveillance or surveillance in general that ascribe priority to security over concerns of individual privacy. I will also demonstrate that the tools for constructing a state of securitisation are exchanged with very little variation between incoming and outgoing governments. The task for whichever party is in government is to maintain the perception that the internet is not only a medium for great economic and social opportunity, but by its nature a risk to the public, and one which necessitates certain powers to be held by the government and security services in order to mitigate that risk. The next section of this chapter will show how this act of securitisation is endemic within any debate or proposition of law surrounding the internet employed by the current government as temporary champions of the position of securitised surveillance norms, in order to provide justification for policy and

law that would usually come under greater consideration for its impact upon the interdependent interests of privacy and other civil rights.

The rhetoric of security

Acts of securitisation are dependent on the language used to frame them. There are particular components to an act of securitisation, and further factors that serve to impede or increase its chances of success. The success of such an act is measured by the creation of a platform "from which it is possible to legitimize emergency measures or other steps that would not have been possible had the discourse not taken the form of existential threats" (Buzan et al., 1997, p.25). The act of securitisation, however, is based upon the framing of a particular object as not only under threat, but that the threat is existential, and that the solution requires immediate response. This could come in the form of something as extreme and obvious as a declaration of war against another state, or something less direct – such as the extension of powers granted to security services to infringe upon the rights of citizens. The application of security to any particular object or discourse is not undertaken for its own sake, rather it is applied as a tool with which to increase the likelihood of success in the implementation of policy or response that would usually be unacceptable under conditions without that securitised component.

Securitisation is based upon the perception of this time-critical and existential threat, not upon its reality. A securitising act is simply the application of rhetoric that describes an object that is at risk and a thing that threatens it. However, the success of that act is dependent on the efficacy of the rhetoric in convincing the audience that the threat is not only real, but serious and immediate enough to justify the proposed solution. Thus, acts of securitisation are in fact interchangeable with the same speech acts responsible for the shaping of norms; only they do so through a particular vector and with a particular shape of norm as their goal. The creation of a securitised norm requires then that "an issue is dramatized and presented as an issue of supreme priority" (ibid.: p.26) – the securitising act – and that the securitising agent creates a state of acceptance of this threat, and the need to act, within its intended audience.

To examine the application of such a framework I will begin by looking at the rhetoric surrounding the extension of surveillance and data collection powers in legislation enacted by the Labour government of Tony Blair. The RIPA Bill was first proposed in February 2000 by the then Labour Home Secretary, Jack Straw, to extend the capabilities of the police, security services, and, under secondary legislation, other government agencies, to allow for interception and access to digital communications data which previously had been loosely covered by the Police and Criminal Evidence Act 1984, the Security Service Act 1989, the

Intelligence Services Act 1994, the Criminal Procedures and Investigations Act 1996, and the Police Act 1997. Before their own separate incarnation these powers had been contained in the Electronic Communications Bill. In discussing this Bill the Labour MP Patricia Hewitt made the assertion that such powers were necessary in the light of the manner in which the "internet is transforming crime as much as it is transforming commerce. It provides new opportunities for money launderers, for fraudsters and for those who trade in child pornography" (HC Deb 29 November 1999, vol 340, col 43). Such a reality was described as justification for the inclusion of powers to seize and break encryption of data by the police services. In this instance Mrs Hewitt engaged in an act of securitisation, one aimed at the justification of action that might usually be deemed as contrary to current rules, but in this case justified as necessary to protect children from an existential, immediate, and growing threat.

As mentioned, the encryption escrow controls and surveillance implications previously contained within the Electronic Communications Bill were subsequently transplanted into the RIPA Bill, which extended the capabilities of security services and government agencies to gather communications data for the purposes of investigating and prosecuting criminal and terrorist acts. RIPA too was quickly connected to the potential dangers of the internet to children; the powers within it described as necessary to allow police services to protect children from the predation of child abusers. The Labour MP Charles Clarke described RIPA – as it could be employed by the National Criminal Intelligence Service – as being a key component of the government's action to tackle paedophilia (HC Deb 13 March 2000, vol 346, col 10).

This connection was to be reiterated in support of the Bill at its second reading before the House of Commons. Jack Straw stated that the powers contained within the Bill "are also key to tackling the serious organised criminals involved in money laundering, human trafficking, paedophilia, tobacco smuggling and other serious offences" (HC Deb 6 March 2000, vol 346, col 768). Not only was a similar inference made – that the powers of interception and retention described in the Bill were necessary to minimise the risk to children of abuse – but it was framed in a manner to indicate a level of seriousness and volume to an extent greater than might have been possible prior to the public availability of digital communications. This is demonstrated by the other forms of criminal activity that are mentioned alongside that of paedophilia, and the digital nature of the surveillance powers that this Bill included.

In each of these instances the Labour government had worked to create a platform of acceptance of the need to extend the capabilities of security infrastructure through the

medium of an evocative referent object under immediate and existential threat: children. The demonstration of this application of particular imagery in the furtherance of securitised norms is, however, only half of the purpose of this section of analysis. I would also argue that children, as the referent object of these acts of securitised norm creation, are in fact selected purposefully on the basis of their latent efficacy as the ultimate panacea for any potential counter. With successful acts of securitisation and thus securitised norm creation being dependent on the strength of the argument constructing a platform for action, the employment of children as the referent object serves to immediately restrict the potential for counter-rhetoric, while concurrently strengthening the securitising speech act. At this stage in the debate there was no evidence supplied for the connecting of the insecurity of children to the solution to this problem being increased powers of surveillance: the acts of securitisation evident in this language relied purely upon the emotive power of a risk to something intrinsically innocent.

While these two Labour Parliamentarians employed rhetoric regarding potential threats to children within debates directly focused upon the creation or extension of securitised powers in the form of legislature, it is not only in debates orientated around RIPA and similar Acts that such language can be witnessed. The relationship between the proposed solution to the existential threat against children employed in the debates on RIPA and the Electronic Communications Bill can be witnessed being further underpinned in the reverse direction, as RIPA and the powers contained within it are brought to bear in debates whose central focus is the referent object. One example of this would be the earlier-mentioned inclusion of reference to RIPA by Charles Clarke MP as a tool to be employed in helping to tackle "international paedophile networks through the National Criminal Intelligence Service" (HC Deb 13 March 2000, vol 346, col 10). Another instance of positive reinforcement between this Bill and the safety of children can be noted in the Labour MP Paul Boateng's statement during a House of Commons debate upon revisions to the Protection of Children Act 1978 when he said:

This has been an important and significant debate, not least because, as we speak, the Regulation of Investigatory Powers Bill is being considered in the other place [House of Lords]. The internet has led to an international dimension in these matters; it has the potential for evil – that is not too strong a word – as well as for great good. (HC Deb 12 June 2000, vol 351, col 701)

This comment came in response to previous mentions of the relatively recent implications of digital communications technologies such as Usenet groups and internet chat rooms upon the already accepted threat of paedophiles. However, the inclusion of reference to RIPA was not

entirely necessary. Furthermore, the language employed was particularly emotive; in the same statement the MP emphasised that the powers contained in the Bill were aimed at targeting "child abuse of the most appalling kind" (HC Deb 12 June 2000, vol 351, col 702).

These speech acts – the conjugation of children with a strong and immediate risk – continued to feature periodically in debates in both Houses of Parliament throughout the Labour party's period of representation. RIPA was eventually passed in 2000 with further additions to the original Act eventually passed in December 2003, April 2005, July 2006, and February 2010. At this stage the application of securitising language and frame of reference to evocative imagery was present but limited. Aside from the protections from abuse provided to children, the Act and its subsequent additions were further justified by the necessity to defend citizens from serious crime. During the House of Lords debate considering the application of the powers contained in RIPA to cross-border surveillance in the Schengen Zone, Caroline Flint described the application of these powers as being necessary for "a limited number of serious offences, including murder, manslaughter, rape, arson, aggravated burglary and robbery, extortion, kidnapping, trafficking of human beings, illicit trafficking in narcotic drugs and so on" (HL Deb 19 June 2003, col 275). The emotive connection to children, then, is not the sole source of legitimacy that this form of speech act relies upon; further connections are built between other criminal activity and the protection from these that might be provided by widening of surveillance powers. Important to note is that, once again, limited to no statistical evidence is presented to support the accuracy of this connection.

Alongside the vocal application of securitising moves the connection between communications data (the particular term for the metadata capture component in RIPA) and crime was further supported in the publication of consultation papers. One such, titled *Protecting the Public in a Changing Communications Environment*, was published by the Labour Home Secretary Jacqui Smith MP in April 2009. The following excerpt from the foreword of this document repeats the demonstrative application of potential threat alongside a solution that has been described in earlier sections of this chapter:

Governed by a strict regulatory framework, communications data is routinely used to investigate terrorist plots, to bring to justice those guilty of serious crimes, to seize illegal drugs and to protect the vulnerable in our society. It is no exaggeration to say that information gathered in this way can mean the difference between life and death. (Cm 7586)

In this particular excerpt, there is no direct connection suggested between a threat to children and the solution offered by the collection of communications data by relevant government

agencies. While this is inferred in the mention of vulnerable people, the first and prime targets of this act of securitisation are terrorists. In this instance, the existential threat is being posed as more general, the referent object not just a particularly vulnerable selection of British society, but society as a whole, by dint of the nature of terrorism. This speech act serves to both generalise and personalise the threat being employed; terrorism inspires a fear both to continued existence of the nation and its security, and to the personal security of those individuals who constitute that nation.

According to Buzan et al. the success of an act of securitisation is not only dependent upon the contextual legitimacy of the securitising agent, but upon the social capital of the particular threat employed. Some threats, by their nature, are more likely to result in a successful act of securitisation when paired with a competent speech act and a securitising agent with appropriate legitimacy (Buzan et al., 1997, pp.31–33). In this document these components are ably applied in the use of eight distinct case studies to demonstrate the need for continued access to communications data. Of these eight, three involve children, and one concludes that through access to communications data 30 children were rescued from sexual abuse and 700 suspects were identified across 35 countries (Cm 7586). Another case study describes how communications data resulted in the conviction of a terrorist responsible for two attempted bombings in June 2007 in London and Glasgow (ibid., p.9). This document alone is the perfect vehicle for the extrapolation of the components of a securitising move, one which employs particular emotive facilitating conditions and evocative speech acts to further amplify the possibility for successfully creating a platform of acceptance.

In the Summary section alone, direct effort is employed not only to suggest an existential threat to particular objects, but to describe the explicit immediacy for the need to act to prevent this threat from being realised. For the former, the explanation that access to communications data is “critical to safeguarding the UK’s national security, and in particular to countering terrorist threat” (ibid., p.2); for the latter, with reference to the increasing uptake of digital communications technology as leading to a decline in the “proportion of communications data that is retained by communications service providers in the UK and therefore accessible to the authorities” (ibid., p.3). Together, they result in the well-reasoned, and difficult to refute, conclusion that “Doing nothing is not an option; crimes that are currently detected would not be detected in the future, lives that are currently saved may be lost” (ibid.). The legitimising power that statements such as these have for normative positions is maximised by the moral division that they create. In attempting to question or undermine the securitised norm which speech acts such as this support, the norm entrepreneur

championing an alternative would be undermined by appearing to support an instinctively immoral position. For instance, any attempt to undermine the move to securitisation called for in *Protecting the Public in a Changing Communications Environment* would put the norm entrepreneur in question in the position of appearing to denigrate the importance of human life, the prevention of serious crime, or the protection of the population from acts of terrorism. Thus, it can be considered that securitised norms, and the speech acts which construct them at the domestic level, are inured against attempts to undermine them through the nature of their calls to moral imperatives and emotive referent objects of security.

Continued securitisation: a cross-party tool

The processes and considered acts of construction in *Protecting the Public in a Changing Communications Environment* are as clear as they are lacking in originality. As already demonstrated, similar connections have been made between the need for the government to have the capability to collect and inspect communications data and the risks posed to the public – and purposefully chosen segments of the public – by every Labour Home Secretary within the period of this analysis. However, the application of threat construction, referring to the threat while subsequently offering a way of protecting or at the least limiting the danger of that threat, is by no means a tool employed by solely the Labour party – it is cross-party. That is to say, it is a tool of securitised norm construction or reinforcement that can be employed by whichever political party is currently in government; even so far as to involve the application of near identical language and connotation.

With the change in government of 2010 to a coalition between the Conservatives and the Liberal Democrats, there were no immediate legislative additions to the surveillance framework. That is not to say that there was a complete absence of securitising speech and action from Ministers, however. The increasing prominence of international terrorism within the public domain was mirrored in a number of debates and statements in which room for the reiteration of the connection between security and the necessity for powers of surveillance could be found.

In the very last days of the Labour government the groundwork was laid for a particular relational rhetoric, taking advantage of the prevailing threat of international terrorism. The nature and format (both in terms of content and structure) of securitisation acts that was employed by the previous Labour government in the assertion and support of securitisation and the intercepting of communications data can be seen in the Coalition government document the *Strategic Defence and Security Review* 2009 (Cm 7948). As part of asserted 'National security tasks and planning guidelines' the new Coalition government assumed the

mantle of defending and securitising state cyber-surveillance by stating the requirement for "investment in technologies to support the gathering of communications data vital for national security and law enforcement" (Cm 9748, p.11). Later in the *Review* the immediacy and existential criterion of securitisation are tacitly fulfilled with a further reference to terrorism. The ability to defend the public from harm is further reiterated to rest, seemingly without exception, upon the capability to gather communications data. Removing or failing to renew such powers is framed as a course that would lead to rapid technological advancement of a kind that would leave security apparatus outdated and restricted in its ability to effectively operate:

This programme is required to keep up with changing technology and to maintain capabilities that are vital to the work these agencies do to protect the public. Communications data provides evidence in court to secure convictions of those engaged in activities that cause serious harm. It has played a role in every major Security Service counter-terrorism operation and in 95% of all serious crime investigations. (ibid., p.44)

The language employed, as well as the connections to terrorism, major crimes, state security, and to the necessity of current frameworks of communications data interception, is markedly similar to that found in documents and debates issued by the Labour government for the same purpose, some of which are mentioned directly above. While this document was written and published under the Coalition government there is a distinct continuation of this rhetoric and goal. The MP Theresa May in her position as Home Secretary would go on to employ similar acts of securitised construction in subsequent debates and government papers. In fact, in May 2011 the same fact, that "Ninety-five per cent of serious crime investigations used retained data" (HC Deb 19 May 2011, col 34WS), was employed by Theresa May in connection with discussions in a European Council meeting as to potential alterations to the European Data Retention Directive. The rephrasing of this statistic was repeatedly employed in response to written questions in the House of Commons; in May 2012 James Brokenshire MP answered a question as to the number of arrests under suspicion of terrorism that had resulted from data collected under RIPA by stating that "communications data has played a significant role in every major terrorist investigation over the last decade and has been used in numerous counter terrorism prosecutions" (HC Deb 1 May 2012, col 1453w). The observation that the same fact was employed across a period of several years is, in isolation, insufficient to ascribe a trend or the intent to construct a particular state of understanding with regards to the necessity and efficacy of communications data-based surveillance. However, taken in concert with the context of surrounding language, the use of referential terms such as "vital" and

"critical" (HC Deb 16 January 2012, col 468W; HC Deb 10 September 2012, col 19W) and the proposition of the Communications Data Bill in the Queen's Speech in May 2012 (HL Deb 9 May 2012, col 1), the connection is far more distinct.

This connection was made by an opposing Conservative MP on the same day of the aforementioned speech when David Davis stated that he was glad to see that the announcement seemed to suggest the opportunity for scrutiny of the Bill before its movement into law "because I am afraid the proposal is very similar to what the Labour Government came up with". He said that he was surprised "that the Government have made the proposal, because both coalition parties opposed it in opposition, and as far as I can see, it goes against the coalition agreement" (HC Deb 9 May 2012, col 33). Mr Davis goes on to reference a speech made by David Cameron at Imperial College London in 2009 while he was leader of the opposition, making the following quotation:

Faced with any problem, any crisis – given any excuse – Labour grasp for more information, pulling more and more people into the clutches of state data capture...And the Government doesn't want to stop with the basic information…Scare tactics to herd more disempowered citizens into the clutches of officialdom, as people surrender more and more information about their lives, giving the state more and more power over their lives. If we want to stop the state controlling us, we must confront this surveillance state (Cameron, 2009).

The manner in which, on switching from opposition to government, the Conservative party also switched roles from the opponents of securitisation to the securitising agents themselves is ably highlighted by Davis with reference to this speech. Furthermore, when examining the language employed earlier in this same House of Commons debate by David Cameron (by this time acting as Prime Minister) it can be seen that the rhetoric of this exchanged position has also been almost directly transplanted: "it is that information [communications data] that has solved almost every serious crime and certainly almost every serious terrorist offence…I do not want to be the Prime Minister standing at this Dispatch Box saying 'I could have done more to prevent terrorist acts, but we did not have the courage to take difficult steps'" (HC Deb 9 May 2012, col 20). Once more, the purposeful connection to terrorism is made, but further to this the language is used to turn the audience to consider that failure to grant or maintain these powers will lead to violence for which they themselves will then be at least partially responsible. As the Committee wrote in 2009, "Doing nothing is not an option." Such an argument is not only powerful in its attention to referent objects with inherent power (the state itself), but is heightened in its impact through the personal application of potential guilt to the government should the threat be realised.

Contesting security: a call to liberty…and cost

Concurrent to the construction of a counter-causal link between the abuse of children, terrorism, and serious crime, and the lack of or limited capability to capture and examine communications data by whichever party is in government (at the time the Labour party), the opposition's critique of policy and general position also comes in the form of a rhetoric that is transposed from one party to the other at the point of transition of power. The most common points of criticism up until the revelations of Edward Snowden in 2013 were infringements on liberty, incompatibility with international agreements and norms, technological incapability, and, most commonly, infringements upon business interests and related costs to industry.

From the theoretical perspective of the Copenhagen School the success of a securitisation act has little to no grounds in the external actions of potential opponents to this construction of political reality. An act of securitisation is successful or not based on the manner in which the securitising agent can employ their own legitimacy, itself constructed from a variety of sources, against the audience which said agent must convince of the existence of an immediate and existential threat to a referent object; a purposeful, political act that utilises imagery and connections with ideally strong social embeddedness to which the audience will feel obliged morally, ethically, ideologically, or emotionally to protect. Here, protection involves the acceptance of a state of politics beyond the realms of normal acceptability as a necessity to provide security – an exchange. I would argue that not only are there more components to a successful act of securitisation that can be engaged upon by the agent to maximise their potential for success, but that those in opposition to this securitising step may, through application of their own act of securitisation (a counter-act) reduce the potential efficacy of the speech acts employed by the securitising agents.

Simon Hughes MP, at the time Liberal Democrat Shadow Spokesperson for Home Affairs, made two central critiques when specifically discussing RIPA in 2000. Firstly, he raised fears that forcing business to create and maintain the capability to collect and store information as detailed in the Bill would mean that "the regime in Britain will be less helpful and more dangerous and threatening to it than a regime elsewhere" (HC Deb 8 May 2000 vol 349, col 534). He also raised the prospect that the Bill was at risk of "getting the balance wrong between the state and the individual" (ibid.). Such an assertion is accurate. During the consideration of RIPA in 2000, the Conservative MP David Maclean made the following observation in the House of Commons as to the nature of Select Committee discussions on that Bill:

It dealt with clauses giving draconian powers to the security service, the special intelligence service, Customs and Excise, MI5, the fisheries inspector, the Department of Health dodgy medicines inspector…The Committee regularised their draconian powers to undertake covert surveillance, directed surveillance, and for some of the top security agencies of the state, electronic surveillance such as tapping e-mails. The Minister of State, Home Office, the hon. Member of Norwich, South (Mr. Clarke), was extremely courteous, and meticulous in assuring the Committee that the powers for people to enter private property and bag all mail and correspondence were necessary only because there were serious issues at stake (HC Deb 10 April 2000, col 105).

This statement contains not only further reference to the illiberal consequences of the Bill, but the assertion that the necessity for these "draconian" measures was based upon serious issues or threats. The extract above contains both recognition of the potentially problematic nature of the powers being granted, as well as an example of the manner of their justification. It is also demonstrative of how not only does the intent to securitise transfer from the party in government to the opposition at the point of exchanging political role, but the language and thus the methodology also is ported from one party to the other.

Just as there is evidence of repeated patterns of language and construction of immediate and existential threat over this 12-year period, and without moderation by political divide, the same is true of the nature and content of the arguments against this same securitising discourse. Not only are the criticisms of illiberal consequences concordantly employed by the Conservatives and the Liberal Democrats, and by Labour and the Liberal Democrats to a lesser degree during Coalition, but the spectre of adverse impact on business is similarly shared. Such a position of critique was expressed in the House of Lords by Conservative Peer Lord Cope of Berkeley when he qualified his acceptance of the threats posed by criminal applications of the internet:

The internet is capable of not only making business more efficient, but of making crime more efficient. It is important to address the problem and move forward alongside other nations, but we should not make our companies – not just our e-companies but all our companies – uneconomic and uncompetitive (HL Deb 19 June 2000, col 16).

In effect, the reference to potential negative economic impacts of securitised policy is meeting the construction of one system of threat and referent object with another. The former system is based upon personal or physical security under threat from terrorists, paedophiles, or criminals, and the latter, proposed to counter it, is a more generalised threat to the economic

security of a nation dependent upon business investment both present and future. There is some notable variation in the language of opposition, more so than can be observed in that of the party in government. While the government sticks with greater rigidity to the structures and linguistic tools of construction without any real detectable political or ideological impingement, the opposition shows a variation in the priority in which it orders its counter claims of threat or risk. During the Labour government between 2000 and 2010, with the Conservatives in opposition, of the earlier listed critiques of the collection of communications data (infringement of rights, technical complexity, financial cost to business/state, incompatibility with international norms) the most common to be applied as an alternate and countermanding act of securitisation was the risk to economic security through the impact on business of legislation, whereas during the Coalition government the most common alternative act of securitisation was geared towards privacy and human rights – a securitisation act along the lines of human security.

In the first session of the Standing Committee into RIPA in March 2000 the second statement, made by Oliver Heald MP, makes significant reference to the potential impacts upon British business, especially with regards to its ability to create an environment attractive to the increasingly lucrative digital industries. Mr Heald references a director of The Federation of the Electronics Industry and British Telecommunications as examples of concerned actors as to the financial implications of RIPA, asking whether Charles Clarke MP, the Minister of State present representing the Home Office, had consulted on these costs or if he is asking Parliament to "give him a blank cheque" (RIPA Deb 14 March 2000). The spectre of damage to business interests continued to be raised by the Conservative party, as well as the potential for costs incurred by the government itself through the development of capability and the reimbursement of costs to business that were allotted under RIPA when it passed into law (HC Deb 12 March 2007, col 112W; HC Deb November 2009, col 1059W). The House of Lords also saw a counter-act of securitisation along the lines of business impact; Lord Cope of Berkeley gave the best summation of this position at an early stage in the Lords' consideration of RIPA after the Bill's second reading when he described the growing consensus of business institutions about the implications of the Bill:

A rare combination of allies against the Bill has developed among business and financial organisations. Today, the British Chamber of Commerce has published a detailed report by an impressive panel, edited by two gentlemen from the London School of Economics and from University College London – neither institution is normally known as a force of conservatism – which concludes, among other things, that the costs to service providers of compliance would

be £650 million over five years, and continuing thereafter. It has also concluded that the effects on the economy would be well over £35 billion over five years in the transfer of business to overseas jurisdictions. These are very serious figures (HL Deb 12 June 2000, col 1404).

In this instance, Lord Cope's reference to the costs of compliance as potentially prohibitive to businesses remaining in the UK, especially businesses that are entirely web orientated – an industry that any country would want to attract – sets the form once again for the shape of Conservative opposition for the next decade and in some cases beyond it. David Davis MP was still holding up the risks of ostracising business through compliance with database creation as well as the negative implications towards individual privacy when the Coalition government was seeking approval for the Draft Communications Data Bill in 2012. He argued that by allowing the Bill to pass in its current form "we would create something, which some Ministers said will cost £2 billion – the London School of Economics suggests that it will cost £12 billion – that will not be effective against terrorism, but constitutes general-purpose surveillance of the entire nation" (HC Deb 9 May 2012, col 33).

Mr Davis's particular case is one which could potentially benefit from consideration, his position is almost unique in that despite the shift in his party's place from opposition to government his position on the matter appears to have remained unchanged. He thus finds himself closer aligned with the Labour party after the formation of the Coalition with regards to electronic surveillance. Labour in effect assume his rhetoric. This comprises both the almost expected Conservative position of supporting business interests, but primarily the position that individual rights, privacy, and other protectionism should take priority or at least equal place in balancing security from physical harm and the erosion of principles of human security.

Labour in opposition take the process of securitisation that they had employed while in government to construct a platform from which digital surveillance policy and law that pushes the boundaries of usual acceptability can be justified and turned upon itself. While the Conservatives, and to a lesser extent the Liberal Democrats, take up the task of maintaining the securitised norm that Labour went to such efforts to construct, the Labour opposition now engages in an act of counter-securitisation that is so similar in approach to that of their own earlier securitisation acts to be all but indistinguishable. Securitisation as described by Buzan and his fellows within the Copenhagen School is by nature employed to prioritise a threat to such an extent that political action that would normally be outside the bounds of acceptability is normalised; this school of thought would also describe political acts to undermine this state of securitisation as de-securitisation. However, I would argue that such terminology is not a

fitting descriptor in this case (Buzan et al., 1997, pp.28–30). They further assert that issues from the gamut of human security, such as the environment, are just as at risk from the normatively negative effects of securitisation as those issues traditionally associated with security: "groups are using a securitizing logic that exactly follows the format prescribed in the previous section: The environment has to survive; therefore, this issue should take precedent over all others" (Buzan et al., 1997, p.38). I would suggest that what was being seen in the case of contestation within the British Parliament over the securitised norm of digital surveillance was *not* an instance of securitisation on the one hand and de-securitisation on the other; it was instead one of *vying moves* of securitisation where the dominant securitised norm is being actively countered through the active employment of a contrasting and directly contradictory *alternative* securitising act.

There are in effect multiple combative securitising acts being forwarded by the Labour party (and to an extent the Liberal Democrats in attempting to balance Conservative interests) against the Coalition government's inherited securitised norm. These are ordered differently, due to ideological influence, then the same counter-securitisation acts employed by the Conservatives when roles were reversed. The securitisation act that enjoyed the greatest popular employment across the Labour party and the Liberal Democrats alike consisted of component parts identical to those found in acts of securitisation dealing with violent threats: a referent object that was threatened, in this case once again the public in a general and individual sense; and a threat that was both immediate and existential: the interference of the state with the right to privacy. An exemplar of this can be extracted from a speech by the Liberal Democrat MP for Cambridge Julian Huppert, which was made in October 2010. In it he references a case where the intercept powers granted to businesses within the Digital Economy Act 2010 led to a mother discovering that her son was gay after her Internet Service Provider (ISP) sent her a letter accusing her of illegally downloading homosexual pornography (the illegality was based on the copyright of the content not its nature). Mr Huppert states that this "is not the way that privacy should be broken" (HC Deb 28 October 2010, col 151WH). Herein he is employing a socially anchored facilitating condition with regards to the right of privacy and the expression of sexual identity being undermined in a relatable case. This statement not only denotes the threat and both personalises and generalises the referent object to both select groups and individuals, but also describes a level of immediacy of action, given that the event employed as the example is not hypothetical, but has recently taken place. The MP goes on to re-emphasise all of these points and to address the current securitised norm which his own seeks to contradict:

I remind the House that the IMP [Interception Modernisation Programme] was an ambitious £2 billion project that would have forced ISPs to log clients' internet and e-mail activity for at least 12 months. That, I believe, is a great infringement of privacy. Indeed, the coalition agreement explicitly stated that

"we will end the storage of Internet and email records without good reason".

There is no doubt that we face threats from cyber-terrorism. Malicious breaches of security could cost the Government, businesses and individuals dearly in all sorts of ways. However, that does not give the Government the excuse to use a sledgehammer to crack a nut. (ibid.)

Not only does this closing statement employ the format and tools of an act of securitisation, but it is also directly targeted at the product of a previously successful act of securitisation and the norm that resulted from this success: the IMP. A second notable feature of this and other speech acts to take on a similar format and intent is the purposeful attention given to the threat relationships employed by the securitising acts which they are opposing. In this example, Mr Huppert directly mentions the threat of terrorism, but he then employs his own framework of security as a counter, once more relating the threat to the individual rather than the state and the potential for the latter's misuse of power.

Norm securitisation: the deconstruction of counter-securitisation and selective institutionalism

The subject of internet privacy and digital surveillance by the state has become more prevalent within the Houses of Parliament due to additions to specific Acts such as RIPA, general debates, and reports from various commissioners responsible for reporting on the government's application of these powers. The responses to these statistics have, since 2010, been increasingly answered with critique from the opposition along the lines mentioned earlier in this chapter.

The response from government, in this case the Coalition, demonstrates how the application of the singular, instance-based framework of securitisation acts is limited. We must analyse repeated speech acts attached to the same regime of securitisation that a previous securitisation act (or series of acts) may have achieved; that is, a *compounding* of securitisation via different logics. This provides further evidence of a state of internal acceptance of a norm of securitisation, itself being a more accurate term for a state of securitisation that continually requires and includes further speech acts to maintain its validity and momentum with regards to policy action.

Such acts in this period of British politics are not only found in the repeated application of the construction of threat and object relationships that I have previously described; they are also

evident in the manner in which the contradictory acts of securitisation employed by opposition to this securitised norm are themselves directly engaged with in an attempt to undermine their efficacy. These challenges take on two forms: applications to a greater, institutional authority; and the deconstruction of contradictory moves of securitisation. The former can be interpreted as a complementary move that can be and is also applied alongside acts of securitisation. If securitisation acts are interpreted to be the active construction of a connection between a threatened object and an immediate and existential threat to that object, employed for the purposes of justifying a shift in politics beyond the norm, then implicit in this action is the recognition that the norm that is being aimed for will formulate policy that likely infringes expectation of freedoms and rights. Within the discourse of digital surveillance this recognition has become explicit, and I argue that it has done so not in a purely reactionary manner, but instead as an attempt to strengthen the chances of success for the surveillance-orientated securitisation act while simultaneously undermining the human security-orientated securitisation act that is being directed against it in challenge.

In the example of the UK I have already explained how, with the utilisation of socially internalised threats to emotive groups, the trade-off with regards to digital privacy and other freedoms has been countered within the discourse regarding the creation and maintenance of a norm of securitisation allowing digital surveillance. The supporting construction of these acts is one which serves to increase the likelihood of an audience's acceptance of the state of securitisation through the explicit minimisation, or at the least subordination, of the damage to freedoms that might be impacted by this policy. Rather than concentrate purely on the construction of threat, these multi-faceted acts of securitisation employ a more nuanced approach by building an immediate and existential threat while at once undermining claims about the costs balanced against the moves described as necessary to counter them.

An example of a securitisation act which at once creates threat, while seeking to maximise its potential for a successful securitisation move in favour of digital surveillance by diminishing the force of the human securitisation-orientated acts directed against it, can be found in Prime Minister David Cameron's statement regarding the annual report of the Interception of Communications Commissioner in July 2012. His opening introduction states that the "Commissioners play a vital role in ensuring that public authorities make use of these powers in a way which is necessary, for a legitimate aim and which is proportionate to what is sought to be achieved" (HC Deb 13 July 2012, col 90WS). This is a subtle yet not undetectable reference to the fact that the powers of collection and application of communications data do have an impact upon the privacy that many expect to be naturally provided in a democratic

society. His closing statement, however, reiterates that the price paid – of limited infringement on privacy – is a necessary and acceptable one for the goal of security from the same threats I identified in the earlier discourse analysis. He goes on: "The Commissioners also highlight the value of the use of these powers and provide a number of case studies to show the benefits they provide, particularly in terms of preventing and detecting serious crime and tackling threats to our national security" (ibid.). In this case, risks to the prevention of serious crime and to national security, and the provision of powers to mitigate these risks, are mentioned explicitly alongside the cost of these powers in the potential for misuse and for the lessening of the expectation of individual privacy. Immediately prior to the above excerpt, Mr Cameron states that he accepts that "there have, regrettably, been breaches and errors in the use of these powers" (ibid.). Mr Cameron is in this case supporting a previous, successful act of securitisation that has through repeated justification become a norm. He does so through the explicit acknowledgement of the cost of this norm and by then actively reducing this cost by depersonalising it and thus reducing the ability of this alternative, human security act to counter the existent norm.

A more obvious of example of this form of construction can be extracted from a written response by James Brokenshire MP in September 2012:

The Government are committed to ensuring that law enforcement and intelligence agencies have the capabilities they need to protect the public from crime, disorder and terrorism, consistent with its wider approach to preserving civil liberties, including the right to privacy and safeguarding national security. Information relating to the activity of criminals online is critical to the investigation and often prosecution of their crimes. (HC Deb 10 September 2012, col 18W)

He is answering a question as to what plans the government had to increase the powers of police forces to monitor criminal activity online. His response builds the relationship between referent object (individuals and the state) and well-known and emotive threats, alongside a recognition of the importance of civil liberties and privacy. This answer further exemplifies the application of a component of the act of securitisation intended to diminish the perception of impact caused by the policies to be enacted under this securitised regime. In reference to the draft Communications Data Bill, which had at this point only recently been published, Mr Brokenshire employed a particular phraseology that directly utilised this tactic and became a critical part of discourse surrounding this draft Bill for years to come. He stated that "this proposed legislation [the Communications Data Bill] will enable more of the communications

data (the who, when, and where of communication, but not its content) required by law enforcement and other agencies to be retained by communications service providers" (ibid.).

In chemistry, the term 'activation energy' is used to describe the threshold of energy that must be met in order to overwhelm the opposing chemical bonds, a necessary step for a successful chemical reaction. In this instance, the attempts by securitising agents in favour of surveillance to diminish the impact on freedoms, specifically privacy, are in essence aiming to lower the activation energy required for a successful act of securitisation. By explicitly accepting a cost to privacy of the success of the proposed act of securitisation, but then reducing the apparent relative price of that cost by stipulating a manner of infringement that at face value appears minimal, the government, through Mr Brokenshire, is in effect significantly lowering the necessary threshold of energy that the concurrent threat construction component of securitisation has to meet in order to successfully be accepted by its audience.

The secondary tactic for counteracting the opposing securitisation acts is the assertion of legitimacy based upon higher institutions. In this case I refer to the EU, and, more specifically, the European Convention on Human Rights and the Data Retention Directive of the European Parliament. These actors in effect, by referencing these international, institutional legal regimes and bodies, circumvent the question of whether civil liberties are being infringed. They do so by stating explicitly that the powers contained within legislation such as RIPA or the Communications Data Bill are beholden to and compatible with the standards of Europe, and thus implicitly cannot be an incorrect balancing of freedoms versus security. Again, there is evidence of this in Mr Brokenshire's 2012 written answer when he states that the Communications Data Bill "will also retain and extend safeguards and oversight arrangements for the acquisition of these data [sic] that exist under current legislation, ensuring compliance with the European Convention on Human Rights" (ibid.).

Demonstrating once more that securitisation and the complementary components discussed in this chapter are independent of political party or ideology, the selective application of and appeals to international norms and regimes can be seen to be employed by Labour and by the Coalition throughout this period. In 2010, four months prior to the general election that saw the formation of the Coalition government, Alan Johnson MP drew upon the European Data Retention Directive as the basis for the Interception Modernisation Programme. He argued that, since it was first negotiated in 2005, "there has been continuous and innovative development of communications services and applications, many of which are not covered by current data retention legislation" (HC Deb 28 January 2010, col 1048W). Using this Directive as a legitimising foundation for the necessity and acceptability of data retention, the Home

Secretary of the time then went on to state that this innovation had “already started to undermine the capabilities of our law enforcement and national security agencies to protect the public” (ibid.).

In responding to a question referencing the implementation of this Data Retention Directive after the formation of the Coalition, the Minister for Policing and Criminal Justice, Nick Herbert MP, stated the government position. This was that the directive “provides a valuable basis for retaining communications data that is critical for serious crime investigations and to counter terrorism, both in the UK and elsewhere in Europe” (HC Deb 17 November 2010, col 813W). Such a statement not only draws upon the legitimacy of the European Parliament, but on the necessity created by the levelling of the threat of terrorism or crime as the alternative to effective implementation; a multi-faceted act of securitisation with a similarity to the construction of the same acts by the previous government.

Regarding the socialising effects of institutional membership and interaction, Liesbet Hooghe argues that top officials within the European Commission (the particular case study central to her research) “take their cues from their national environment. Several roads lead to Commission norms, but few run through international socialisation” (Hooghe, 2006, p.862). There is evidence to support such a conclusion within the discourse regarding digital surveillance in the UK. As demonstrated above, there are examples of MPs employing the European factor of surveillance norms and legislature to give greater legitimacy to their statements, and as a counter to the criticisms of their opposition with regards to infringements on civil rights. However, there are examples, especially after the transition to Coalition government, where the European frameworks are still employed but are themselves held up as only partially effective solutions to the threats that have been created. This is especially true when these European legal underpinnings are questioned within the national institution in which they were formed and the prospect of redressing the balance of privacy versus security, in favour of the latter, is raised by Europe.

In a briefing to the House of Commons, the day after a European Extraordinary Council meeting, Theresa May describes how an evaluation of the Data Retention Directive will suggest “that changes should be made to the Directive which potentially include greater restrictions on the data types that are retained; greater restriction to access to the data; and greater harmonisation including possibly shortening the periods of mandatory data retention” (HC Deb 11 May 2011, col 38WS). Her immediate response to this possibility is as follows:

The UK strongly supports the existing directive as it provides a valuable basis for retaining data that are [sic] critical on an ongoing basis to counter-terrorism and serious crime investigations, both in the UK and elsewhere in Europe. We welcome the fact that the evaluation report recognises the value of retained communications data to maintaining security in the EU. We recognise the importance of strong data protection but have concerns that some of the changes the Commission are considering would have an adverse impact on UK operational capabilities.

These conjoined statements suggest that the borrowing of legitimacy from the European Institutional level in earlier political statements was in fact just that – borrowing. It gave the appearance of socialisation, of the acceptance of norms as described at the institutional, international level. The reality, however, is that this was a relationship of expedience. Rather than a trickle down spread of norm acceptance from the EU to the UK at the national government level, it was instead a joint, unequal acceptance of similar norms which led to a shared and in a way interdependent rhetoric; right up until the point that these institutional norms no longer provided the framework of security and digital surveillance that the UK government was itself in favour of.

At this point it is not difficult to see why a liberalisation of the norms of data retention from Europe might prove problematic to the position of the UK government. The progression of the Interception Modernisation Programme (initially a Labour platform that included individual ID cards for British citizens, which was rebooted under the Coalition) included as a core component the Communications Data Bill (which would in 2016 come into force as the Investigatory Powers Act 2016). Much like RIPA, this Bill was reliant upon the acceptance of communications data retention as a necessary tool for the prevention of acts of terrorism and serious crime. The removal of the European level of institutional support and thus the continued legitimacy of this tool was a serious threat to the credibility, and thus the success, of securitisation acts reliant upon, and the securitised norm that in turn relies upon, these acts.

Norm crisis and response: demonisation of functional actors and the emphasis on emotive threat

The revelations of Edward Snowden caused a dramatic shift in the inter-relation of institutional norms of securitisation at the international and national state level. With the release of previously classified documents to journalists at the *Guardian*, *Der Spiegel*, and others, Snowden shed light upon the way in which the norms of state digital surveillance were being acted upon by both the UK and its allies. By displaying the reality of how the success of these

norms impacted upon the day to day application of digital surveillance on the citizens of Europe and its constituent states, Edward Snowden managed to add weight to the counter-acts of securitisation forwarded by the opposition in government and from civil society groups and to undermine the original securitising acts of digital surveillance by emphasising the detrimental impact of this norm on individual freedoms.

Insights into programmes engaged in by the members of the Five Eyes treaty signatory nations, such as the data-sharing regime of Tempora, resulted in a reassessment of the balance between physical security and human security that had previously rested in favour of the former. A significant impact of this was the rejection of the European Data Retention Directive after a legal challenge before the European Court of Justice (ECJ). Previously, this Directive had been the institutional and legal foundation for claims of international legitimacy for localised national norms of data retention for the purposes of security. The ECJ declared the Data Retention Directive invalid in April 2014, stating that "by requiring the retention of those data and by allowing competent national authorities to access those data, the directive interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data" (Court of Justice 2014 54/14).

This section will demonstrate how, as a result of the withdrawal of an international and institutional source of legitimacy for the norm securitised within the UK, the nature of the acts seeking to support this construction changed. I will show how, alongside the continued emphasis of threat to particularly emotive groups such as children, the discourse, both in political forums of debate and in more public domains, became more prolific and was enacted with an even greater level of evocative imagery and application of facilitating conditions.

Institutional norm divergence: rejection of legitimacy

The release of evidence by Edward Snowden demonstrated how the legal frameworks based on the securitised norms of surveillance were being employed. The direct and personal infringements of privacy and the scope of surveillance that were shown through this documentation served to add greater impetus and greater legitimacy to the acts of counter-securitisation that had been employed by political opposition, private individuals, and civil rights groups.

The joint court case brought by Digital Rights Ireland (DRI) and a number of private individuals against the Data Retention Directive began with a case directed not against Europe but against the Irish government in 2006. In announcing the legal challenge directed initially at the Irish government, DRI made the following statement:

We also challenge the claim that the European Commission and Parliament had the power to enact the Data Retention Directive. We say that this kind of mass surveillance is a breach of Human Rights, as recognised in the European Convention on Human Rights and the EU Charter on Fundamental Rights which all EU member states have endorsed. (Digital Rights Ireland, 2006)

DRI directly referenced the same European directives and legal frameworks that the British government continued to employ as a source of legitimacy even as this case continued. The case continued for eight years, progressing from the Irish High Court to the ECJ. It acts as a litmus test, demonstrating which form of securitisation, in favour of surveillance or in favour of securitising individual rights, is currently dominant at both national and international levels. Thus when, in light of the leaks by Edward Snowden, the ECJ ruled in favour of DRI and invalidated the Data Retention Directive, it was apparent that not only had the international balance shifted heavily out of alignment with the position held by the Irish and British governments, but that employing institutional legitimacy to support the securitised norm of surveillance at the national level in these countries was no longer going to be effective. This had an even greater impact than it may have done at any other point. This is because, concurrently to this dismissal, and alongside the Snowden revelations, the British government was seeking to extend the reach of the current regime of surveillance in the form of the aforementioned Communications Data Bill.

As a result of the rejection of this Directive, which formed the basis for the UK's legal framework for data interception and digital surveillance, there was another shift in the form in which securitisation acts were constructed and applied. Rather than drawing upon the legitimacy of Europe to aid in the successful application of securitisation acts – and maintaining the normative state created by this – the Conservatives in particular began to instead undermine the framework that was the cause for this Directive's dismissal: the European Convention on Human Rights.

The UK had progressed from enacting the Data Retention Directive while holding the Presidency of the EU Council to building its legal frameworks of data retention and surveillance around this Directive, to utilising the legitimacy of the international and institutional source of this foundation, to having to reject that same legitimacy. The result was the rapid creation of a new legal framework – the Data Retention and Investigatory Powers Act (DRIP) – which "simply preserved the existing capabilities and extended current safeguards to respond to the European Court of Justice judgment on the Data Retention Directive 2006" (HC Deb 24 October 2014, col W), according to James Brokenshire MP.

The EU Data Retention Directive was ruled as invalid on 14 April 2014. On 10 July the DRIP was published, and then introduced to Parliament on 14 July, before receiving Royal Assent on 17 July. The debate surrounding this Act, which processed so rapidly through Parliament and into law, was in effect a distillation of the longer period of discourse that I assessed referencing RIPA and the continuing need for those powers up until this point in time. The metaphor of distillation is fitting not only for the period of time over which these norms were in effect rebuilt, but also for the tools employed to do so (the securitisation acts), which employed the same formulae and components, but did so in a more concentrated and in many ways less subtle form.

On 10 July in the House of Commons, in a speech initially given by the Home Secretary Theresa May and then repeated by Lord Taylor of Holbeach, Mrs May made the following statement alongside the publication of DRIP:

I can tell the House today that the Government are introducing fast-track legislation – through the Data Retention and Investigatory Powers Bill – to deal with those two problems. I deal first with communications data, because we must respond to the ruling by the European Court of Justice that the data retention directive is invalid. The directive was the legal basis upon which the Governments of EU member states were required to compel communications service providers to retain certain communications data where they do not otherwise require it for their own business purposes (HC Deb 10 July 2014, col 456).

In order to justify the fast-tracking of this process, normal principles and practice must be circumvented, and in this instance this was done through the application of an act of securitisation, one which again employed the emotive relationships of particular threats and referent objects, but this time concentrated to a much higher degree. In this statement Mrs May lists a number of events and describes the importance of communications data to the investigation of these events and the potential to prevent similar events in future: “the Oxford and Rochdale child grooming cases, the murder of Holly Wells and Jessica Chapman, and the murder of Rhys Jones” (ibid.) are all employed. Each of these contains a high level of social capital due to the nature of the victims of these crimes (all of them children) and the level of coverage they had in national news. This made them powerful facilitating conditions to employ to add impetus to an act of securitisation.

In moving DRIP to read a second time before the House of Commons, Mrs May stated that without the powers sought in that Bill, “we run the risk that murderers will not be caught, terrorist plots will go undetected, drug traffickers will go unchallenged, child abusers will not

be stopped, and slave drivers will continue their appalling trade in human beings" (HC Deb 15 July 2014, col 704). While the Bill was before the House of Lords, she stated that without "access to communications data, the investigative capabilities of public authorities in relation to online child abuse would be significantly damaged, and vital evidence would be inaccessible. If companies do not retain that data and we cannot access it, it will become impossible in future to carry out such operations" (HC Deb 17 July 2014, col 1011). Every debate in the House of Commons or the House of Lords with regards to DRIP contained reference to the potential risk posed to children if the Bill were not passed (HC Deb 29 November 1999, vol 340, col 43; HC Deb 13 March 2000, vol 346, col 10; HC Deb 10 July 2014, col 456; Cm 7586). Most also contained references to terrorism and organised crime (HC Deb 14 January 2015, col 869; HL Deb 19 June 2003, col 275; HL Deb 19 June 2000, col 16). The methods seen (applied over an extended period of time in order to create the right conditions) and the normative position (in which communications data and its collection should be allowable under RIPA) can be seen playing out again here, but compressed and concentrated in such a manner as to make the purposeful construction involved all the more apparent.

It is also repeated several years later when, due to a sunset clause in DRIP, there was again a need to formulate a new legal framework to allow for the functional application of the securitised norm of surveillance which the previous governments – Conservative, Coalition, and Labour – had worked so purposefully to construct. Yet again, the selection of children to be the referent object for which to construct an immediate and existential threat was employed, alongside the direct threat to the nation through the catch-all of "national security" (Cm 7586). With the Communications Data Bill still under discussion in a number of committees and a key part of government strategy, a number of instances with high social capital were employed to further strengthen the chances of success for the related acts of securitisation. This time, though, these acts were not limited to children as the referent objects, but were more generalised. In January 2015, one week after the terrorist attack on the offices of *Charlie Hedbo* in Paris, Theresa May MP made the following statement in the House of Commons:

We have always been clear that the police and the security agencies must have the capabilities and powers they need to do their job, and following the attacks in Paris the Prime Minister has reiterated that commitment. Unfortunately, when it comes to communications data and the intercept of communications, there is no cross-party consensus and therefore no Parliamentary majority to pass the legislation to give the police and security services the capabilities they need. Let me be absolutely clear: every day that passes without the proposals

in the draft Communications Data Bill, the capabilities of the people who keep us safe diminish; and as those capabilities diminish, more people find themselves in danger and – yes – crimes will go unpunished and innocent lives will be put at risk (HC Deb 14 January 2015, col 869).

In the House of Lords the connection between the Paris attacks (on the Bataclan theatre and the Stade de France) later that year and the need for the power to retain and access communications data was made just four days after these second attacks. Lord King of Bridgwater said:

For more than two years, we have been trying to consider the gaps that exist in our armoury of what is available to our intelligence services to protect our country. Two weeks ago in this House I asked a question about the Investigatory Powers Bill [the new iteration of the Communications Data Bill], pointing out that we now embarked on a pretty leisurely process which, if we are lucky, will get those powers into effect by next September or October. I wondered at that time what events might happen between now and then. I am all too sorry that within two weeks that has proved to be the case (HL Deb 17 November 2015, col 23).

Lord King goes on to suggest that in the light of this the Bill should surely be put through the remainder of its considerations towards being passed at an accelerated rate. Both of these statements employ the political capital of the very recent and very high-profile acts of terrorism to maximise the strength of the securitisation act in which they are engaging, and thus the likelihood of success with regards to creating the platform for which this Act and the powers within it will be granted.

The implications, then, of the ECJ's decision to invalidate the Data Retention Directive were a divergence of securitised norms. While the ECJ set about asserting the primacy of civil rights and the ownership or protection of data, the UK government instead set about re-constructing the normative foundations of the existent regime of data collection and inspection. To do so, it employed the same components of securitisation and of success maximisation as employed by previous governments. The difference was, that due to the damage inflicted by the spotlight shone by Edward Snowden's revelations, and the counter-norms of human security employed by civil rights groups and now the institutions of Europe, these acts of securitisation had to be amplified to meet this threat.

Conclusion: normative resilience and ideological ambivalence

My analysis of various acts of securitisation employed by successive governments of the UK has led me to a number of conclusions. Firstly, that the usage and structure of securitisation

acts shows little to no variation from one government to the next. While the discourse and rhetoric employed or the manner in which it is prioritised might change depending on the ideological nature of the opposition, there is little to none of this differentiation on this issue for whichever party or coalition of parties is in office. The support of a securitised norm of surveillance, the use of facilitating conditions with effective political capital, the use of emotive referent objects such as children, and the creation of threats which are both immediate and existential to these units, have all been identified in the Labour government's discourse around the Regulation of Investigatory Powers Bill; the additions made to this Bill under the Coalition government; and in debates around the Data Retention Directive, the Data Retention and Investigatory Powers Bill, and the draft Communications Data Bill.

The concept of securitised norms and the specific manner and nature of their construction can thus be considered to be a phenomenon that is endemic within the domestic politics of the UK and other states. The efficacy of these norms is, at the very least, implicitly recognised by those within domestic politics who fulfil the role of norm entrepreneurs. The greater resilience and potential for successful acceptance by the targeted audience that is intrinsic to the manner in which securitised norms are constructed results in a political toolset for norm entrepreneurs that is seemingly impossible to ignore. The evidence provided by the manner in which these norms can be witnessed across governments of various political leanings within the UK, coupled with their noted existence in countries such as the USA (with policy documents such as the PATRIOT Act (Ackerman and Roberts, 2013)), Turkey (with the justification of press repression (Ellis, 2016)), and Egypt (with the statements supporting the extension of the state of emergency (Reuters, 2018)) suggest that norm securitisation is a process which enjoys international uptake due to its obvious efficacy.

Secondly, I have found evidence that the construction of threat and its reference to an object, although the necessary component for an act of security, is not a standalone entity, especially when considering how a securitising actor seeks to maximise its chances of successfully creating a platform for a shift in policy away from normal standards. A targeted deconstruction of acts of de-securitisation or counter-securitisation is a key factor in the success or failure of a securitisation act. Within this particular framework, this has been shown through the manner in which the civil liberty infringement risk of a successful securitised norm of surveillance has been directly countered through a process of explicit recognition and then minimisation of threat; the example of communications data being repeatedly referenced only to the who, when, and where, and not the contents of communications, being a key example.

Securitisation acts are repeatedly, with recurring structure and language, employed across the divide of ideologies and over an extended period of time. This shows that these acts are part of an ongoing process; one which is comparable to the development and support of a norm – in this case a securitised one. The difference is that the manner in which securitised norms are constructed appears to grant them not only greater longevity once successfully ported into public debate, but also greater resilience in the face of information which is contradictory to that used in its construction, or against specific attempts to remove or replace this securitised norm. The facilitating conditions provided by global events as ammunition for the support of a securitised norm have a great level of political capital. The revelations as to the scope and scale of the infringement of civil liberties resulting from this securitised normative basis, coupled with the removal of international institutional legitimacy with the revoking of the European Data Retention Directive, presented what appears to have been a minimal challenge to the strength of these surveillance-orientated norms. With the usage of specifically emotive language and speech acts, constructed connections to emotive referent objects such as children, and through the employment of particular contextual acts of criminality or terrorism as facilitating conditions within the UK, these norms appear to have shrugged off challenges to their legitimacy. Such resistance to what should be a serious normative challenge to its legitimacy exemplifies the manner in which securitised norms enjoy an enhanced level of resilience when compared to norms of de-securitisation, thanks to the particular manner in which they are constructed by their entrepreneurs.

Securitised norms alone have great resilience. The securitised norm of digital surveillance can be supported through the application of conditions and threats which serve to give it an even greater, and perhaps unique, ability to shrug off opposition. In a time of terrorist threats and post-fact politics, governments, both in the UK and elsewhere, are faced with a need to protect the security of their civilians against very real threats. The allure of using communications data to provide that security is undoubtedly strong. The power that such a tool provides is difficult to value; and with threats of so many kinds continually pushed before the public consciousness, the force to create a near indomitable norm of digital surveillance is within easy reach.

Chapter 5 – Cyber-war: decrypting norm development from actor decisions

Introduction: an alternative model for norm extraction

While the previous chapter of this thesis directed its attentions towards the norm development and life cycles relevant to digital surveillance, this chapter will examine a sector of cyber-security that at once offers a different series and type of main actors, and also a process of norm development at odds with the implicit constructions that were demonstrated in the previous chapter. By turning this analysis to the subject of cyber-warfare we effectively lift the framework of analysis from the domestic examination of the development of *internalised state norms* and their interaction with international institutions to the macro level of *inter-state norm development*; once again alongside the impact of or upon international institutions. Such an expansion of analysis allows for a more inclusive and complete examination of the manner in which the norms of cybersecurity develop than would have been possible through the framework of the previous chapter alone. The cyber-warfare component of this chapter necessitates the consideration of how states interact with each other, their allies, and their potential opponents; specifically in the formulation and then the acting upon of the boundaries of expected behaviour in the military application of cyber-capability. Concurrently, the traditional security component of state-on-state balances of power and potential conflict result in a manner of norm construction distinctly different from the model and motivations for it outlined through the previous chapter.

In short, digital surveillance norms centre around the juxtaposition of the ability of the state to provide better physical security balanced against the risk that the manner of providing this security itself undermines individual security in a more esoteric manner – by undermining expectations of the right to privacy. Norms surrounding cyber-warfare, however, are seated more firmly within the traditional inter-state security dynamic. The dilemma of state cyber-capability, or the lack of it, is much more reminiscent of historical instances where technological advancement has been militarised. While there have been and continue to be arguments among military scholars (Rid, 2011; Stone, 2013; Brunner and Cavelty, 2009) as to the scale to which the militarisation of cyber-space has in fact influenced military and security affairs, this chapter will, like its predecessor, target its efforts in a supplementary direction and not attempt to directly involve itself with this particular debate. Previous academic enquiries into the subject of cyber-warfare commonly first seek to construct or extract a definition of what this term means before applying this concept to the act of prediction or explanation of state action or future action. From such methodologies, pejorative statements as to the validity or lack of validity for this term are produced. It is my belief that such methodologies

begin from an incorrect position and thus produce not only unhelpful definitions, but also lines of questioning that have led to an academic quagmire out of which it is increasingly difficult for the literature to extract itself.

I will argue through this chapter that cyber-warfare and the development of international norms of control, application, and capability are occurring in a manner which is at odds with current assumptions about dominant, dialectically-driven models of norm construction (Finnemore and Sikkink, 1998). Norms of cyber-warfare between states do not develop solely through the direct application of political constructionism that have been witnessed and demonstrated in the previous chapter of this thesis and in other publications (Stevens, 2012; Finnemore, 2017; Finnemore and Sikkink, 1998); instead, the norms governing the accepted use, development, and in some cases control of cyberweapons by state actors are shaped through the direct employment of these same technologies between securitising norm entrepreneurs. This is a process of norm development that is both reflective of historical developments of military technology and currently active in international developments. The security-centric norms of cyber-warfare are built primarily through the actions of norm entrepreneurs; these actors having a greater or lesser impact upon the overall shape of these norms dependent on the success or failure to achieve the goals of this same act, as well as the international response to it. The development and nature of cyber-warfare norms are implicit; their current shape and the direction of their evolution must be decrypted from the actions of key actors within the realm of cyber-warfare. Methods or attack vectors, the nature of targets, and the reciprocal reaction to these actions by the victim state and the broader international community are not the only forces operating on the shifting international and regional norms of cyber interaction, but they are the most influential.

This chapter will not argue that the models of norm construction outlined in its predecessor, or in broader literature, are not present when examining the evolution of norms regarding cyber-warfare. The structure of this chapter will reflect that of the previous section on cyber-surveillance, notably in that it will direct its analysis at a particular case study: the Russian Federation. Reference to other states will not be entirely absent from the chapter, however. Recognising that the framework that this chapter supports suggests a level of objectivity towards the nature of international norms of cyber-warfare due to the role and influence of states as norm entrepreneurs, some attention will be paid to the manner in which the USA and other countries have operationalised their conceptions of cyber-warfare. Cyber-warfare itself is a concept that has been, and continues to be, defined and understood in a number of different, and often contradictory, ways. For the purposes of this chapter, cyber-warfare will

be taken to be any action by a state that attempts to influence the political affairs of other states or is intended to further a political goal when cyber-capability is employed to reach this goal. Such a definition leads to the inclusion of concepts such as cyber-espionage, destructive cyber-attacks, and influence campaigns targeted at nations' publics. This definition is purposefully broad and is selected as the first stage in a process of refinement. By taking a broad interpretation of the Clausewitzian definition of warfare – "a continuation of State policy by other means" (Clausewitz, 1940, p.8) – I am allowing a wide variety of inter-state activity to be considered as part of this chapter's analysis.

This will allow me to demonstrate, through a case study analysis of Russia's operationalisation of cyber-warfare over an extended period of time, not only what shape the international norms of cyber-warfare are beginning to take, but also how they have been shaped in this manner. While this chapter will directly focus its analysis and argument around the Russian Federation it will be noted throughout that other states, and thus other norm entrepreneurs, are themselves engaging in cyber-warfare, reflective of the manner in which they understand the term, and are concurrently seeking to shape the international norms regarding this subject, often with a different preferred end status, but not necessarily through different means.

Russia has been selected for this chapter's main focus for distinct, conceptual, and demonstrative reasons. The aim of this chapter is to test the hypothesis that the norms of cyber-warfare are undergoing a developmental process which diverges from the principle expected by much of academia. It will further seek to demonstrate that the cause of this divergence is the purposeful leveraging of particular weaknesses in the standard normative processes within international affairs, schisms in domestic and international political systems, and most notably the peculiarities of the technology which is central to this phenomenon.

The USA: the comparative divide of international institutional norms and national operationalised norms

Augmented power and hybridised military norms

Before engaging with the main effort of this chapter in addressing the norms of cyber-warfare through the Russian case study, there is utility in considering a state whose methods of operationalisation offer a stark contrast to those exhibited by Russia. The USA provides a useful comparative example to the methodologies and stratagems used, and the active attempts to influence the nature of cyber-warfare norms, by the Russian Federation. While the

latter state's methods and goals can be considered to be more subversive and leading towards a technological and normative means more heavily orientated towards the political element of Clausewitzian warfare, the former's actions suggest a vision of cyber-warfare which is complementary to existent military methods and goals.

The USA is a major actor both in terms of its impact on the development of norms of cyber-warfare and international standards in general, and as both the culprit and target for a number of notable attempts to employ cyber-attacks in a political manner. Extracted from the USA's actions with regards to cyber-warfare, the state's norms are best described as business as usual; the manner in which the USA has both employed and responded to cyber-attacks suggests that the direction of its policy is at least in part a result of the implicit shaping of international norms, a process which the USA has itself influenced, if unintentionally. The adoption of militarised cyber-capability by the US military does not represent a massive departure from the status quo. Instead, the ability to achieve military, and thus political, goals through the use of cyber-attacks can be seen as the continuation of a historical trend within military affairs. Civilian technologies have often been adopted by the military, employed to achieve military objectives in a manner that allows for greater chance of success, lower risk to personnel, or a combination of the two. The current military dependency on networked computer infrastructure, partnered with its inherent insecurity, means that the militarisation of the digital space is all but inevitable. Cyber-capability can be utilised in many cases as a direct replacement of methods and techniques previously achieved through other, non-digital, means. Cyber-attacks are employed to achieve goals traditionally associated with military action and even utilise similar terms to describe them, with their selection based upon the limited risk and cost of their use as opposed to those of their traditional counterparts.

The augmentation of American power abroad includes a range of cyber-attack methods with similarly varied intentions: signal disruption and misinformation parallel to ongoing military action; targeted attacks designed to cripple or undermine specific projects or critical national infrastructure; and information gathering. In its 2015 budget the USA sought to cut the Department of Defense's annual budget by $75 billion over two years, while at the same time providing a significant boost to funding to the National Security Agency and US Cyber Command. During the same year it has been estimated that the USA employed its cyber-capability against several states, and in turn was the victim of cyber-attacks from an even larger number of other states (Valeriano and Maness, 2014, p.356). It is the nature of these attacks, their scale, and the responses to them that offer us an insight into the contributions of the USA to the development of international norms of cyber-warfare, as well as their own

definition of this same term. The relevance of the USA as a case study for this norm-centric analysis is further enhanced by the nation's membership of the North Atlantic Treaty Organisation (NATO).

NATO has, over the past several years, paid distinct attention to the implications of a militarised cyber-space. NATO has been galvanised into action, both in terms of policy creation and with regards to securing its own capability within this sphere of military affairs, as a direct result of the application of this Clausewitzian concept of political power upon its member states. The large-scale, if technically simple, attacks upon Georgia in 2008 and Estonia in 2007 supplied sufficient impetus, when coupled with a concurrent trend of the research into and application of what can be called cyber-weapons by both members of NATO and other states, for the necessity of evaluating the compatibility of these capabilities with existing norms and their legal counterparts. One of the most notable products of this process, which is particularly useful in this chapter's analysis, is the Tallinn Manual (*The Tallinn Manual on the International Law Applicable to Cyber Operations*). Led by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), this document aimed to examine whether existent international law, itself the codification of international norms, was compatible with the potential military applications of a state's nascent cyber-capability.

This document and its conclusions exemplify the expected process of international norm development within relevant international institutions. The discursive process that went into the production of the Tallinn Manual's recommendations again epitomises the dialectic, discursive manner in which norm development literature describes the process of norm contestation and development. I argue, however, that this deliberative method of norm development is secondary to a more demonstrative, operational approach to the setting of normative boundaries. The two Talinn Manuals themselves act as codified evidence of what appears to be a well-ensconced normative position that the usage of cyber-weapons and concepts of cyber-warfare fall squarely within existent boundaries ascribed by international laws of armed conflict, and that the technological implications of this form of war offer insufficient grounds for the significant expansion or re-evaluation of these norms or standards. The actions of states, however, including NATO members, would suggest that not only are the ongoing re-evaluations of this conclusion stimulated by operationalised norm development, but also that this manner of norm development is having a greater impact upon the nature of these norms than the constructive processes taking place within international institutions. The US responses to apparent breaches of these norms, to which it itself should seemingly be beholden due to its NATO membership, tend to signal not only a compliance with the Talinn

Manual's findings but also a faith in the resilience of discursive norms. After instances of non-compliance with these standards, such as those of Estonia and Georgia, the USA offered limited response through condemnatory statement, responding to the breach of NATO's normative position through a purely discursive attempt at reiteration.

There are a number of differences between the Russian concept of cyber-warfare and that of the USA. The purpose of this brief consideration of the position and impact of the USA is to construct a platform from which to demonstrate that, while the vision of cyber-warfare that states might hold may be different, the manner in which the norms of this phenomenon are constructed are not. The norms of cyber-warfare could, conceptually, be separated into two categories. One is concerned with considering cyber-warfare as defined by the technology employed; that the norms of development and employment should be delineated on the basis of the nature of the weapons that might be employed as part of such a conflict. Such a categorical conceptualisation will direct normative debate down a comparative pathway that seeks to examine the impact of cyber-weapons and their similarities to existing military technologies. The second category considers cyber-warfare from the aforementioned political imperative of warfare found in Clausewitz; the norms of cyber-warfare should then not be considered from the purely technologically comparative perspective, rather it should be examined how the cyber component of cyber-warfare may be aimed at directly shaping politics. The former conceptualises cyber-warfare through its ability to influence politics indirectly, with military force as a stepping stone. The latter notes instead that cyber-warfare, due to the particular relationship between society, politics, and technology, can directly interface with politics or society, altering it in favour of the aggressor and ultimately granting a political, and thus military, victory without the traditional trappings of physical combat.

A further idea that requires explanation is the variation between the concepts of war and warfare. War, put most simply, is a state of being, one assumed by a state or states who have moved outside the realms of normal politics to utilise force to achieve their goals. Warfare is the means employed to reach these goals. Traditionally speaking, it is assumed that a state of war has a definitive beginning and an end. When one state has defeated its opponent, war ends. However, concurrent to the use of cyber-capability that will be discussed throughout this chapter, the nature of war has been changed. The definitive boundary between the state of peace and the state of war has been blurred as applications of force that function outside the boundaries of inter-state cooperation operate without temporal boundaries, and expand the targets of acts of warfare to encompass non-military audiences and to shape the politics of opposing nations from the ground up rather than the reverse. As will be seen later in this

chapter, Russia has had significant influence in this shift, while the majority of states which it has targeted have been at war without realising it.

While a non-violent, non-physical understanding of cyber-warfare may appear to be a nonsensical expansion of the concept, broadening what warfare is beyond the point of it holding qualities or features recognisable to the form with which it is generally considered, this shift is not only a relatively simple, short conceptual leap, but it is also a confluent and compatible progression of understanding when taken in context with an already expanding definition of war. The US military already engages in this more indirect form of warfare with its well-established Psychological Operations programme, simultaneously providing a supplementary example of both the expansionary nature of the evolving nature of warfare and the compatibility of non-violent applications of force towards a political goal. According to the US Army, the purpose of Psychological Operations is to "induce or reinforce foreign attitudes and behaviour favorable to U.S. national objectives. PSYOP are characteristically delivered as information for effect, used during peacetime and conflict, to inform and influence" (Department of the Army, 2005, p.1): thus, the possibility of utilising information to achieve a military goal is not one of which the USA or its allies are unaware.

The USA's vision of cyber-warfare does in fact show similarities with how PSYOP are included within the realm of non-violent military capability: as augmentative, supplementing military capability and strategy. Such an application of cyber-warfare has been repeatedly employed in numerous global conflicts, either acting as a delivery method for the PSYOP material or as a more effective replacement for military action that would previously be carried out in the physical domain. Sabotage, surveillance, and other acts of espionage, previously requiring a physical application of force or use of a human in physical space, are instead carried out through the medium of targeted hacking and the destruction or theft of digital assets. Such a usage lends credence to the argument that cyber-war as a term is an over-extended misnomer, resulting in the militarisation of concepts such as espionage, which some have argued are the remit of intelligence and law enforcement agencies and not state militaries or international military alliances (Lee and Rid, 2014, p.9).

This position is indeed compatible with the manner in which the USA engages in cyber-war. Attacks which were purely cyber in nature, such as the targeted destruction of centrifuges being used to enrich uranium in Iran in 2009 by the Stuxnet worm, or the 'Left of Launch' approach to undermining North Korean ballistic missile development, achieved military, strategic goals through methods which are discernible from historical forms of sabotage only by their digital component. Another example of cyber-warfare by the USA can be found in the

more recent and more diffuse campaign against ISIS in Iraq and Syria. In this conflict the USA has taken and employed an even more obviously augmentative application of cyber-capability. By intercepting and jamming the digital communications networks relied upon by ISIS, and through feeding misinformation back into that network, the USA has been able to maximise the physical military efficacy of its allies and aerial attacks (Sanger, 2016). Particular examples have been stated to include feeding information regarding at-risk allied convoys into ISIS communications networks, drawing out an attack at a known time and place which can then be ambushed by allied troops on the ground, or neutralised by an allied air strike.

Neither this manipulation of information, espionage of a digital age, nor the networked iteration of sabotage have caused direct, physical harm to the soldiers of opposing armies or groups. Both of these applications of cyber-warfare apply an indirect form of force on the battlefield, achieving military goals either by themselves, through non-violent application of force, or through acting as a force multiplier. This augmentative approach to cyber-warfare is further supported by the position which the USA has assumed in the discourse-directed construction of the norms regarding cyber-warfare. As a member of NATO the USA has lent its support to the entwined positions of the organisation, on the application of international law of armed conflict to issues of cyber-warfare and the potential for cyber-attacks to satisfy conditions of an armed attack contained within the mutual defence clause of the organisation (Healey, 2011).

In the later sections of this chapter, those focused upon the Russian case study that forms the central example, it will be argued that the Russian Federation has purposefully engaged in a process of norm construction that is more subversive and more active rather than discursive. It must be noted that the USA has also contributed to this implicit form of norm construction, the aforementioned Stuxnet and Left of Launch campaigns contributing to the formation and crystallisation of norms of cyber-warfare that are less restrictive and less restraint-orientated in much the same manner as Russia's probative attacks against Western targets, or its more targeted uses of cyber-attacks in Ukraine, or against the Democratic National Committee in the USA. Likewise, attacks such as the WannaCry ransomware which in 2017 struck the National Health Service in the UK, an attack that is now believed to have been carried out by the North Korean People's Republic (Bossert, 2017), have similarly served to contribute to a parallel norm construction process.

In short, norms, specifically in this instance, appear to be constructed in two parallel streams, competing against each other. These streams are made distinct from one another by the method of construction which they employ. One of these streams is the more commonly

expected, discourse-driven process of norm development explored by the likes of Martha Finnemore (2017). The other, competing process relies upon the direct action of the states or norm entrepreneurs involved. The purpose of the following, case study-specific section is to demonstrate that an increasing number of states can be seen to be employing cyber-attacks in a manner which makes them norm entrepreneurs in this implicit, action-driven steam of norm construction. However, their contributions to this process are best described as incidental. Whereas Russia has first recognised the existence of this parallel process and then sought to exploit it, the USA, Iran, China, North Korea, and Israel may have all carried out cyber-attacks, augmentative or directly violent, but the resultant input to the shaping of international norms regarding cyber-warfare is most likely accidental. While it may be that further study could demonstrate that there exists similar norm-shaping intent behind the actions of these states, the remainder of this chapter will direct its analysis to the actions of the Russian Federation in cyber-space. By examining cyber-attacks attributable to Russia from a broader perspective than has previously been considered, the remainder of this chapter will show how the subversion of the norm development process through purposeful action serves as a cornerstone of a shift in Russia's military doctrine; an intentional series of acts aimed at implicitly shaping international norms of cyber-warfare while at the same time fulfilling political goals.

Russia: making warfare political

When making any claim as to how warfare has changed, or as to how it continues to retain immutable features that can be found at any point in human history, any author is bound to draw on Clausewitz – as indeed this chapter already has. The most fundamental of this Prussian militarist's conclusions, that which has best withstood the critical debates surrounding the study of war since his death, is his conjoining of war with politics: war is "a continuation of State policy by other means" (Clausewitz, 1940, p.8). War is thus described as an intermediary stage in achieving political goals by employing military means. The aim is to use force to create a position where political goals can then be achieved, in the most classic of cases through the dictation of terms to the defeated party by the victor. Intrinsic within this relationship is the understanding that there is a distinct separation between times of peace and times of war, with war being an intermediary stage intended to result in a state that is favourable to the politics with which the victor wishes to engage.

This distinct separation is beginning to blur. Emile Simpson, in his book *War from the Ground Up* (2012), ascribes these change, at least in part, to the lack of polarity in modern conflict: warfare is not only no longer fought between two sides, but military actions must be directed

based upon their effects on a diversified array of audiences (Simpson, 2012, pp.3–4). Within the more polarised concept of war, military decisions would be taken based upon the military necessity or utility to be gained through each use of force. The physical destruction of enemy personnel, the capture of territory, the blockading of cities would all be considered on the basis of their direct effects upon the enemy and whether they would ultimately contribute to the enemy's defeat, and thus the political opportunity to dictate terms and shape politics in that region to the victor's liking. Modern examples of this form of conflict are, however, hard to locate. Simpson singles out the military campaign to destroy the Tamil Tigers in Sri Lanka in 2006–07 (Simpson, 2012, p.1). What has taken their place are conflicts in which war is no longer an intermediary stage, but where combat itself has become political.

In Afghanistan, Simpson argues, combat activities and their aims must be measured by their impact upon a number of different audiences, many of these being contradictory. The globalisation of conflict has led to a diversification of actors involved in war, which in turn has meant that the conditions of victory and the end of war have also become more diffuse. Simpson, through the lens provided by the military campaign in Afghanistan, explains how the end of polar conflicts has resulted in combat itself now being employed as a form of, and thus shaped by, politics:

One can apply military pressure against the enemy in the Taliban, and more broadly to the insurgency. However, the defeat of insurgents in the military sense may assist in, but does not translate into, victory for the coalition because the interpretation of the conflict in terms of military metrics may well be a frame of reference to which most audiences do not ascribe. (Simpson, 2012, p.3)

Simpson continues to use the Afghan counter-insurgency, NATO, the UK, and other allied states for his examples of how military affairs have resulted in the application of military resources in a manner seeking to satisfy audiences often far removed from the physical region in which they are engaged. His observations are even more relevant when considered against the manner in which Russia has embodied this shift – most notably in the manner that it has employed the potential of cyber-operations.

Recent examples of Russian military intervention, that being the traditional conception of the term involving the deployment of military personnel, include a brief war in Georgia in 2008, the annexation of the Crimea and resultant civil conflict in 2014, and the intervention in the Syrian civil war from 2015 until the present. Each of these conflicts involved the same overlapping non-polar audiences that are the reason for the shifting of combat into direct

political action, according to Simpson (2012, pp.1–3). In each instance one of these audiences was the international community at large, another was the Russian public. Each of these also included a regional audience: Middle Eastern states with the Syrian intervention; European with Georgia and Ukraine. Even these can be considered at a more granular level, however. Different states within the Middle East could be considered as separate audiences, likely to react differently depending on the military actions of Russia within Syria. With the Georgian and European example, audiences could be further subdivided into overlapping regional alliances: NATO; the European Union; the Baltic Nations.

It is the consideration given to another type of audience, coupled with the opportunity to shape the politics of this group, presented by networked information systems that makes Russia's approach to this political combat unique – and also the focus of this chapter. The following case study will demonstrate that Russia has actively and purposefully engaged in a subversive shaping of the norms of cyber-warfare, distinguishing the state from its international peers in the process. The motivation for this engagement has been the desire to maximise the efficacy of its politicised combat against the most diverse, largest, and potentially most varied audience possible – the international public. By including this particular audience within Russia's consideration of its international goals, the divide between peace and war is further muddied. Low-level cyber-attacks intended to steal information, then tactically employed as part of misinformation campaigns directed against key individuals or institutions, coupled with complex attacks interrupting or damaging critical national infrastructure, all allow Russia to directly influence the politics of the audience within whichever region or state they wish. The destabilising effects of the messages of incompetency, corruption, and insecurity that this combined method of combat brings to bear allow for the inclusion of an even wider series of international affairs into the remit of this case study. If war is no longer a means of reaching the conditions where politics can resume its usual form, if instead acts of warfare are themselves political, and the object of this political war is the satisfaction of a specific populous, then, on reflection, any action seeking to influence or satisfy this audience is itself an act of combat. This means that the cyber-attack against Estonian networked infrastructure at the hands of so-called "patriotically minded" (Higgins, 2017) hackers now attributed to a group affiliated with the Russian state (Geers, 2009), the attempts to influence the American Presidential elections of 2016 (FireEye, 2017), similar efforts targeted at the French Presidential election of 2017 (Borger, 2017), and towards the Brexit referendum (Booth et al., 2017) in 2016, can all be considered as instances of a cyber-war.

Cyber-warfare in this format can be considered a marriage of necessity, with the same effects of diversifying opponents and global conflicts impacting Russia as have NATO and its allies, and potential opportunity. The force-multiplying capability of cyber-warfare has already been considered in this chapter with regards to the USA's augmentative approach to its capability. However, by directing attacks at an opponent's population, the impact of these attacks relative to their cost can be dramatically increased. A further motivation is that the norms governing this particular vector of attack are, as yet, ill-defined, non-existent, or weak. This status is further complicated by the manner in which the norms relating to some routes through which a state might engage with international publics mostly relate to privately owned Internet Service Providers. What Russia has achieved is to recognise the direction in which warfare is changing, further noting the opportunity to maximise the power that can be leveraged through the confluence of our technological dependence, the potential for norm construction through direct action, and the loopholes already present within existing norms.

Background noise: espionage in plain view

Valeriano and Maness described the majority of cyber-operations as typically "probes and faints to harass an enemy and demonstrate capability" (2015, p.355). Such operations can be described as what I term low-level cyber-attacks. These are attacks which, taken on their own, are unlikely to result in drastic economic, political, social, or military change upon their target. Low-level cyber-attacks can be technically complex, such as the compromising of secure databases and the theft of personal information, or they can be relatively simple: a direct denial of service attack being a prime example. The measure of the term low-level is dependent upon its effect. Preferably, it would be defined based upon the intent of the instigator, but due to the nature of inter-state cyber-operations, the extraction of concrete information as to the intent of the perpetrator is extremely difficult.

The term low-level is purposefully juxtaposed with my conclusions as to the potential impact of this form of attack. The normalisation of low-level cyber-attacks between states, resulting not only from their numeric growth over time, but also from the apathetic reactions to them by both the victim state and the international community at large, has amplified the danger they pose. Low-level cyber-attacks have been transformed by the process of operationalised norm development to become a far greater threat. Both action and inaction by norm entrepreneurs in low-level cyber-attacks between states has led to the development of an international norm of cyber-security that accepts these attacks as a by-product of an international communications network; they have become white noise. To demonstrate this,

we only need consider the scale of attacks between states, their timing, and the responses to them. China, the source of a large number of cyber-espionage incidents directed at the USA and the UK (Grierson, 2017), has been repeatedly reprimanded by both of these victim states (Hope, 2013). Such reprimands, however, have proven largely ineffective (Alperovitch, 2015) and have failed to be repeated or reinforced.

Valeriano and Maness have provided the opportunity to begin to extrapolate both the how and the why of norm development with regards to low-level cyber-attacks. Further contextual examination also allows for the demonstration of the potential dangers that this process poses. As the basis for a number of follow up studies regarding the nature and impact of what they term cyber incidents upon international relations, Valeriano and Maness begin by constructing a dataset of inter-state incidents of varying classifications of severity (Valeriano and Maness, 2015, p.5). In total they extrapolate 110 cyber incidents occurring between 2001 and 2011, with the USA and China contributing the largest number of attacks; the latter usually initiating the attack and the former most often the target (ibid.). In analysing this dataset, the authors conclude that while it is undeniable that cyber incidents between states were occurring during this period, states demonstrated restraint both in terms of number of attacks initiated and in the severity of these attacks. While the authors recognise the potential danger of unopposed cyber incidents between state actors, even those limited in target or scope, with regards to the potential shaping of international norms (Valeriano and Maness, 2014, p.357), they fail to develop this point any further. Their study instead acts as a foil to the increasingly vociferous discourse in news media, political statement, and academia that paints images of a "cyber Pearl Harbour" (Stavridis, 2017) or "chaos in our streets at home due to sudden crashes in our critical infrastructure" (Patterson, 2010).

However, there is, in the manner of classification of the term 'cyber incident', an academic version of minimalisation that mirrors the same normative process that is ongoing with low-level cyber-attacks between states. In their original 2010 paper Valeriano and Maness describe how they employ the term cyber incident to act as the collective term for individual incidents of an attack utilising the same technical attack vector against the same target.

> For individual cyber conflicts, we use the phrase 'cyber incident'. Incidents such as Shady Rat include thousands of intrusions, but accounting for every individual intrusion the operation made is impossible and unwieldy. Therefore Shady Rat and other multiple-intrusive incidents are coded as just one incident per dyad as long as the goals and perpetrators remain stable. (Valeriano and Maness, 2014, p.352)

This approach does offer methodological clarity, and the ability to analyse masses of data in a manner that would simply be unachievable if each intrusion were itself treated as a cyber incident. It also results in the skirting of a numeric and subsequently normative trend within these same individual intrusions. The academic utility gained by this act of categorisation simultaneously undermines the model's ability to be reflective of the reality of how these same intrusions are interpreted by both the victims and their perpetrators.

Since 2011 the reliance of states on cyber operations of all levels to achieve their international policy goals has notably increased. Even employing the amalgamative definition of cyber incident utilised by Valeriano and Maness, the 2017 Symantec Internet Security Threat Report suggests that in 2016 alone the number of cyber incidents between states has shown a marked increase on what is reflected in Valeriano and Maness's dataset (which concluded in 2011). In 2016 there were at least 10 notable state-affiliated cyber-espionage groups that were active in carrying out state-targeted cyber operations, and they originated in at least five distinct countries (Symantec, 2017b, p.17). Notable attacks and incidents include the theft of email records from the Democratic National Committee during the US Presidential election campaign of 2016, attacks directed at power plants in Ukraine, and the theft and subsequent leaking of internal documents from the World Anti-Doping Agency (Symantec, 2017b, p.16).

Low-level cyber-attacks, including individual attacks that would only be counted as a component of a cyber incident, have meanwhile shown a high rate of growth over the last couple of years; a trend which appears to be increasing exponentially as more actors – state and otherwise – seek to employ digital means of achieving political or criminal ends within an increasingly digitally-dependent economic, social, and political landscape. According to a RAND Corporation report offered as testimony to the USA's Homeland Security Committee on Cybersecurity, Infrastructure Protection, and Security Technologies, "in 2014, more than a billion personal data records were compromised by cyberattacks – a 78 percent 'surge' in the number of personal data records compromised compared with 2013" (Porche, 2016, p.4).

It is within this trend of high-volume, regular, and low-level attacks that Russia has acted to fulfil two symbiotic goals. One of these works towards achieving a direct state of victory or dominance over opposing nations and entities, the other serves to shape the normative position that allows these methods of attack to continue with minimal punitive response and to maximum effect. The securing of both of these goals is concurrently achieved. By carrying out low-level cyber-attacks Russia simultaneously probes its opponent's digital defences and, when successful, may gather intelligence upon an individual, group, institution, or state that serves as one of several kinds of ammunition within the information warfare stage of their

hybridised and politicised form of modern warfare. At the same time, the cyber-attacks that achieve these goals contribute to the shape of international norms of cyber-warfare between states.

The campaign to interfere in the 2016 US Presidential election provides an all but complete picture of both the direct results-driven goals, and of the role in the shaping of international norms that Russia's emergent strategic position has resulted in. It provides evidence that outlines a multi-staged strategy, that employs a combination of low-level cyber-attacks against political organisations, institutions, and individuals, which provides the ammunition for a campaign of information warfare carried out through social media.

On 10 March 2016, 30 phishing emails designed to appear to be from Google were sent to various email addresses owned by staff members at the Democratic National Committee, all of whom had previously worked on Hillary Clinton's last attempt at winning the Democrat party nomination for President (Satter, 2017). In this same year, Kaspersky Labs recorded 154,957,897 instances of its anti-phishing system being triggered by its users (Kaspersky Labs, 2017a). This statistic is mirrored, however, by reports from McAfee that suggest that in the fourth quarter of 2015 the number of new phishing URLs, such as faked password reset pages similar to those included in the emails sent to the DNC, was in the region of 1.4 million (McAfee Labs, 2017). Despite Kaspersky software being banned from all US governmental computers (Solon, 2017a) as a result of being a potential vector of cyber-attack in its own right due to close ties with Russian government, the numbers remain demonstrative. The initial 30 emails, only one of which led to a successful infiltration of the DNC network, were quickly followed by a further 130 phishing emails. Amongst the total 154 million triggers of the anti-phishing system, these 160 attempted acts of cyber-espionage are easily lost. Kaspersky further ascribed 2.71 per cent of the total 46,557,343 recorded triggers of its anti-phishing software in Q2 of 2017 to networks owned by government institutions (Kaspersky Labs, 2017b). This equates to a smokescreen for Russian efforts to undermine the political and social cohesion of the USA and other states through 1,262,245 phishing attacks targeting government entities running Kaspersky software during 2017.

The vulnerability created by the status quo generated by allowing the white noise of low-level inter-state cyber-attacks to continue without direct counter had thus been exploited in order to gain access to the sensitive information of a foreign political organisation. It took several more rounds of phishing emails, working with addresses at the DNC and registered to hillaryclinton.com – all of which had been gleaned from the initial access – before attention was turned to personal Gmail accounts. On 19 March 2016 a phishing link was generated and

sent to John Podesta, then Chairman of Hillary Clinton's Presidential campaign, which was then clicked on at least twice, thus giving the attackers access to Podesta's emails, his calendar, and his contacts (Satter, 2017).

In effect, failing to act to curb the propagation of low-level cyber-attacks such as those which granted this access is as much an act of norm construction as actively engaging in these acts. Russian subversion of this process builds upon the recognition of the resilience of norms constructed through action and the subsequent lack of response to that action. Such a conceptualisation of these norms is evidenced through the growth of low-level cyber-attacks between states, in raw figures as well as in the number of actors engaging in them. As each state engages in this kind of non-physical application of force and is met with limited, or no, punitive response, the status quo, the norm that allowed this action, is only further entrenched.

Responses to this form of cyber-driven espionage do exist. They do, however, consist in the most part of targeted discourse from states that have been affected by Russian or other state attributed cyber-attacks. In 2015, as part of a series of visits to countries including the UK and the USA, the Chinese President Xi Jinping signed an agreement with both the British Prime Minister David Cameron and the US President Barack Obama to cease cyber-espionage attacks against either state (Mason, 2015). While not a punitive response, this agreement is evidence of an attempt at shaping the norms governing the usage of cyber-capability to steal from or influence rival states. Further evidence can be found in an Executive Order issued by the Obama administration in early 2015. Executive Order 13694 effectively establishes that cyber-attacks upon the USA and its businesses that are of a sufficient order of magnitude will be punished through the application of economic sanctions against the perpetrators and beneficiaries (Executive Order 13694, 2015). Neither this signalled threat of punitive measures, nor the conciliatory, discursive approach to shaping these norms appears to have had the desired overall effect: one day after the signing of the agreement with the USA, on 26 September 2015, Crowdstrike, a cyber-security business that serves both government and private sector interests in the USA, reported in a blog post authored by one of its founders, Dmitri Alperovich, that it had detected a resumption of cyber-attacks attributable to the Chinese state (Alperovitch, 2015).

Similar dissuasive actions have, more recently, been directed at Russia from the UK. After internal investigations by the social media platforms Twitter and Facebook revealed the potential for Russian interference in the country's referendum on exiting the European Union (Booth et al., 2017), the British Prime Minister, Theresa May, openly accused Russia of being

behind attempts to undermine the democratic processes of other countries and the rules-based system upon which international cooperation is based:

…we meet here at a moment when the international order as we know it – the rules based system that the United Kingdom helped pioneer in the aftermath of the Second World War – is in danger of being eroded.

A moment when some states are actively destabilising the world order to their own ends, claiming that the rules and standards we have built, and the values on which they rest, no longer apply. (May, 2017)

These remarks were then later reported to be followed up during a visit to Moscow by the British Foreign Secretary, Boris Johnson, who raised these same accusations with his counterpart Sergey Lavrov, and warned that Britain's own cyber-capability could be employed as a more direct punitive measure (Woodcock, 2017). These two instances of political rhetoric were coupled with the announcement by GCHQ, the British agency responsible for cyber-intelligence and security, a few days prior to Johnson's visit to Moscow, that they had developed an offensive cyber-capability capable of crippling a target state (Intelligence and Security Committee, 2017). These instances all contribute to a position of deterrence which in turn can be construed as an attempt to construct a normative position that might act as a restraint on future Russian action. The report updating Parliament as to the UK's cyber-capability contains specific reference to the laxity of international standards of behaviour regarding the utilisation of cyber-capability against other states, despite there being a stated consensus as to the applicability of the laws of international armed conflict to the emergent digital domain.

The practice and precedents of how cyber activity ought to be classified under existing international legal principles and concepts [are] underdeveloped. As a result, the application and analysis of existing legal norms to the analysis of cyber activity can vary considerably. (Intelligence and Security Committee, 2017)

As the later sections of this chapter will discuss, attempts through rhetorical or indirect means may be too little, and come too late, to rein in the development of these norms to a position that firmly orientates them within these existing international legal principles.

These reprimands, the responses to Russian-attributed low-level cyber-attacks and campaigns of misinformation, are effectively limited in two regards. Firstly, they are insufficiently punitive to make the repeat of these acts too costly given their benefit, and secondly, they are reactive. The democratic destabilisation that Theresa May noted in her 2017 speech has already been

achieved and is now being almost self-maintained. The Podesta emails, all 50,000 of them (Satter, 2017), provided the ammunition for a campaign of information warfare that was, and is, the continuation of a wider campaign that began several years previously. The information gathered through this phishing attack, in the form of Podesta's emails and other sensitive information held by the Clinton campaign, was then leveraged to inform the strategy of and supply a grain of truth to a prolonged engagement in cyber-space for the collective consciousness of the American people right in the midst of a Presidential election. The success of this intelligence/ammunition-gathering stage only reinforced the potential for these methods to be employed again, and against more targets. Success at this preliminary, supportive stage, coupled with an ineffective or non-existent short-term response to the low-level cyber-attacks employed, resulted in a solidification of the operationalised norms dictating inter-state cyber-attacks. The lack of punitive response suggests to other parties that this is an action that is acceptable, below a threshold that requires chastisement, and the success of the attack encourages a repetition of this method in future.

The successful provision of ammunition for a campaign of information warfare through phishing, achieved through the active subversion of this weak set of international norms, has led to the use of this method of attack being repeated against further targets. Each of these targets share similar traits: the UK, Germany, Denmark, France, the Czech Republic, and Spain have all been subject to attempts to undermine their domestic political processes through similar means (Booth et al., 2017; Rankin, 2017; Boffey and Rankin, 2017; Tait, 2017).

The case of Germany, in fact, predates the Podesta breach, suggesting that Russia has perhaps achieved earlier successes through this method of attack which have further encouraged the continued expansion of this form of warfare, and concurrently provided greater legitimacy to its preferred cyber-norms through this operationalised method of construction. In March 2015 the German Bundestag was infiltrated by a group called Fancy Bear. Once again through a phishing email, this time appearing to be from the UN, access was gained to the Bundestag's network, simultaneously culminating in and revealing itself by closing down all computers connected to this network (Delcker, 2017).

Delcker (2017) reports fears held by German lawmakers' cyber-security advisers and politicians that this hack may have provided the ammunition to Russia to undermine German elections two years later. He also draws attention to a further reason why this method of attack was and continues to potentially be successful. One member of Parliament, when asked whether he and his staff had paid greater attention to cyber-security following the 2015 hack, was reported in this article as stating "I couldn't give a shit" (Delcker, 2017).

These attitudes, and the implications to security that arise from them, are more prominent than might be expected, and certainly more than would be hoped for. A Chatham House study into the perspectives on cyber-security in business discovered that issues of cyber-security were generally considered below the board room level (Cornish et al., 2011), with the dominant position being that these were issues best covered by a business's IT department, not warranting the attention requisite with board level oversight. Such a position of wilful ignorance only heightens the potential success, and thus likelihood of repetition, of these tactics.

Indeed, during the French Presidential elections in 2017 the campaign of then candidate Emmanuel Macron suffered first a theft of information from their campaign's network, followed by a release of this information *en masse* to the public on 5 May through the anonymous link-sharing website PasteBin. In a statement reported in *Wired* explaining what had occurred, Macron's party, En Marche!, stated the following:

The En Marche! party has been the victim of a massive, coordinated act of hacking, in which diverse internal information (mails, documents, accounting, contracts) have been broadcast this evening on social networks. This files which are circulating were obtained a few weeks ago thanks to the hacking of professional and personal email accounts of several members of the campaign. (Greenberg, 2017b)

The *modus operandi* was identical to that found in the Podesta and Bundestag hacks. The major difference in this instance was the much-compressed timescale. While these two incidents saw the ammunition gathered by each hack turned upon a related political campaign either a year later, as with Podesta, or two years later, as with the Bundestag, the information stolen from En Marche! was leaked less than two weeks after the hack which supplied it. This variance lends further credence to these hacks being evidence of the politicisation of combat which has reshaped Russian strategy.

The audience to which this act of political combat was addressed was clearly the French voting public. The aim once again was the destabilisation of the domestic politics of a rival foreign power, with the centre-left campaign being the target. This suggested that the preferred outcome in this instance was either the success of the right wing National Front headed by Marine le Pen, or a state of increased discord within French politics and society. The short time-frame of this particular operation suggests one of two explanations which potentially provided equal contribution to the timing: firstly, that the data security practices of En Marche! prevented the successful theft of data at an earlier time and so left a limited window

of opportunity for the data to be employed against Macron's campaign; or, secondly, that the release of information was left until two days before the election itself in order to limit the potential for a counter-narrative to be employed by En Marche! in response.

The latter of these two explanations gains further credibility due to the particulars of the French Presidential campaign. For the duration of the two days prior to the election itself, French Presidential candidates are barred from speaking publicly. Together, these explanations suggest that Russia was without the ammunition required to fulfil its goals until a point relatively late in its campaign of information warfare against France. When that ammunition was finally provided, the window left in which it could be employed was far smaller than in previous examples of this method of attack. In order to maximise its impact, given the limited time available, further departure from previous iterations of these campaigns was required. Rather than a prolonged campaign of misinformation through diffuse vectors and across public-facing media outlets, all of the data stolen from the En Marche! campaign would be released at once, at a time chosen to both maximise its impact and minimise the target group's ability to defend against the attack.

A further insight to be gained from the French example of this form of cyber-warfare is that, partially as a result of this rushed timescale, this attack did not result in the same success as previous iterations. It thus serves as an exemplar of how this operationalised method of norm construction through political combative acts in cyber-space can potentially be challenged by circumstance or specific responses. In response to the leak of these stolen documents, the French Electoral Commission ordered French media not to publish any of the document's contents (Dearden, 2017). With the breach of this order constituting a criminal offence, this served as an effective restraint upon French media companies. The Russian form of information warfare employs the ammunition derived from its targeted low-level cyber-attacks in a particular manner; it utilises the manner in which publics – their audience – in developed countries receive their news from increasingly diverse sources, most notably social media. This vector once again exploits a weakness in another form of international norms, those norms embodied and held by international internet services and their policies. Social media platforms such as Facebook, Twitter, and Instagram, as well as groups such as Wikileaks, provided a route to circumvent previously domestically controlled sources of information to engage directly with a state's political and social cohesion.

Nature and nurture: leveraging inherent insecurity and reliance on networked information

In a post in January 2018, Facebook product manager Samidh Chakrabarti stated that social media "At its best, allows us to express ourselves and take action. At its worst, it allows people

to spread misinformation and corrode democracy" (Chakrabarti, 2018). Facebook and some other social media networks and online services, especially those which have diversified into providing a medium for the sharing of stories and news in more diffuse forms, occupy a position where their success in supplanting more traditional news sources and in reaching such a high level of saturation of userbase has also made them a near perfect tool for a purposeful campaign of information warfare: their success is also the source of their insecurity.

If the information stolen by Russian-affiliated groups such as Fancy Bear, implicated in the Podesta phishing attack (Satter, 2017; McAfee Labs, 2017), the theft of data from En Marche! (Greenberg, 2017b; Trend Micro, 2017), and the Bundestag attacks in 2015 and 2016 (Delcker, 2017; Trend Micro, 2016, 2017) is the ammunition for a Russian campaign of information warfare, it is best described as the explosive component of a missile: social media is the delivery system.

Such a weaponisation of social media (May, 2017) arises out of a confluence of two forms of inherent weakness: technological and normative. The technological can be further divided into two particular issues: those arising from the level of anonymity that can be provided by social media (a trait shared with attacks taking place within the cyber domain in general); and those arising from the level of dependence on social media and networked technology which has become characteristic of developed Western nations. The normative weakness in this instance arises out of the privatised nature of these tools of social interaction. The norms that moderate the use of platforms owned by Facebook, Google, Twitter, and others are grounded upon the fundamental principles of these organisations. Examination suggests that, alongside the business-orientated norm of actions and policy being driven by maximisation of profit, this impetus is further shaped by the imposition of a norm shared by many internet-based companies: the primacy of free access to information, globalisation, and resisting censorship. These values are revealed and also challenged in the interaction of these companies with the legislative effects of norms constructed and enacted by states within whose borders they operate or international institutions whose area of governance they fall under. This can be seen in Google's fraught process of compliance with the European Union's 'right to be forgotten' (Hern, 2015), the ongoing disagreement between Facebook and Germany over the use of legal names on their platform (Toor, 2015; Reuters, 2016; Lomas, 2015), and the pressure that the government of the UK has been applying to Twitter about the policing of threatening or abusive content on its platform (Ruddick, 2017; Cox, 2017). What these platforms have previously failed to consider within their internal construction of norms and standards is what, if any, control they should exert over the content their users (businesses or

individuals) post with regards to the manner in which such rules might expose or even create a digitally dependent Achilles' heel for the democratic process.

Proxy war by proxy: plausible deniability 2.0

Both the means of acquiring the ammunition for Russian campaigns of information warfare and this form of politicised combat rely upon the ability to plausibly deny any accusations of responsibility for these attacks or their outcomes. In a parallel to the concept of norm securitisation examined in the previous chapter, deniability in this instance is not required to be broadly employed. The target audience of Russia's misinformation warfare is the publics of whichever state each campaign is seeking to destabilise. The ammunition-gathering stage, the method of delivery, and the information fed into the political discourse through this mediatised method has to be separable from attribution to Russia only to the degree that the intended audience is fooled. Furthermore, it only must retain this level of deniability for a limited space of time. This further incentivises this method of exercising power upon opposing states. States acting through proxies when interfering in the interests (foreign or domestic) of opposing states that may be too powerful to confront directly (thus risking retaliation) is something of a tradition between the USA and Russia. The Cold War provides numerous examples of such circuitous and diversionary relationships between state actors and their client states, or often non-state pawns. The USA's relationship with groups such as the Mujahideen in Afghanistan and Pakistan and Russia's with Fidel Castro's Cuba are now being reconstructed in a digital form.

The 2016 US Presidential election provides a perfect example of how the nature of networked communications, social media, and our use of the latter provide an opportunity for a state – such as Russia – to gather ammunition for and then to carry out a campaign of information warfare, maintaining the level of separation at each stage necessary to create the conditions for success. Further, the resurgence of proxy warfare, with social media platforms and other networked services taking the role of proxy states or non-state actors, shows that the norms that Russia's actions have been continuing to shape have not come into existence without any previous basis. They are instead the synthesis of historic norms and the capability shift that has arisen out of networked communications. Those historic norms similarly evolved through operational acts of construction rather than discursive ones, and were necessitated by a period of history where this same dyad – the USA and Russia – were in distinct opposition, but due to each other's nuclear potential were unable to directly realise their conflict. The historical norms of the Cold War and the various proxy wars are in the process of rejuvenation and evolution. While the proxy wars of the Cold War were still traditionally Clausewitzian – seeking

to militarily impose the conditions from which a political process could begin – the modern iteration has been significantly influenced by the technological opportunity presented by social media platforms and internet-enabled diffusion of information. In the previous century, conflict between the USA and Russia was separated by an opaque level of disconnection between the sponsoring states and the actions of their vassal states or actors. Now, though, the necessity for plausible deniability and the level to which it can be achieved through technological means has resulted in a degree of separation that sees the proxies being entirely unaware of their status as such.

There are three stages of comparison that will allow for the exposition of this evolution: firstly, we can consider the motivation for plausible deniability and the manner in which it was constructed and then applied during the Cold War; secondly, the manner in which Russia employed criminal hacking groups in Estonia and Georgia in 2007 and 2008 respectively; and thirdly, how Facebook, Twitter, and Wikileaks were used to co-opt existing socio-political division and specific movements to undermine the US Presidential election in 2016.

To expose the nature and motivation of plausible deniability and the norms of proxy warfare in its traditional, Cold War-era iteration, the counter-revolutionary efforts directed at Fidel Castro's Cuba serve as an effective example. The 1961 Bay of Pigs invasion of Cuba by Brigade 2506, a military wing of the Democratic Revolutionary Front (DRF), was funded, planned, and directed by the CIA. This Clausewitzian military endeavour sought to use force to achieve a status where the political aims of the USA could be realised – the removal of a Communist, client state within the USA's geographical area of influence. It achieved this through indirect means, however, utilising the DRF and Brigade 2506 as its proxy, with Cuba under Castro fulfilling the same role for the USSR. This instance exemplifies the manner in which both sides employed proxies to conduct military campaigns against each other's interests. The plausible deniability of these cases may appear minimal in hindsight, but they were sufficient for the purposes of avoiding direct confrontation between the two superpowers. In the current century, evidence of a shift to a more distinct level of separation between Russia and its proxies, concurrent with and as the result of technological dependency and the insecurity of that same technology, can be found within the rise of the so-called 'patriotic hacker'.

In April 2007 the Estonian government announced that it would be moving a Soviet-era statue out of the centre of the city of Talinn. Russian-language media outlets within Russia and Estonia protested the decision, culminating in two nights of rioting in Talinn on 26 and 27 April. Also on 27 April, Estonia was targeted by a large scale Distributed Denial of Service (DDoS) against its networked infrastructure. This resulted in Estonian banks, government services and

websites, and news services being unreachable. Cash machines failed, intra-governmental communications were unreliable, and news broadcasters had their connections with their viewers effectively severed. These attacks came in three distinct waves. After the first attack, a second spike in the severity of the attack came on 3 May, with the largest spike beginning on 9 May and dramatically dropping off almost exactly 24 hours later. The final of these three is most notable, and the reason why the then Estonian President, Toomas Hendrik Ilves, has stated that this "was the first, but hardly the last, case in which a kind of cyber-attack … was done in an overtly political manner" (Ilves cited in Tamkin, 2017). On 9 May Russia celebrates its Second World War victory in Europe. When questioned by the *Guardian* as to the suggestive timing, and about Russian-language instructions as to the means and timing of these attacks being circulated online prior to their start (Davis, 2007), the then Russian ambassador in Brussels, Vladimir Chizhov, had the following response: "If you're implying that [the attacks] came from Russia or the Russian government it's a serious allegation that has to be substantiated. Cyber-space is everywhere" (Traynor, 2007). While this attack was powered in part by massive botnets – networks of computers infected with malware that made them and their owners the unknowing co-conspirators in this politically motivated cyber-attack – the individuals who knowingly took part were actively making themselves the proxies of Russian state interest. This plausible deniability was a step beyond that of its predecessors. While the ownership of the large botnets could be traced to Russian criminal organisations, and the individual actors that joined in were able to do so due to Russian-language instructions, the level of separation between the sponsor and its vassal was greater than in previous conflicts. The attack could have real impact due to modern reliance on networked computing. This was a digitally-enabled proxy war where Russia had leveraged the popular opinion of its Russian-speaking diaspora, making its citizens proxy digital soldiers in its conflict with its Estonian rival.

The final example, which provides the most perfect concealment for the intervention in a rival state's internal affairs, is one which progresses the conscription of a state's own citizenry as proxy digital warriors in information warfare to its next logical stage: making the rival state's citizenry the proxies in the war against them. The manner in which Russia interfered in the political and social discourse surrounding the US Presidential election of 2016 provides an example of the necessary levels of obfuscation that have been achieved to allow for such a strategy to be successful. There are in effect two kinds of proxies involved in this instance. The first are the social media platforms that have been employed as the delivery method, connecting the Russian state to the American population in a manner that, to this population, is sufficiently opaque as to be unnoticed. This first set of proxies allows for the manipulation of

information delivered into the political and social discourse of the second (this being the American public).

Facebook provides a particularly good case study of this process in action. The manner in which this social media platform was employed by the Russia-based Internet Research Agency (IRA) and other Russian agencies demonstrates the process from the ammunition-gathering stage through to the effective recruitment of the American publics to physically manifest political and social divisions, thus undermining the stability of American political structures and most notably the democratic processes represented by the 2016 Presidential elections. According to Facebook, around 10 million people in the USA viewed adverts that had been sponsored by either the IRA or another Russian-led entity, and 44 per cent of these views took place before the election on 8 November (Schrage, 2017). This means that prior to the election itself roughly 4.4 million Americans were exposed to political adverts sponsored by another state, adverts which, by their nature, will have been targeted to a specific demographic audience based upon particular interests. These tools, designed and usually applied to ensure that marketing campaigns reach the audience most likely to be encouraged to purchase or engage with the advertised product or campaign, grant further granularity to the delivery of this form of cyber-warfare. Much as when selecting which weapon system to use in kinetic warfare, especially when driven by the principles of proportionality, distinction, and discrimination of the laws of armed conflict, this allows for information warfare campaigns to more precisely target the audiences suitable to the nature of the campaign in question. To maximise the effect the right form of information, or misinformation, must reach the audience most likely to react in the preferred way.

The potential impact of this marketing-strategy-meets-information-warfare approach was further amplified after the initial figures of 100 million were further revised in a written statement from Facebook delivered to the US Senate Judiciary Subcommittee on Crime and Terrorism. It stated that when taking into account how these adverts were then further disseminated by its users as they shared them among friends, the likely number of Americans who saw, if not fully engaged with, these adverts was better estimated at 126 million (Byers, 2017). According to the Pew Research Centre, 137.5 million Americans voted in the 2016 Presidential election (Krogstad and Lopez, 2017), which represents 61.4 per cent of the total voting population of 223.9 million. This means that, in a worst-case scenario, 56.2 per cent of the total number of adults that could vote were exposed to political messages formulated and designed by a foreign power. Obviously this percentage fails to take into account the percentage uptake of Facebook as a platform by that same total voting base, as well as the fact

that only the aforementioned 61.4 per cent of those actually voted, and that the level of exposure to these adverts is not expressed within these figures. It does, however, demonstrate the potential power inherent in this method of information warfare. With considered employment of the ammunition gathered during earlier phishing campaigns, and effective usage of marketing tools, it would potentially be possible to conscript a large proportion of that total voting population. At its most effective level such a stratagem could allow for Russia, or any other state, to drive a wedge through existent socio-political divides by tailoring the content and targeting of these adverts to reach and find fertile ground with both sides of these prevalent debates.

Facebook again, in this leaked written statement to the Senate Subcommittee, noted that these adverts were "seemingly intended to amplify societal divisions and pit groups of people against each other" (Byers, 2017), further commenting that "most of these ads appear to focus on divisive social and political messages across the political spectrum, touching on topics from LGBT matters to race issues to immigration to gun rights" (Byers, 2017). The divisive intention of these adverts, and through them the wider campaign of information warfare directed against the USA by Russia, is perfectly illustrated in events that took place in Houston, Texas on 21 May 2016. Two groups of demonstrators – one staging a 'Stop Islamization of Texas' demonstration organised through the Facebook page 'Heart of Texas', and one staging a 'Save Islamic Knowledge' demonstration organised through the 'United Muslims of America' page – turned out in response to the opening of a new library at a local Islamic Centre. Besides taking place at the same time, these events had something else in common. They were both organised based upon Russian adverts, and both the Facebook groups in question were managed by the Russian 'troll factory' the Internet Research Agency (O'Sullivan, 2018).

The protestors on both sides of this physical dispute were seconded through the careful and purposeful exploitation of underlying social divisions within American society and politics. Recruiting these individuals directly would certainly prove ineffective, the ideology of these and other divided segments of American society would make the concept of acting on behalf of another state to destabilise America anathema, rendering the tactic instantly ineffective. The opportunity presented by social media platforms, in this instance Facebook, is to present a layer of abstraction – a curtain that conceals the state-serving interests behind the actions or protest suggested by using a proxy (Facebook). In this example, Facebook is being employed as a proxy recruiter to conscript American citizens to embark upon a destabilising campaign of political action, online and in the real world, directed at groups with which they already feel at

odds. While, at the same time, those groups are likewise being recruited to carry out a parallel campaign directed against their aggressors.

It is useful to note, outside of this American case study, that the employment of social media to galvanise a socio-politically destabilising response by Russia against other states is not limited either to the USA or to Facebook. At the height of the Brexit debate in the UK, when social tension along ethnic and political lines was already aggravated, a tweet made from an account later linked to the Internet Research Agency made a significant contribution to the social discourse and an impact on public consciousness. The tweet was posted on 22 March 2017, in the aftermath of a terrorist attack in London in which a car was purposefully driven into pedestrians on London Bridge. It included an image of a woman in hijab walking past where one victim was on the ground and was captioned:

> Texas Lone Star (@SouthLoneStar)
> Muslim woman pays no mind to the terror attack, casually walks by a dying man while checking phone#PrayForLondon #Westminster #BanIslam (22 March 2017, 4:19 p.m. Tweet)

While the accuracy of this descriptor was undermined by the photographer who took the photo, who stated in the *Independent* newspaper that the woman's "behaviour was completely in line with everyone else on the bridge" and that she was "visibly distressed" (Mortimer, 2017), this combative act of misinformation was sufficiently in line with the pre-existent bias of its intended audience within the British public that its veracity wasn't questioned until much later. By which point, this tactical application of misinformation through another social media platform had become a part of the already fragile social discourse surrounding multiculturalism and integration. This particular Twitter account is one example of those that were created and managed solely to act as digital agent provocateurs, giving the appearance of shared identity or ideology, while in reality that appearance provided the cover required to give legitimacy to the destabilising messages, fake news, and stolen information pedalled by this and similar accounts. As part of ongoing investigations into the interference with political campaigns by Russia carried out by state entities and the by social media services themselves, a large number of Twitter accounts have been linked to this form of campaign. Twitter itself released a statement suggesting that they had removed 50,258 accounts thought to be linked to the Internet Research Agency, stating that tweets from these accounts had reached at least 677,775 Americans (Swaine, 2018). While Twitter's shift to a policy of actively purging accounts believed to be a part of this political influence campaign raises issues regarding free speech and censorship, it also provides insight as to the reach that these Twitter accounts have had, and continue to have, with the American public.

On 21 February 2018, Twitter engaged in another mass purge of accounts which exhibited "behaviours that indicate automated activity or violations of our policies around having multiple accounts, or abuse" (Gallagher, 2018). As reported by Ars Technica, shortly after this purge a number of notable figures within the alt-right movement in the USA began to report a significant drop in the number of their followers. While these drops cannot be wholly attributed to accounts managed by the IRA, it is likely that, considering that these accounts were the target of Twitter's actions, a significant proportion of these now purged accounts were operated by this organisation. The fact that a large number of these accounts followed and, in some cases, actively retweeted content from Richard Spencer, a notable individual with the alt-right movement and others within this same movement provides evidence of the level of interaction that these accounts achieved within American political and social discourse.

It is also worth noting that accounts such as these have not limited their attentions to shaping the outcomes of the Presidential elections as their only route towards political and social destabilisation. In the wake of the school shooting in Parkland, Florida on 14 February 2018, accounts known to be controlled by Russia, most of them automated 'bot' accounts, began to push messages related to the shooting. These included the use of hashtags such as GunControlNow, NRA, and the name of the shooter: Nikolas Cruz (Griffith, 2018). Hamilton68 and RoBhat Labs continue to track politically motivated twitter bot accounts, the former focusing solely upon Russian-operated accounts and the latter on more general accounts. Despite the strategy of misinformation employed within the USA by Russia coming under an increasing level of public scrutiny it would appear that it maintains enough efficacy to be continued.

The normative credibility of this form of information warfare is further validated by the fact that it is not constrained to application solely against the USA. Evidence of Twitter bots controlled by Russia exists in relation to a number of other political campaigns in Europe over the past several years. The example given earlier referencing the terrorist attack in London is only one notable example of a coordinated campaign directed against the UK's social and political discourse regarding its position within the EU. Some of the same accounts that would later be employed against the USA, and others seemingly created specifically for the purpose, engaged in a divisive marketing campaign, picking contentious topics which could be employed to stoke resentment towards the European Union (Burgess, 2017). Common topics in these tweets included migration, Islam, and terrorist attacks in Europe. One study identified 156,252 Russian-affiliated accounts that employed the #Brexit tag in the run up to the referendum, which posted almost 45,000 messages in the 48 hours surrounding the 23 June vote

(Gorodnichenko et al., 2017). While a large proportion of these tweets were made after the vote, their impact, both prior to and after the vote, was amplified by a further trend noted in this report; that human users on Twitter acted as the most effective disseminators of the message initially introduced by these Russian-controlled accounts (Gorodnichenko et al., 2017, p.11). With regards to the campaign of misinformation warfare around Brexit, the bot Twitter accounts operated by Russia acted as the vectors for misinformation to feed into public debate, whereupon that public itself would disseminate the message through retweets.

A further, and final, point to note: social media is not the only vector through which this combative form of information warfare has been applied by Russia. It is the credibility offered to the fake identities and ideologies behind Russian-controlled social media accounts that allowed for Russian influence to be extended to American and British citizens. The legitimacy offered through this digital medium of social interaction, and the opacity of communications online in general, allowed for the appearance of solidarity to be taken as genuine, thereby recruiting individual citizenry and their social and ideological causes to the Russian goal of destabilisation. This search for legitimacy, required to act as diffusion as to the reality of the source and intent of the information offered, allowed for a number of other information delivery systems; central among them was the website WikiLeaks, and its founder Julian Assange.

The particular attraction of WikiLeaks as another proxy and recruiter of proxies is its pre-existing legitimacy as a source of unbiased, apolitical information. WikiLeaks' main purpose, according to its website, is the "analysis and publication of large datasets of censored or otherwise restricted official materials involving war, spying and corruption" (WikiLeaks.com, n.d.). It is best known for releasing materials passed to it by whistle-blowers such as Chelsea Manning – who gave the site a large cache of military and diplomatic cables which it then published in full in September 2011. It was work such as this, and the exposure of abuses of power and corruption, that led WikiLeaks to gain accolades such as Assange being voted *TIME* magazine readers' person of the year in an online poll in 2010 – reflecting and cementing its legitimacy as an apolitical media outlet. Its position as such makes it an ideal vector for the dissemination of weaponised information or disinformation campaigns.

Messages employed on Facebook and Twitter predominantly targeted those of a more conservative or right wing ideological leaning (Gorodnichenko et al., 2017, p.9). In the case of the US Presidential election there is evidence of a bias towards electing Donald Trump, as well as a high level of negative bias against Hillary Clinton (Hamilton68, n.d.; Robhat Labs, 2017). There is, as demonstrated by the examples of purposefully clashing Facebook events

previously mentioned, evidence that despite this preference the underlying aim of this campaign of information warfare was to create a state of political and social disquiet and destabilisation. In order to achieve this goal with as great an efficacy as possible the stratagem could not focus entirely upon one ideological grouping alone – it had to stir up similar levels of unrest within the opposing ideological position as well. This was achieved in two ways, the first involving the assassination of candidates' ideological credibility, and the second through employing a medium of spreading misinformation that would, through its reputation, hold a greater legitimacy with left wing audiences.

WikiLeaks as a vector for the insertion of misinformation necessitated a distinct methodology, very different from that utilised through social media. While Twitter, Facebook, Instagram, and others allow for the message directed at the target audience to be shaped and altered to purpose, that is not the case with WikiLeaks. Information hosted and thus offered to audiences through this medium is in a raw format. In this instance the ammunition, the information gained through phishing campaigns such as those directed at the DNC or Emmanuel Macron, was simply released to the public generally without alteration. While the content could not be significantly altered, the timing of these releases could itself be employed to maximise effect, so too could the sheer volume of information released.

In the case of the Podesta emails, WikiLeaks began releasing their contents on 7 October 2016 and continued to release more throughout October, with the total number of transcripts numbering into the thousands (WikiLeaks, n.d.). To contextualise the timing of this, the Presidential debates between then candidates Donald Trump and Hillary Clinton began on 26 September and culminated on 19 October. While the timing served to offer ammunition to arguments undermining Hillary Clinton, the scale of the archive of emails and the source which offered it served to obscure the intent of this release. In a similar manner as to how Facebook and Twitter provided a curtain behind which Russia could conceal its role in the messages transmitted to American audiences, Wikileaks, its previously liberal credentials, and the volume of information offered, obscured the guiding hand of the Russian state in this act of democratic sabotage.

The central benefit to the exploitation of weak norms of cyber-war, particularly the targeted use of information to achieve military goals within an opposing nation, is that these aims can be achieved concurrently to the strengthening of the norms which allow them. The apparent efficacy of Russia's operationalised construction of cyber-war is based upon two key factors: firstly, the concurrency of action with norm creation is both more rapid and more difficult to

refute through discourse-driven means; and secondly, the combative use of information to achieve military aims has proven to be incredibly successful.

The Podesta emails, leaked through WikiLeaks, were analysed and then taken up both by Hillary Clinton's opponents within her own party and by her rivals in the Republican party. Most notably, her speech made to Wall Street firms such as Goldman Sachs was released as a transcript as part of this email dump. Both Bernie Sanders and Donald Trump made reference to this transcript when campaigning against Mrs Clinton. The former references this speech, and the fee that Clinton apparently received for it, in the Democratic party debates in April 2016 (CNN, 2016), and the latter makes the following statement, where he describes Clinton as belonging to a global elite responsible for stripping wealth from the USA, during a speech at West Palm Beach on 13 October 2016:

We've seen this first-hand in the WikiLeaks documents in which Hillary Clinton meets in secret with international banks to plot the destruction of U.S. sovereignty in order to enrich these global financial powers, her special interest friends and her donors. (Donald Trump in Chokshi, 2016)

While Trump's utilisation of WikiLeaks provides another success and thus further support for the Russian norm of cyber-war, it is the uptake of this leaked information by Sanders that adds the greater support for this norm and its operationalised method of construction. In employing the material provided by WikiLeaks, even in a more subtle, nuanced manner, Sanders both provides a further success to this form of cyber-war and gives greater resilience to the norm underpinning it: it is effective demonstration that this methodology, when effectively employed through a variety of attack vectors and with careful selection of timing, can not only reach, but successfully influence the political and social dynamics of an opposing state in line with the aggressor's aims.

This strategy (destabilising an opposing state from within) is, as discussed earlier, by no means a phenomenon unique to our modern, social mediatised age. The recruitment of proxy actors is a well-documented methodology of inter-state conflict when the initiating state cannot risk direct confrontation with its opponent. The information sources provided by the internet and which concurrently make them into attractive tools in campaigns of information warfare have had a unique effect upon the modern iteration of proxy actors in inter-state conflict. While under previous, historical states of conflict state actors would aim to recruit and act through willing accomplices, terrorist organisations and separatist groups, social media and other internet-based sources of information such as WikiLeaks have provided a medium by which a

state can seek to directly influence the politics and social affairs of its opponents, recruiting proxies which are entirely unaware of their role. Not only is this capability reflective of Russia's blurring of the boundaries between politics and war, but it is evidence of the effective exploitation of either weak or non-existent norms which might otherwise have restrained the deployment of this form of warfare. The success of this method, evidenced by the continued unrest in the American political and social spheres, the shambles of British politics in the wake of the Brexit referendum, and the continued difficulties of the German state to form a political consensus, has only served to further entrench the norms constructed parallel to their active employment.

Destabilisation as the goal: undermining legitimacy through damaging critical national infrastructure

This chapter has thus far focused heavily upon a form of cyber-war which is significantly abstracted from the traditional, military framework. While it is undeniable that the form of cyber-warfare considered in the majority of this chapter requires acceptance of the position that an act of war doesn't have to involve a physical component, it would be remiss to suggest that such a component is entirely absent from the category. Cyber-attacks between states can result in physical damage and there is increasingly evidence that they have done so, with an increasingly broad range of state actors demonstrating this kind of cyber-capability. This form of destructive cyber-attack shares three particular traits with the information-centric form discussed earlier in this chapter: firstly, Russia has acted as a norm entrepreneur in the utilisation of this form of attack; secondly, the aims of these attacks are destabilisation of political and social cohesion within target states; and thirdly, the construction of these norms is similarly operationalised. The process of norm construction with regards to destructive acts of cyber-war is reflective of those of its non-destructive cousin. Cyber-attacks are carried out, their success affirms the normative basis of these attacks, the limited or non-existent response further ratifies this norm, and finally the success of this methodology and ineffectiveness of the response results in the exporting of this norm to other actors. This normative chain will be demonstrated once again through the consideration of the Russian case study. I will look at a series of cyber-attacks, attributed to Russia, directed against the energy sector in a number of states, and at how a similar methodology appears to have been adopted by North Korea.

Cyber-attacks against critical national infrastructure such as power, communications, and emergency services have become increasingly prevalent within discussions concerning state security and in the news media. Reports regarding the intrusion of state-sponsored attackers into state power generation networks have become more common in reported news

(Greenberg, 2017a), and are increasingly raised by cyber-security firms (Symantec, 2017a) and within the discourse-shaping national security policy of powerful state actors (McGoogan, 2017).

In December 2016 Kiev, the capital of Ukraine, suffered a significant power outage. A single transmission station was taken offline, which resulted in Kiev losing roughly a fifth of the city's total power capacity for an hour. This was the first strike of a piece of malicious code which was designated as 'CRASHOVERRIDE', or, more pertinently, 'Industroyer'. The security firm ESET described Industroyer as the "biggest threat to industrial control systems since Stuxnet" (Cherepanov and Lipovsky, 2017). It further described how Industroyer "is an advanced piece of malware in the hands of a sophisticated attacker" (Cherepanov and Lipovsky, 2017). While the destructive impact of this particular cyber-attack may appear limited compared to military attacks with comparable objectives, it creates a series of implications based upon its wider context. This was the second cyber-attack against Ukrainian power infrastructure, the first having taken place almost exactly a year prior. This attack appeared to be the culmination of a modus operandi strikingly similar to that of Russian information warfare strategy. In 2014 a series of infected documents and phishing emails were directed at electricity distribution companies in Ukraine. A digital forensic analysis of the cyber-attack in 2015, which left a large proportion of homes in the Ivano-Frankivsk region of Ukraine without power, revealed that the same group was likely responsible for both attacks (Lipovsky and Cherepanov, 2016).

Both of these attacks coincided with the ongoing conflict between Russia and Ukraine regarding the annexation of the Crimea by Russia on 18 March 2014. The security firm Dragos, in confirming the analysis of ESET that "it appears the Kiev transmission substation targeted in 2016 may have been more of a proof of concept attack than a full demonstration of the capability of CRASHOVERRIDE" (Lee, 2017), further adds the reassurance that this piece of malware would be able to cause "more than a few days of outages, and even to get a few days, would require the targeting of multiple sites simultaneously which is entirely possible but not trivial" (Lee, 2017). While this final pronouncement offers a welcome counter to the doomsday scenarios with which cyber-war is often associated, the limitation of this form of attack is in this instance technical, not as a result of restraint.

Further evidence of the active construction of cyber-warfare norms within Ukraine is the malware named NotPetya, so called due to its initial categorisation as another instance of a piece of malicious code named Petya. NotPetya, first found in June 2017, was a piece of ransomware – malicious code which encrypts the infected machine and demands a ransom, generally payable via anonymous cryptocurrency transaction, to acquire the decryption key.

Researchers at Kaspersky Labs and Comae technologies both concluded, however, that NotPetya was a form of destructive malware masquerading as ransomware. Both companies separately concluded that NotPetya didn't contain any of the necessary tools for decrypting infected machines, even if the ransom was paid (Ivanov and Mamedov, 2017; Suiche, 2017).

NotPetya caused significant damage, and on a large scale. While the majority of infected machines were centred within Ukraine, the initial infection being through a piece of accountancy software predominantly used by the Ukrainian state, it spread internationally. Maersk, the international shipping company, was forced to replace or reinstall 45,000 PCs in the space of 10 days (Chirgwin, 2018).

The number of probative, testing attacks targeted or centred around Ukraine does not only lend credence to the conclusions of the international community as well as the security community that these attacks were likely carried out by Russia. Ukraine presents an opportunity to develop both the capability of and the normative framework for a more destructive form of cyber-warfare, allowing for the utilisation of the same methodology of operationalised norm construction which was, at the same time, being applied to the development of information warfare. Ukraine presented a test-bed for this form of operation due to the success of Russia's annexation of the Crimea and the relatively ineffectual responses of the international community. Much as Brexit provided an early proving ground for the technical capability and efficacy of cyber-espionage and the manipulation of social media, Ukraine's critical national infrastructure provided a true-to-life model in which to both test destructive cyber-capability, and to concurrently begin shaping the norms related to it. The limited responses to Russian annexation of Ukrainian territory were similarly expanded to both the cyber-attack CRASHOVERRIDE and to NotPetya. Despite significant evidence as to both the potential risk posed and the Russian source of these attacks, it wasn't until February 2018, eight months after its initial discovery, that the UK ascribed the attack to Russia (NCSC, 2018). Comparably to the operationalised construction of information warfare norms previously discussed in this chapter, this discursive response is unlikely to create any significant resistance to the affirmation of Russia's preferred norms regarding destructive cyber-attacks. Indeed, evidence for the diffusion of a normative position that allows development, preparation for, and testing of this form of weaponry can be seen in the utilisation of similar tactics between another set of international opponents.

On 13 May 2017 the WannaCry ransomware left the UK's National Health Service (NHS), the shipping firm FedEx, Germany's national rail operator and other companies and institutions across the globe locked out of their computer systems and databases in what was described at

the time as the largest outbreak of malware of this kind in history (Bodkin et al., 2017). Similar to NotPetya, which was to be discovered a month later, WannaCry not only demanded a ransom payment in order for the machines to be decrypted, but also failed to deliver on this promise whenever the ransom was actually paid; demonstrating that the financial component of this attack was ancillary to the damage and disruption that it caused (Bossert, 2017). Aside from the scale and spread of this attack, WannaCry infected more than 230,000 computers in over 150 countries (Nakashima and Rucker, 2017). It is this attack's source which holds particular interest: attributed to North Korea by both the USA and the UK, this attack demonstrates how the norm constructed through the operationalised usage of this capability by Russia within Ukraine, and with more restraint against other targets, has reached a sufficient level of legitimacy to be adopted by North Korea, which in turn makes it a norm entrepreneur. Evidence gathered by Kaspersky Labs and Symantec suggests that the source of the WannaCry ransomware was the Lazarus Group (Symantec, 2017c; GReAT, 2017). This group had previously carried out the attacks against Sony Pictures in 2014, also attributed to North Korea, and the theft of $81 million from a Bangladeshi bank in 2016 (Solon, 2017b).

With this attack, North Korea not only provides evidence that the normative position constructed by Russia has gained a new adherent, it also itself becomes a norm entrepreneur. Its utilisation of cyber-capability with WannaCry fits within the broad remit granted for this form of activity by the norms of cyber-warfare constructed through similar, if more restrained and focused, attacks carried out by Russia against Ukraine, Estonia, and Georgia. WannaCry, and thus North Korea, serves to further contribute to the operationalised construction and the legitimisation of the normative position implicit within the usage of this form of cyber-attack. The variation from the Russian iteration, the broader targeting and minimal evidence of care with regards to collateral damage, and the potential international response resulting from this is reflective of the position which North Korea has taken with other methods of war. North Korea's continued nuclear programme and its development and testing of intercontinental ballistic missiles is mirrored within its testing and deployment of cyber-capability against opposing states.

The effectiveness of this once again operationalised construction of norms does not rest entirely upon the actions of the state or states who employ these methods; it also depends on the nature and efficacy of the response made by the victim of these attacks and the international community more generally. The contrasting set of norms, which should shape and govern the responses by both the UK and the USA, can be extracted from the aforementioned Talinn Manuals Both the UK and the USA are members of NATO, the key

sponsors of the legal examination in the first and second of these manuals. It is unsurprising then that in responding to both the NotPetya attacks and, most notably, WannaCry the language used is reflective of the normative position of these codices – that the use of destructive cyber-attacks is beholden to the same rules of international armed conflict as traditional forms of attack, and that WannaCry in particular was sufficiently indiscriminate to fall foul of these prescriptions (NATO Cooperative Cyber Defence Centre of Excellence, 2017).

A statement released by the NATO Cooperative Cyber Defence Centre of Excellence in June 2017 not only attributes both NotPetya and WannaCry to state actors, but reiterates that NATO's position is that a "cyber operation with consequences comparable to armed attack can trigger Article 5 of the North Atlantic Treaty and responses might be with military means" (NATO Cooperative Cyber Defence Centre of Excellence, 2017). This response is critically undermined, however, by the fact that key members of NATO have themselves engaged in cyber operations that could be considered in breach of the normative principles within this statement and expanded in the Talinn Manuals. The USA's use of the malware Stuxnet in 2009 to destroy Iranian centrifuges in Natanz (Lindsay, 2013), and the fact that the foundations of the code used to craft both NotPetya and WannaCry were hacking tools developed by the US National Security Agency (Ivanov and Mamedov, 2017), seriously detract from the legitimacy and thus power of such discursive statements with regards to enforcing a normative position.

The Russian examples of destructive cyber-attack and those carried out by North Korea lead to several conclusions. Firstly, and most categorically, destructive cyber-attacks capable of causing physical harm in a manner comparable to traditional concepts of military force are not only possible, they have already been employed. Secondly, the normative basis for these destructive, high-level cyber-attacks has been developed in the same operationalised, implicit, and active manner as those regarding low-level attacks and the nature of information warfare of which they are a part. This process is also predominantly contributed to by the same actor – Russia. Further to this, these attacks have been repeatedly met with the same discursive-driven attempts to enforce or create a normative counter-position; and, in a reflection of responses to low-level attacks and information warfare, these responses have been ineffective and critically undermined by the complicity of other states who outwardly support restraint-orientated norms constructed through discursive means. Finally, the success of both this technical capability in providing the desired results to the aggressor and of the parallel construction of a normative basis is further demonstrated by the adoption of these methods by other state actors; who, through this process, become norm entrepreneurs themselves,

contributing to the continued diffusion of a normative concept of destructive cyber-war which eschews restraint.

Contesting information warfare: too little, too late?

Through the examination of the two facets of Russian cyber-warfare strategy this chapter has tested this thesis's hypothesis concerning the existence and the relative normative power of operationalised norms, and the inherent weaknesses of their discursively constructed counterparts. It has also detailed how the campaign of cyber-warfare considered here, the Russian example, is granted its efficacy through more than just its unique technological component. While the anonymisation granted through cyber-espionage and the social media-driven campaigns of information that utilised stolen data is a unique capability, the level of plausible deniability allowed for a previously unprecedented level of access to the target audience. The technological component is what allows for what can be described as the most effective example of Psychological Operations ever carried out by a state actor: the interconnectivity of critical infrastructure creates the pathway for a state to employ cyber-attacks in a destructive manner to achieve effects which would previously have required a large-scale military intervention.

The most notable component of this form of warfare, however, is the normative component. As considered in the previous chapter, states face the difficult challenge of seeking to update norms and policy to keep up with technological capability and integration that develops at a rate without any effective comparison. This is not only true on the domestic level. The concept of cyber-war, although long considered by state militaries and academics, has previously only been examined through a normative lens, which takes for granted the discursively constructed norms forwarded by the international community. Discussions of the implications of the international laws of armed conflict and the norms which they represent is evidence of an academic methodology which is approaching the problem from the wrong direction. These norms were, in effect, copied and pasted from the original form onto the concept of cyber-war. What this chapter has done is examine the construction of norms through the active utilisation of the form of warfare to which these discursive norms are meant to apply. This approach has led to the conclusion that this operationalised methodology of norm construction produces a normative position faster and with greater resilience to challenge than the discourse-driven alternative. The norms of cyber-warfare which the international community and the academic community have taken for granted are further undermined by the simple reality that Russia is not the only state to contribute to this nascent normative position.

The development of cyber-weapons, and their employment, by the USA and the UK has not only contributed to furthering the legitimacy of Russia's normative position, but also has undermined any attempts to challenge the direction in which Russia's actions have taken the norms of cyber-war. The credibility and thus efficacy of accusations of breaching normative constraints on cyber-war are critically undermined when the institutions making these accusations and their members have engaged in attacks which bear striking similarities to the attacks carried out by Russia, and later by North Korea.

Beyond the implications of rapid technological change upon the norms of international conflict, this chapter has further exposed that there are, within the targets of these norm producing attacks, inherent vulnerabilities which lend the attacks, and thus the development of these norms, added weight. The campaign of cyber-attacks and destabilising information warfare directed against the USA prior to and continuing since the US Presidential election of 2016, as well as similar stratagems employed in France and the UK, can all ascribe a portion of their success to their timing and the prevailing social and political divisions within their target countries. The partisan divide in the USA is still so severe that despite the evidence of a foreign state interfering in their elections a distinct punitive response has yet to be enacted. Within the UK the political disarray resulting from the Brexit referendum continues to divide public opinion and threaten to undermine political cohesion. While this form of cyber-war might rely upon successful low-level phishing attacks to provide ammunition, aided by the acceptance of the *white noise* of these low-level attacks between states, the most notable component is the resurgence of populist political and social positions within the victim states. Cyber-war provided the means, the pre-existing splintering of social and political cohesion provided the ideal conditions for attack.

Finally, I would conclude that this chapter demonstrates that Russia, in embarking upon norm construction with regards to both low-level and destructive cyber-attacks, has not merely benefited from achieving the goals set out for these attacks; in so doing it has also further cemented this less restrained form of cyber-warfare within the international community. With North Korea's uptake of this form of cyber-war against its perceived enemies, the hermit kingdom takes its place alongside Russia and indeed the USA, the UK, and Germany as securitised norm entrepreneurs with regards to cyber-war. In so doing, they begin to contribute to a normative position that opens up the digital domain as a new theatre of war and produces a new form of warfare. Russia has gamed the system; through engaging in operationalised norm construction as opposed to engaging within the dialectically-driven model, Russia has stolen the lead, building a normative position through an essentially

uncontested process. Once this process had provided Russia an obvious advantage – power – then the digital equivalent of Pandora's box had been opened and cyber-war, broadly framed in the Russian mode, had begun to spread to other state actors. The closure of this box would appear unlikely or at least extremely difficult. Those actors that might have engaged in an effective defence of the international norms codified in documents such as the Talinn Manual are themselves guilty, even if unintentionally, of undermining these same norms through their own forays into cyber-war. A norm of cyber-warfare in which states assume a position of restraint is not entirely out of reach. It will, however, take a concerted effort to rebuild the necessary legitimacy of norm entrepreneurs supporting this position and will require this opposing normative position to be constructed and defended by an operationalised process of norm construction all of its own.

Chapter 6 – Cyber-terrorism: a reciprocal process of norm construction

Introduction: considering overlapping types of securitised norm construction

Cyber-terrorism norm construction is engaged upon by both states and the terrorist organisations themselves. Terrorist actors utilise threat, issue cyber-specific calls to arms, and engage in limited cyber-attacks in an augmentative manner in order to supplement their coercive power. These actions are then supplemented/enhanced by state actors employing these statements and actions to further securitise the discourse around cyber-terrorism and justify a stricter state of securitised digital policies – as seen in the previous chapter. Unlike Russian efforts to operationally shape the norms of cyber-warfare, these terrorist organisations are unwitting practitioners of active norm construction. While Russia recognised and exploited the confluence of weak norms and technological flaws, terrorist organisations threaten a level of damage that they cannot achieve. Their goal is to coerce through fear, piggybacking on an emergent realisation among states and individuals as to the risk we have exposed ourselves to with our reliance on network infrastructure. That does not mean, however, that they do not contribute to the developing norms of cyber-terrorism. If and when that capability is achieved, the framework for its employment will be based upon the groundwork of action and discourse that has preceded it.

There are two issues surrounding the role of states with regards to the norm construction of cyber-terrorism. Firstly, the manner in which they appropriate the over-stated and unintentional contributions of terrorist actors to the development of these norms, using them as facilitating conditions to add legitimacy to the securitisation of the digital domain and the apportioning of resources to counter what is in reality a small or non-existent threat. The second issue is the shift in this securitising narrative when, once again relating back to the previous chapter, evidence of a real threat enabled through this same domain results in a switching of focus away from terrorism and towards the danger of cyber-warfare. The same rhetoric and reference to facilitating conditions is then applied by state actors to what is a more realistic and temporally pressing threat. These two examples demonstrate that the manner in which norms are commonly constructed by states and non-state actors, be it driven by discourse or through operational methods, can be found across securitised issues. Further to this, they demonstrate that in the case of terrorism, the inter-dependence of discourse-driven construction by states and operational construction by non-state actors constitutes what can be described as a feedback loop; the threats or acts of the terrorist organisation are used by a state actor to describe an inflated level of risk in order to justify expenditure or policy, this risk then serves to heighten the public's fear of acts of cyber-terrorism, which

concurrently legitimises securitisation by the state and encourages terrorist organisations to continue to threaten attacks which are now even more prevalent within the consciousnesses of their intended targets.

The final theoretical concept that cyber-terrorism and the previously considered topics of cyber-warfare and surveillance serve to support concerns the negative imperative applied to the concept of securitisation from its most well-known sources. The Copenhagen School, Barry Buzan most notably, posit that the purposefully constructed shifting of politics from the normal to the securitised through the employment of emotive imagery and facilitating conditions is an inherently negative phenomenon. What can be concluded through the analysis of securitised norm-construction surrounding cyber-terrorism and the supplanting of its position by cyber-warfare, most notably through the medium of information warfare, is that this process was not unnecessary. It was simply misdirected. The prioritisation, increased awareness, and resource-gathering potential of securitisation employed towards cyber-terrorism and terrorism in general was misdirected. The flaw was not with the process of securitisation, it was with the target.

This chapter will be split into three major sections. The first two will consider the construction of norms of cyber-terrorism from the perspectives of two of the core types of norm entrepreneur involved within this process: terrorist organisations, and states. These two sections will draw upon statements of intention, justifications for proposed policy or action, and actual operational employment of either acts of cyber-terrorism or counter-terrorism. In these sections there will be some crossover with the source material analysed for the purposes of the first chapter of this thesis – the cyber-surveillance chapter. This is specific to considering states' role in the construction of cyber-terrorism norms. However, in order to offer a more convincing argument that properly demonstrates the strength of the theoretical concepts involved, I analyse further examples so as to develop the argument of the previous chapter. These include proposals to curtail encryption-based technologies and to enforce responsibilities and constraints upon Internet Service Providers and social media.

The section which focuses upon the role of terrorist and non-state actors as norm entrepreneurs with regards to the norms of cyber-terrorism will primarily consider statements of capability, calls to arms, and claims of responsibility made by various actors that fit this categorisation. With regards to the evidence of operationalised norm construction, the notable difference between these two norm entrepreneurs – to be illustrated by this chapter's analysis – will be provided by the actual acts of cyber-terrorism carried out by these groups. The final section of this chapter will examine the reciprocal relationship between these two

kinds of norm entrepreneur. I will demonstrate how the construction of cyber-terrorism norms is a process which is shaped by two different kinds of norm securitising norm entrepreneur, each with opposing motivations.

Cyber-terrorists: the illusive threat

For the purpose of clarity, it is important to ascribe more depth to what is meant within this chapter by the term cyber-terrorist. Within current usage there is a distinct contention between academic literature and news media representation. In a manner reminiscent of the definitional arguments over cyber-warfare and crime, a great deal of academic focus is centred upon whether cyber-terrorism – the threatening phenomenon described in the statements of politicians and by news media – has any factual, empirical basis. This chapter will seek to contribute to this debate, ultimately concluding that the norms of cyber-terrorism evident within the policy and statements made by the UK are based upon an acceptance of a capability that has not to date been demonstrated by any of the applicable non-state actors to which they are targeted. This itself offers insights into the relative power and nature of norms and the manner of their construction with regards to cyber-terrorism.

The two opposing positions (those found in the news media and those in academia) regarding this terminology can be broadly explained as existing in relation to whether the *cyber* component of cyber-terrorism is related to a group's *methodology* or its *ideology*. The academic interpretation of the term commonly suggests two problems with the apocalyptic scenarios described by politicians or in opinion articles (Stohl, 2007, p.225): firstly, there is the suggestion that cyber-terrorism as a referent to the method of attack has yet to demonstrate its efficacy at resulting in the death or destruction attributed to the conjoined concept of terrorism; secondly, there is the ascription of cyber-terrorism to be a unique form of terrorism in and of itself. The most notable refutation of this position is that cyber-terrorism, in an ideological sense, has yet to be seen empirically; the only acts of cyber-terrorism that can generally be noted are carried out by actors to supplement other, traditional forms of attack – as a force multiplier (Cavelty, 2008, pp.19–21). By ideology in this sense I refer to some form of coherent system of thought which results in a related programme of political ideas or actions. Anonymous is the only group that might provide a larval form of an *ideologically* as opposed to a *methodologically* defined example of cyber-terrorism.

This chapter will engage with both of these counter-positions to the apocalyptic narrative in popular media discourse and by state actors themselves. I will achieve this by addressing both a group which could potentially offer an example of an ideologically motived cyber-terrorist organisation, and by ensuring that evaluations of the potential threat physically posed by

cyber-terrorist actors are measured against both the technological possibility of damaging cyber-attacks and the motivation of terrorist actors to employ them. The groups that I will consider are Anonymous, al-Qaeda, and the Syrian Electronic Army, and the states which will be analysed for their input into the norm construction of cyber-terrorism will be Israel and the UK.

Cyber-terrorists: playing on expectations

As previously stated, the purpose of this section is to examine the role that actors that could be called cyber-terrorists take in the development of the securitised norms of cyber-terrorism. I will demonstrate how the threats made by these actors, with regards to cyber-attack, are rarely translated into the promised action or destruction. Following on from this, an explanation will be offered for why these groups threaten and carry out this kind of attack. Finally, I will connect the two, demonstrating that there is evidence of both discursive and operationalised norm construction to be found in the analysis of the actions and statements of terrorist actors. This is similar to that engaged upon by Russia with cyber-war, as explained in the previous chapter. Furthermore, I will offer the conclusion that terrorist actors, much like state actors, are bound to try to maximise their potential power through the acquisition and usage of cyber-capability; in the case of terrorist actors the difference is the lack of evidence of this capability. Discursive acts of securitisation both seek to multiply the fear output of these organisations and to inflate the perceived effects of what limited acts of operationalised construction they do manage to achieve. Much as the *cyber* element of cyber-terrorism is described in the literature as often nothing more than a force multiplier, the discursive element of terrorist groups' input into this process of normative construction is a *norm multiplier* – serving to maximise the impact of what limited, augmentative cyber-capability these groups can in fact employ.

<u>The cyber-terrorists: ideological, state-affiliated, innovators</u>

To gain insight into the role that various terrorist groups have played in norm construction we must first search for examples of direct action or statements made by these groups that can serve as evidence for such an impact. Taking into account this thesis's overarching argument for operationalised norm construction, I will include within this analysis not only evidence of the threats or statements made by the groups, but the actual usage of cyber-capability that these groups employ. While previous studies of cyber-terrorism have given attention to the impact of cyber-attacks actually carried out by groups, this analysis tends to be directed at answering questions as to the reality of the threat posed by the author's proposed definition of cyber-terrorism (Heickerö, 2014, p.564). This chapter, in contrast, seeks to demonstrate that

the language and nature of discursive norm construction evident in a terrorist actor's threats, calls to arms, and claims of responsibility are components of a *broader* process of securitised norm construction. Furthermore, that these discursive acts of norm securitisation are accompanied and amplified by these same groups actively engaging in cyber-attacks. This constitutes further evidence of operationalised norm construction.

To these ends, three different terrorist groups will be considered. For each of these a particular attack or form of cyber-attack will be described, later to be used as the material evidence towards ascribing a two-stage, operationalised and discursive construction of securitised norms to cyber-terrorist actors. Through this consideration I will move from description to explanation, developing the theoretical framework established in previous chapters. These attacks will then be used in the remainder of this chapter to demonstrate how each of these three non-state actors have engaged with the norms of cyber-terrorism in a manner, both discursive and operational, that would allow them to be considered as norm entrepreneurs as framed by Finnemore and Sikkink (1998). These three groups will be the hacker collective Anonymous, al-Qaeda, and the Syrian Electronic Army (SEA). This is by no means an exhaustive list. However, it does allow for the consideration of the two categories of cyber-terrorist actor that previous debates have delineated. The latter two, the SEA and al-Qaeda, are both groups which employ cyber-capability in an augmentative manner; they employ cyber-attacks either alongside other, more physical forms of attack or in a manner which supports these physical means of violence. Anonymous, however, is an example of a group who, at least to some extent, appears to possess the ideological connection which allows for its ascription as a potential cyber-terrorist group to be akin to calling al-Qaeda an Islamic or religious terrorist organisation. The following sections will provide brief summaries of the terrorist actors and notable cyber-enabled attacks that they have engaged upon. Following sections will build upon these examples to demonstrate how the groups and their actions relate to my theoretical claims regarding securitised norm emergence and construction.

Anonymous: one person's hacktivist is another person's cyber-terrorist

Beginning with Anonymous, we will focus on attacks targeted at Israel. Op [Operation] Israel, a large-scale attack by Anonymous and affiliated individuals and groups against the Israeli state, first took place on 7 April 2013, and has since become an annual event, purposefully timed to coincide with the eve of Holocaust Remembrance Day (*Times of Israel*, 2013). Anonymous reiterated the motivation for this specific attack and others directed by its loosely connected

membership against Israel as a response to the occupation of Palestine. It released the following statement through an affiliated Twitter account:

> OpIsrael Anons (@Op_Israel)
> #opisrael for solidarity with Palestine. #opisrael for raising awareness about the Palestinian people. They are under the Israeli occupation for 667 years. It's time for Palestinians to live in peace, freedom, dignity. (7 April 2015, 5:42 p.m. Tweet)

Cyber-attacks directed at Israel as part of this ongoing and annual campaign consist of Directed Denial of Service Attacks (DDoS), the theft and release of data, and website defacements. In relation to the construction of norms of cyber-terrorism, these attacks resulted in a great deal of contention between the aggressors and the victims about the damage caused. A notable instance of this occurred as part of OpIsrael 2013, where attacks were directed at the public-facing website of the Israeli security agency Mossad. A DDoS successfully took this website offline for a short period of time, during which Anonymous also released, through one of its Twitter accounts, what was claimed to be a list of the personal details of 35,000 Mossad agents (Sarkar, 2013).

The Syrian Electronic Army: state sponsored/affiliated cyber-terrorism

Two members of the SEA were added to the cyber 'most wanted' list of the US Federal Bureau of Investigations (FBI) in 2016. The agency justified the decision by stating that the SEA "provide[s] support to the Assad regime", and that it attempts to do so by bringing "harm to the economic and national security of the United States in the name of Syria" (Bertram, 2017).

This "harm" included hacks which hijacked the social media accounts of prominent individuals and groups, with the USA as the target for some of the most notable examples. In October 2013, the group gained access to the Gmail account of Suzanne Snurpus, a staff member for Organizing for Action, a lobbying group which worked closely with then US President Barack Obama. The SEA then used this access to replace all web addresses included in the President's Twitter account and Facebook page to direct to a video hosted on YouTube, which purported to "show the truth about Syria" (Berkman, 2013). Earlier that same year, in April 2013, the group hijacked the Twitter account of the Associated Press and posted the following tweet:

> The Associated Press (@AP)

> Breaking: Two Explosions in the White House and Barack Obama is injured (23 April 2013, 12:07 p.m. Tweet)

As a result, the Dow Jones, America's stock index, dropped by one per cent in two minutes. The S&P index similarly suffered a one per cent drop over three minutes, resulting in a plunge which, for a short period of time, wiped $136.5 billion from the index's value (Foster, 2013).

Al-Qaeda: mobilising for cyber-jihad

The terrorist group responsible for the September 2001 attack on the World Trade Centre in New York fulfils a particular role within this set of case studies. While the SEA provides an example of a terrorist organisation that primarily utilises cyber-capability and has a notable state affiliation, Anonymous provides an example of a group that can demonstrate how the normative processes this chapter will describe are equally applicable to groups whose connection to the *cyber* component of their categorisation extends beyond methodology and into ideology. Al-Qaeda is an example of a group which pre-dates the technology that serves as the necessary foundations for cyber-attacks. It has shown an intention to utilise cyber-capability alongside the more physical and direct acts of violence that it had previously employed. At the same time, al-Qaeda cannot be distinctly linked to a state in the same manner as can the SEA.

Al-Qaeda can claim ownership of, or at least the most responsibility for, the concept of cyber-jihad. The concept of cyber-jihad in literature, news, and law often extends to encompass acts which would be better described as supporting or assisting acts of terror: disseminating information; communications; planning; and the radicalisation of 'home-grown' terrorists (Davis, 2006, pp.120–121; Pallister, 2007; Rubin, 2014) – al-Qaeda having engaged in all of these. As the most well-known terrorist actor when the cyber-terrorist discourse was becoming more prevalent, thanks to the World Trade Centre attack, al-Qaeda has become a prominent example of a cyber-terrorist actor.

Dancho Danchev, a security blogger researching the uptake of cyber-capability by terrorist organisations, analysed various publications of al-Qaeda. Based on this, he suggested that while the *Cyber Jihadist's Encyclopaedia* – written in Arabic – contains information almost exclusively related to carrying out physical forms of attack, with almost no mention of cyber-attacks (Danchev in Gold, 2012, p.2), the English-language *Inspire* magazine and the *Cyber Jihadists' Hacking Teams News Letter* were very different. The former predominantly featured

articles explaining the benefits of joining al-Qaeda. The latter, written by a group known as HaCKErS Al-AnSaR or the OBL Crew – the initials of Osama bin Laden – showed far more evidence of organisation, technical ability, and instruction towards the use of cyber-attacks in support of al-Qaeda (Gold, 2012, p.16).

In the wake of Osama bin Laden's death in 2011 the British government warned of a response coming in the form of "cyber-jihad" (Morris, 2011). Meanwhile, the USA had been connecting al-Qaeda, cyber-attacks, and nuclear insecurity since only a short period after the 9/11 attack (Schultz, 2002, p.105).

Maximising impact: acting the part

The previous chapter demonstrated how securitising norm entrepreneurs might choose an operationalised method of norm construction, at once benefiting from achieving political goals from the cyber-attacks that formed the basis of this process *and* shaping the normative position in a manner that would allow for maximum effect and potentially repeated use of this effective set of tools. This chapter will argue that, while cyber-terrorist actors also employ an operationalised component in their role as securitising norm entrepreneurs, the normative impact of their efforts is unintentional. Instead, I will argue that those who might come to be referred to as cyber-terrorists utilise cyber-capability out of the confluence of two intersecting driving forces: firstly, the implicit rejection of norms – which is almost the definition of terrorist actors; secondly, the obvious benefits to the utilisation of the internet – in a number of different ways – to maximise the potential for a group to successfully achieve its goals.

Terrorism in general is itself a political tool, the usage of which coincides with the actor involved exempting themselves from norms which otherwise might limit political interaction to discourse or non-violent, non-harmful action. While the definitions of terrorism are as numerous as they are contentious, they do provide an insight as to how these groups' roles in the construction of cyber-terrorism norms are motivated through the overlapping influence of a political tool reliant upon the leverage of fear and the removal of limitations in the pursuit of political goals.

Hoffman describes terrorism as a close cousin of psychological warfare: "Fear and intimidation are precisely the terrorists' timeless stock-in-trade" (Hoffman, 2002). Primoratz adds that "the terror is meant to cause others to do things they would otherwise not do" (Primoratz, 1990, p.129). Between these two statements is described a phenomenon that relies upon fear to achieve the political aims of those who employ it. This tool is employed precisely because

other methods of achieving these political goals have failed, and in recognition of the coercive power that fear can provide to those who wield it.

The emergence of cyber-terrorist groups or the diversification of existent groups into utilising this toolset is down, at least in part, to the recognition by these groups of a state of fear that was already beginning to take root within targeted audiences. Statements by politicians, such as that by US Congressman Curt Weldon in 1999 that cyber-terrorism was one of the greatest threats to the American way of life (cited in Poulsen, 1999), have contributed to a growing sense of fear of an amorphous concept of cyber-terrorism. Embar-Seddon notes that Richard Lazarus, in 1966, directly connects the uncertainty contained within cyber-terrorism with an individual's natural fear of the unknown:

The most destructive forces working against an understanding of the threat of cyber terrorism are a fear of the unknown and a lack of information or, worse, too much misinformation. The word cyber terrorism brings together two significant modern fears: the fear of technology and the fear of terrorism. Both technology and terrorism are significant unknowns. (Embar-Seddon, 2002, p.1034)

Cyber-terrorism presents an almost unique opportunity for existent terrorist groups, or for those seeking a political goal for whom normal methods of political engagement have failed. Any act which can be classified as cyber-terrorism makes use of a prevalent fear regarding acts of terrorism irrespective of their source or methods, along with the fear of another unknown – that of technological insecurity. Cyber-attacks not only present a manner in which terrorist actors can maximise their coercive applications of fear by tapping in to the instinctive fear of the unknown; they also present an opportunity to maximise the effect of acts of terrorism while minimising the risks or costs.

These groups need to maximise the impact that their attacks have upon the audience they are trying to reach. Jenkins stated in 1975 that:

They [terrorists] are frequently described as mindless, irrational killers. But terrorism for the most part is not mindless violence. Terrorism is a campaign of violence designed to inspire fear, to create an atmosphere of alarm which causes people to exaggerate the strength and importance of the terrorist movement. Since most terrorist groups are small and have few resources, the violence they carry out must be deliberately shocking…Terrorism is violence for effect. Terrorists choreograph violence to achieve maximum publicity. Terrorism is theater. (Jenkins, 1975, p.4)

I noted in the previous chapter that Jenkins would later amend the concluding statement of this paper – that "Terrorists want a lot of people watching, not a lot of people dead" (Jenkins, 1975, p.4) – in 2006 to state that "Many of today's terrorists want a lot of people watching and a lot of people dead" (Jenkins, 2012, p.119). Critically, Jenkins still argues that terrorists are driven to create theatre, a spectacle which draws attention to their cause in a manner that induces fear in those who witness it first hand and those who learn of it later. The change, he argues, is due in part to the fact that "terrorism [has] become commonplace and the need for headlines demanded higher body counts" (Jenkins, 2012, p.118).

The pressure to compete with an increasingly large pool of other groups competing for headlines, coupled with the continued restrictions on these groups due to limited resources, has resulted in a series of methods of attack that have been able to satisfy both the requirement for fear-inducing spectacle and maximum effect for minimum cost. Most recently, this has resulted in the increasingly common usage of motor vehicles as weapons to cause mass casualties at highly public events: the University of North Carolina in the USA in 2006 (Rocha et al., 2006); the French city of Nice in 2016 (Associated Press, 2016); the Berlin Christmas market attack in December 2016; the attack on Westminster Bridge in the UK in 2017 (Withnall et al., 2017). This method of attack had been specifically mentioned in al-Qaeda's online magazine, *Inspire*, in 2010. It called for lone wolf actors in countries where publics support the "Israeli occupation of Palestine, the American invasion of Afghanistan and Iraq or countries that had a prominent role in the defamation of Muhammad" to use pickup trucks "as a mowing machine, not to mow grass but mow down the enemies of Allah" (CNN, 2010). The increased utilisation of this method from 2016 until the present provides further evidence of the pragmatic selection of methods of attack employed by terrorist organisations, in keeping with Jenkins' conclusions: attacks using motor vehicles such as those listed create the maximum amount of fear and the greatest spectacle for the minimum cost to the organisation perpetrating or, as is more common, encouraging the commission of terrorist attacks by loosely affiliated lone wolf actors.

This means that, while cyber-terrorists *do* play a role in shaping the norms of cyber-terrorism, both in terms of operationalised construction through the carrying out of cyber-supported and purely cyber-attacks and discursively as a result of threats and claims of attribution, the motivations for this input are *not* the same as those of the Russian state. Russia's impact on the nature of the norms of cyber-war is intentional, the motivation for shaping international norms resulting from the continued, if less compelling, need for even Russia to operate within international standards. However, the impact upon norms of cyber-terrorism by terrorist

actors is accidental. Unrestrained by international norms or standards, terrorists, by their nature, operate moderated by pragmatic limitations. The SEA, Anonymous, and al-Qaeda all aim to induce fear within the target of their attacks with the intention of that fear leading to specific policy changes. The success of these attacks is measured not necessarily by their immediate impact, but by the extent to which they influence a wider audience and thus the impetus for the desired change. Cyber-attacks may not result in the physical carnage and trauma that has become the common source of spectacle and impact of modern day acts of terrorism; however, they can provide a similarly powerful spectacle through the exploitation of an existent fear of the technologically unknown. Fear doesn't require a physical spectacle, especially when said fear is already rooted within the audience: it simply needs enough evidence to be credible, supported by a framing that maximises that fear – a complementary, discursive act of norm construction designed to supplement the facilitating conditions provided by a minimal, accidentally supplied operationalised method of construction.

Big threats and limited attacks: operational and discursive norm construction in parallel

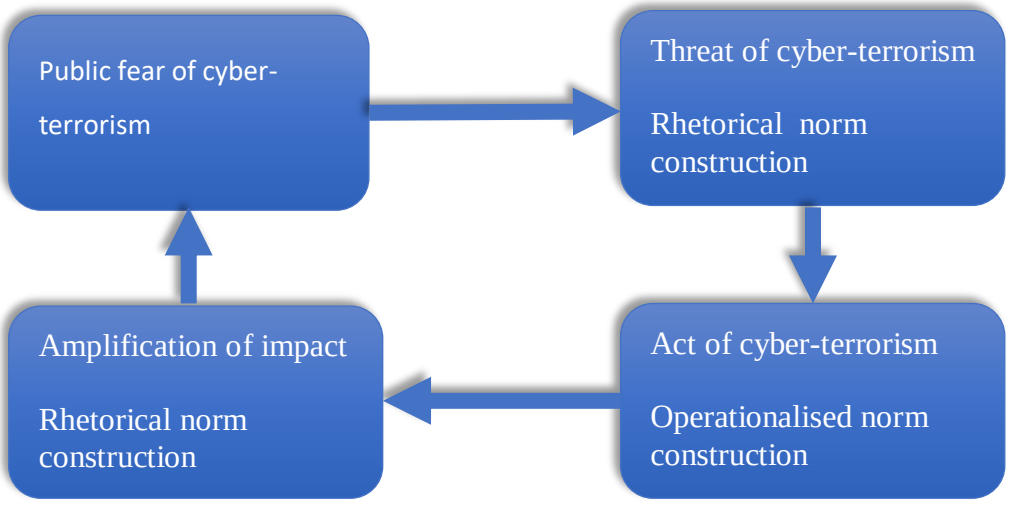


Figure 1: The cycle of cyber-terrorism norm construction: the terrorist's role.

As mentioned, cyber-terrorism has yet to produce a violent spectacle comparable to the use of explosives or the weaponisation of large vehicles in crowded areas. Of the three groups employed as case studies in this chapter, none of these groups has managed to cause a single death through the application of a cyber-attack alone. Al-Qaeda are the only group of these three to have carried out attacks that have resulted in death or physical injury. The cyber component of these attacks – despite the assertions of the group's press releases and magazines (Gold, 2012) – have been limited, providing at most varying levels of inconvenience (Cavelty, 2008, p.20). The internet has predominantly been used by al-Qaeda, and other

groups which similarly predate the concept of cyber-terrorism, to provide resources that can be used in planning and preparation of attacks which cause physical harm, alongside providing a relatively secure and effective means of communication and recruitment (Gill et al., 2017, p.107).

The SEA, an organisation that commits attacks solely through cyber-capability, similarly has only achieved what could, at the extreme end of the spectrum, be referred to as severe inconveniences. Like the al-Qaeda affiliate the OBL Crew, the SEA relies mostly upon DDoS, website defacements, phishing, and account hijacking (Geers and Alqartah, 2013). All of these are relatively simple attacks with regards to their level of complexity and the knowledge necessary to carry them out. The group's relatively limited technical knowledge is further highlighted by the fact that the malware used for its most complex attacks – those which resulted in the theft of personal user data from the Swedish firm Truecaller and others – was a pre-made tool readily available from underground marketplaces offering the sale of malicious code (Wilhoit and Haq, 2014). While thefts of this kind and large-scale DDoS can have a significant impact upon a target, as demonstrated by the attack, named Mirai, on the service provider DynDNS in 2016, which was of such a scale that it caused notable impact on services such as PayPal, Twitter, Reddit, GitHub, Amazon, and Netflix (Nixon et al., 2016). No DDoS carried out by the SEA or the OBL Crew were of a sufficient size to cause a level of impact comparable to Mirai, itself an attack carried out by a non-state actor; most likely a member of an online hacking community seeking to demonstrate an exploit that might later be offered for sale (Nixon et al., 2016).

Cyber-terrorist groups, as unwitting securitising norm entrepreneurs, are obviously not involved in the shaping of the same set of international norms that will be held by states and institutions, used to define and inform policy and legislature designed to restrict, punish, or control the risk of cyber-terrorism. The norms to which they are unknowingly contributing are those which will instead inform the less restrictive, but still not unlimited, norms of acceptable action and interaction of terrorist organisations and their use of cyber-capability. Despite contributing to different sets of overlapping norms, there is a definite relationship between the two, one which will be examined in greater depth in the final section of this chapter. One shared feature between these two groups relates to the nature of norm securitisation as explained in the first chapter of this thesis. The success of a state's move towards the securitisation of a norm is not based upon the veracity of the existential threat used to justify this shift. It instead rests upon whether the target audience – the general public – accepts and thus internalises this securitising logic. Such a relationship is reflected in the manner in which

terrorists employ and then publicise either direct cyber-attacks or cyber-capability-enabled attacks.

Our previous analysis has shown that the OBL Crew and the SEA employ relatively ineffective attacks, demonstrating a relatively low level of internal technical knowledge through the reliance and repeated utilisation of pre-made malware tools bought on the black market. The technical prowess – or lack of it – is not what provides the simultaneous impetus to the terrorist's cause and to the securitised set of norms to which these attacks and their associated management relates. Much as with state-centric norms, the success of an act of terrorism – and the contribution to terrorist-oriented norms which coincides with these acts – rests upon the impact on and the reaction of a shared target audience: the general public. Any act of cyber-terrorism, then, must be framed in a manner which maximises the instillation of fear within this target audience.

Figure 1, above, demonstrates how the terrorist role in the construction of terrorist-oriented norms regarding cyber-terrorism is cyclical in nature. There are several components: a public fear of the technological unknown; the threat of acts of cyber-terrorism; an act of cyber-terrorism; and the claim of responsibility and amplification of that attack. These components all feed into a recurring cycle which blends discursive and operationalised methods of norm construction to provide maximum impact of the act of cyber-terrorism in progressing the group's goals. Concurrently, this also facilitates the construction of a repeating, cyclical process of norm construction which, with every successful completion of a cycle, further reaffirms the set of terrorist-oriented norms which justify and perpetuate this form of attack by existent terrorist organisations and emergent groups.

To give evidence of this process I will turn again to the three case study groups: al-Qaeda, Anonymous, and the SEA. The SEA presents a number of examples of instances where it contributes to both the discursive and the operationalised components of this cycle of norm construction for cyber-terrorist norm sets. This cycle consists, in its perfect and most normatively effective form, of a series of discursive and operationalised elements of norm construction. All of these depend upon and enhance a state of public fear regarding the risk of cyber-terrorism. The operationalised component in the case of the SEA is provided by actual attacks against the group's targets which employ cyber-capability, such as the hijacking of the Associated Press's Twitter account and the social media accounts of President Obama. The discursive elements, both those carried out prior to and following these operationalised components, relate to the group's threats, claims of attribution, and statements amplifying the impact of these attacks. Terrorists, as accidental norm entrepreneurs, maximise the impact of

their operationalised acts of norm construction through the supplementation and augmentation of these acts through discursive methods: directing threats, news releases, and statements at their intended audience through social media accounts and other direct channels of communication (Melki and Jabado, 2016, p.94).

Figure 2: Syrian Electronic Army (Official_SEA16), 3 April 2015, 6:38 p.m. Tweet.

The SEA has only a limited ability to communicate threats to its target audience. Although the use of social media has, to an extent, allowed for terrorist organisations to circumvent previous routes of communication that relied upon news media intermediaries (Bertram, 2016, p.227), the group's Twitter presence and Facebook presence with regards to reaching beyond its supporters is limited by both the utilisation of Arabic as the dominant language employed and its relatively small following on both platforms. A common theme of the group's English-language tweets is to either reiterate and emphasise the impact of its previous attacks, or to retweet messages or links to articles or other material that frame the SEA itself as a significant threat with a high level of technical capability. An example being the tweet shown in Figure 2.

The article linked to in this tweet, as previewed on Twitter, appeared with the title 'The Syrian Electronic Army's Most Dangerous Hack'. The title of this article alone suggests that the group

poses a serious threat to those whom it targets. This impression is further emphasised by the reference to military plans being leaked: it suggests that the group possesses a level of capability which allows it to pose a threat to militaries, themselves associated with security and power. This tweet acts as a discursive amplifier to the operationalised component of this norm construction process signalled by the attack itself. By framing this relatively limited attack as successfully making a military organisation its victim, it suggests to the audience receiving this media that the SEA is more powerful, at least in terms of cyber-capability, than its military rivals.

A further relationship between the operationalised component and discursive component of cyber-terrorist norm construction links back to the earlier assertion that the reality of high-level cyber-capability is less important with regards to the efficacy of acts of cyber-terrorism and the simultaneous impact on norm construction than the appearance of that capability. The SEA and other groups, by targeting large corporations, states, and militaries, lend credibility to the impression that the groups' cyber-capability is far more dangerous than the reality.

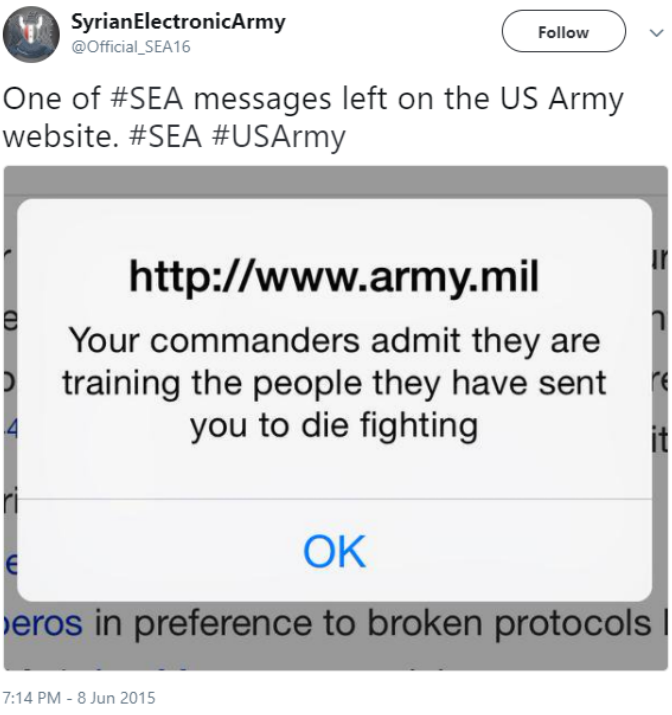


Figure 3: Syrian Electronic Army (@Official_SEA16), 8 June 2015, 7:14 p.m. Tweet.

The tweet shown in Figure 3, including a screengrab from a publicly accessible web page owned by the US military, exemplifies how the SEA utilised a discursive method alongside a specifically chosen target for the operationalised component in order to amplify the impact of its act of cyber-terrorism. This, in turn, results in the increased credibility for a normative position of cyber-terrorism that incentivises and legitimises this method of terrorism.

Anonymous provide another example of a group that, through a process involving discursive and operationalised methods, contributes to the norms of cyber-terrorism. Anonymous is commonly referred to as a hacktivist collective (Coleman, 2015). Indeed, it can be considered as the prime exemplar of a group which fits the definition of this term. Such terminology comes with a return to the old catechism concerning how one person's terrorist is another's freedom fighter. The methodology in that case, as in this, is often the same. For the purposes of this chapter we are considering the implications of cyber-attacks upon the construction of norms; Anonymous's ideological position may well impact upon the level of input into this normative process that the group's actions have; however, such an analysis falls outside the scope of this thesis. What can be noted, however, is that Anonymous engages in the same cyclical and cumulatively recursive process of norm construction through its actions as the SEA, al-Qaeda, and indeed any other pre-existent terrorist organisation that subsequently turned to cyber-capability to achieve its goals.

By considering the collective OPIsrael campaigns that were previously mentioned, we can extract evidence of discursive elements of norm construction – prior to and following the attacks – as well as the operationalised component – that of the attacks constituting this campaign. The discursive elements in this case consist both of threats which portray an inflated presentation of the damage the group can achieve and claims of success which similarly exaggerate the actual effects. Prior to the 2013 iteration of OPIsrael, CNET reported on a now inactive Anonymous-affiliated Twitter account stating that the upcoming attacks would "disrupt and erase Israel from cyberspace" (Musil, 2013). During the attack itself, in that same year, various Twitter accounts managed by the loosely-affiliated group released statements that sought to quantify the damage being done to Israeli digital infrastructure. Some of these drew particular attention to websites taken offline by DDoS attacks:

> Anonymous (@YourAnonNews)
> Anonymous Operation Israel | Target: Down | mod.gov.il | #Anonymous #OpIsrael #FREEPalestine #Revolution (7 April 2013, 12:24 p.m. Tweet)

This tweet, similarly to the previously cited example from the SEA, draws attention to the fact that the group has apparently taken down the Israeli military's web page. The attack (the operational component) is designed to maximise the appearance of threat to the public, and thus their potential for fear. Choosing the military as a target provides the material for a simple act of discursive norm construction – in the shape of a tweet – that not only serves to amplify the potential for fear generation in the target audience, but by so doing enhances the

efficacy of the normative signalling contained within this entire cycle. Another example of this, with a slight difference, can be seen in the following tweet, also relating to the same Anonymous series of attacks against Israel in 2013:

> #OpIsrael (@Op_Israel)
> #Anonymous partial damage report, 100k websites, 40k Facebook pages, 5k twitter & 30k Israeli bank acc got hacked ~ $3-plus billion damage (7 April 2013, 5:52 p.m. Tweet)

More general messages, such as this tweet, serve a similar end; in this instance the numbers acting as the feature which is meant to amplify the perceived power of the terrorist organisation and simultaneously the legitimacy of its normative position. Each discursive component contributes to the overall efficacy and the momentum of repeated recursions of the cycle. If an attack is deemed a success in cultivating or producing fear in the public then it increases the likelihood that a similar act will be repeated. In each instance we also find that the operational component is the foundation of the constructive cycle. While there is a relationship between the attack itself and the discursive elements – be they the precursory threats or the acts of amplification which follow – these are dependent upon the existence of an operational component. The attack that constitutes this act does not necessarily have to result in significant damage or impact against the target, it simply needs to have the capacity to be framed in a manner that gives the appearance that it has. This feature can be further exemplified in instances where groups seek to apply their own discursive acts to another actor's operationalised component; claiming responsibility for and concurrently amplifying a cyber-attack which they themselves did not carry out.

Examples of this can be seen by returning to the Mirai DDoS attack that was mentioned earlier. Taking place in October 2016, this attack was – at the time – one of the largest DDoS ever recorded and had significant impact upon some of the most in-demand internet-based services. Targeted at DynDNS, this attack managed to degrade the service of this key service provider, leading to severe slowdowns or complete downtime for sites including Twitter, the Guardian, Netflix, CNN, and Reddit for users in the USA and Europe (Woolf, 2016). This attack was so named for its use of the Mirai botnet, itself unique in that it included a large number of Internet of Things devices among the infected devices used to power its attack. Notably, two groups claimed responsibility for this attack on Twitter while the group believed to be most likely behind the attack after further analysis only discussed the attack on closed forums (Nixon et al., 2016).

WikiLeaks released the following message via its Twitter account, claiming the attack as being the responsibility of its supporters as a response to the treatment of WikiLeaks and especially its head, Julian Assange, who faced the possibility of extradition and trial in the USA.

> WikiLeaks (@Wikileaks)
> Mr. Assange is still alive and WikiLeaks is still publishing. We ask supporters to stop taking down the US internet. You proved your point. (21 October 2016, 10:09 p.m. Tweet)

This act of rhetorical norm construction allows WikiLeaks to appropriate the impact of the actual attack for its own ends. The normative impact of both the operationalised stage of this process of construction remains, the claim of responsibility from WikiLeaks and the manner in which its language amplifies the impact of the attack serves as further legitimisation of the cyber-terrorist's set of norms. In effect, overlapping claims of responsibility and amplification serve the group's interest by suggesting to an audience a greater power or influence than it in fact holds and, at the same time, form a supplementary act of norm construction.

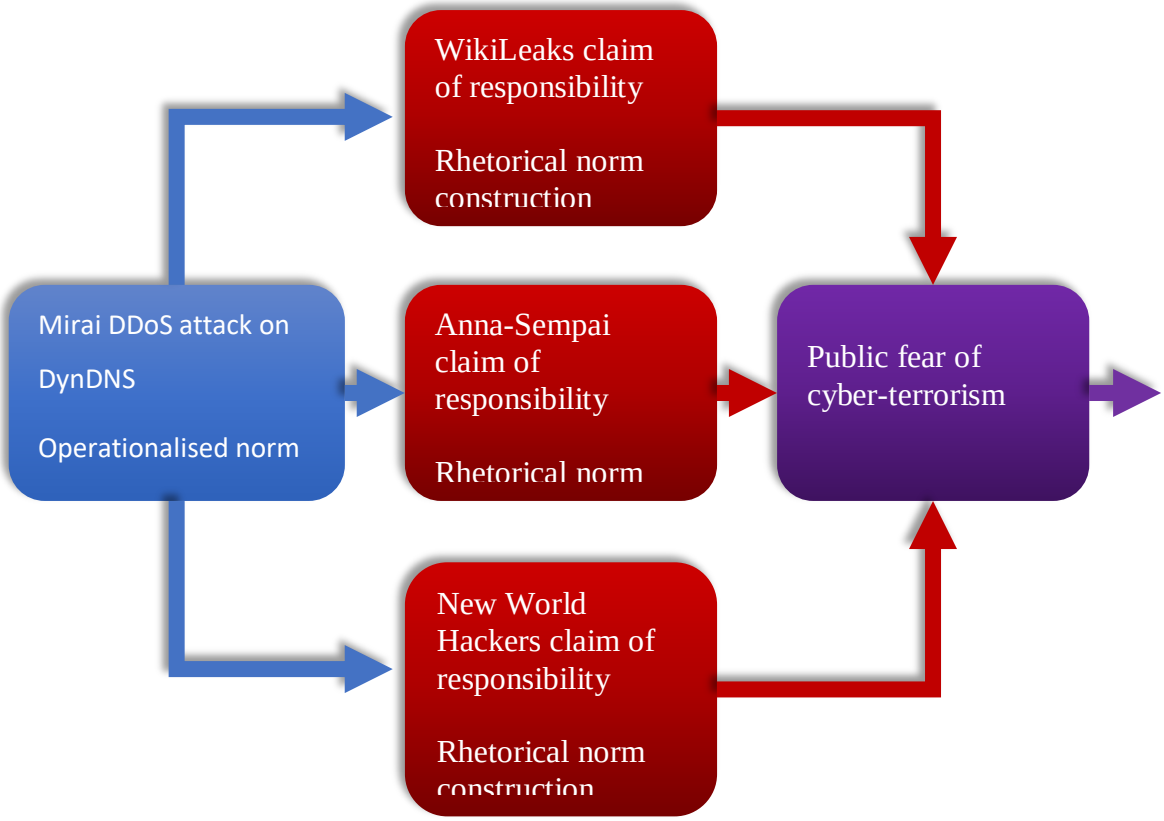


Figure 4: Branching rhetorical norm construction case study – Mirai DDoS.

The Mirai attack against DynDNS was also claimed by another group – New World Hackers. This group's claim of responsibility, shown in the tweet below in Figure 5, essentially results in there being three concurrent instances of rhetorical norm construction branching off from one operationalised foundation (see Figure 4).

Figure 5: New World Hackers (@NewWorldHacking), 21 October 2016, 5:40 p.m. Tweet.

None of these attacks have resulted in particularly long-lasting damage, the majority being quickly mitigated with the flaw which enabled them being patched soon after. The Mirai attack against DynDNS was eventually routed through a service designed to deflect DDoS, resulting in user access to affected services returning to normal in less than a day (Nixon et al., 2016). The effectiveness of cyber-terrorists, both towards their political goals and as norm entrepreneurs, is not relative to the amount of damage that their attacks cause. It is dependent upon how serious that damage, and the threat of future attacks, is made to seem by the audience at which it is directed. Successful progress towards the group's political goals is achieved through the use or claim of responsibility for a cyber-attack – the majority of which cause very little real damage – augmented by the framing of this attack as more than it in fact is. The rhetorical amplification of a minor attack concurrently cements the set of norms referent to terrorist organisations that supports the continued use of these methods as capable of creating a fear-inducing spectacle with minimal cost.

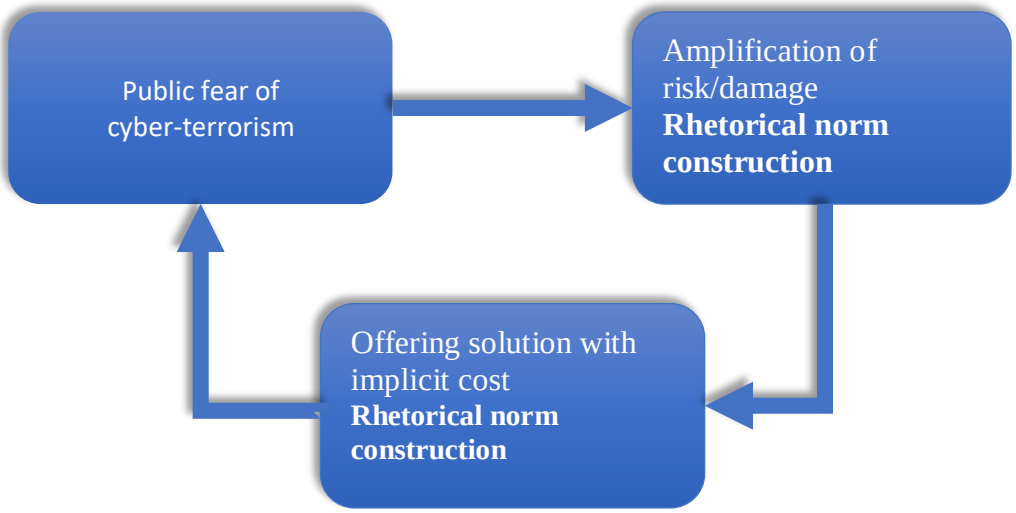


Figure 6: The cycle of cyber-terrorism norm construction: the state's role

The purpose of norm securitisation, from the perspective of the state norm entrepreneur, is to produce a position in which an elevated response in terms of policy and resources can be dedicated to the issue in question. Buzan and the Copenhagen School in general describe this shift as pejorative in nature, serving to justify policy and the expenditure of resources that would never be justified without the allusion to an existential fear created for this purpose (Buzan et al., 1997, p.23). Such a logic ascribes an absolute concept of right that is perhaps limited by its failure to consider the concept of whether, in some cases, the ends might justify the means.

While the conclusions as to how norms of cyber-surveillance were constructed demonstrated in Chapter 3 of this thesis might be taken to support the Copenhagen School's position, I would argue that possibility of the misuse of securitisation is dependent upon over-extension or misjudgement, it is not a move which is without exception an unequivocal grasp for greater state power. Waltz, in *Theory of International Politics*, notes that "states will ally with the devil to avoid the hell of military defeat" (Waltz, 2010, p.166). Waltz proposes a defensive form of structural realism that suggests that states prioritise security above all else: attempts to accrue power, through policy, norms, or the development of military capability, are all aimed at maximising the security of the state. Increased powers of surveillance, bundled alongside greater control over digital content and the development of offensive and defensive military

cyber-capability are, if considered as efforts to ensure state security, themselves not instinctively immoral. The problem arises from the method in which they are constructed and the extent to which they represent an overextension towards security at the cost of an unequal impact to concepts of human security such as privacy.

Securitisation can be embarked upon in order to prioritise issues that are in need of attention and resources that have not naturally been allocated by *normal* politics. The securitisation of climate, for example, can be argued to be a necessity; the only way to ensure that an otherwise under-resourced issue which poses a genuine existential threat is given the attention – domestic and international – that it requires. The issue with securitised norm construction when it comes to the state-centric set of norms regarding cyber-terrorism is that the threat lacks the legitimacy that might be provided by a truly existential threat. Thus, the prioritisation allocated to it as a result of successful securitisation and it therefore loses its lustre under detailed scrutiny.

The norm construction relative to sets of state-oriented norms of cyber-terrorism provides the perfect case study to demonstrate an example of when norm securitisation is directed and employs a process of amplification to a risk which doesn't in fact pose an existential threat. Unlike the role played by cyber-terrorists as norm entrepreneurs, states play a purely rhetorical role in the construction of cyber-securitised norms. While cyber-terrorist actors supplement their operationalised norm constructive actions, states only engage in rhetorical forms of norm construction. Furthermore, these rhetorical instances of norm construction engage in amplification in a manner identical to that of the cyber-terrorist actors.

States, in effect, have their own cycle of cyber-terrorist norm construction (see Figure 5). The existent state of public fear over technological unknowns in relation to cyber-terrorism again serves as the starting point, into which each cycle contributes its norm shaping input. In the case of states, the two other components of this cycle are: firstly, the amplification of the risk or the damage caused by acts of cyber-terrorism; and secondly, the offering of a solution which necessitates a trade of freedoms for security.

Both of these components contribute to the continued existence and the heightening of public fear surrounding new technology and the insecurity potentially implicit with the reliance on it. The aggrandising of the risk or impact of cyber-attacks is an act solely motivated by the goal of supporting a normative position that grants the ability to legitimise their securitisation act relative to – what appears to be – a serious threat. The second of these rhetorical acts of norm construction, however, is better understood as an unintended consequence of an attempt to

immunise the securitised norm that is being produced from the challenge that might be created by a counter-narrative. Such a concept is considered in greater detail in Chapter 3 of this thesis, regarding cyber-surveillance, and will be reiterated in this section.

Threats versus reality 2.0: inflating the risk

A previous chapter of this thesis considered the manner in which states, in particular the UK, have employed facilitating conditions – often coming in the shape of various terrorist attacks – to invoke or demonstrate the existence of a threat which the public should be afraid of. Chapter 3 of this thesis – considering the norm construction of state cyber-surveillance – drew upon particular debates surrounding the Investigatory Powers Act 2016, the Regulation of Investigatory Powers Act 2000, and various other pieces of British legislation that showed evidence of the construction of a securitised norm on which this legislation's legitimacy could rest. While this chapter provides numerous examples of facilitating conditions which are then amplified for this purpose, the following two sections will attempt to broaden the pool of cases employed to consider this issue.

The first of these will examine the framing of encryption as it relates to its potential to enable acts of terrorism. I will examine how the framing of this technology within public political discourse about terrorism is conducted in a manner which aims to inflate the danger posed by encryption, over-stress the cyber-component of actual acts of terrorism, and thereby legitimise the securitised norm underpinning policy which would otherwise prove contentious.

Encryption is a tool which can, at best, be considered to enable or enhance a terrorist group's ability to organise, prepare, or carry out an attack; it is not, in itself, a technology which causes harm. Despite this, there are a number of notable instances where this technology has been singled out specifically as representing a threat through its potential as a means of communication for terrorists. Besides its particular mention as posing a risk, the language employed when framing it as such further amplifies the actual threat it poses, and cyber-capability of terrorists in general poses, to the state or its publics.

The last two Prime Ministers of the UK have made public statements regarding encryption, both framing the technology as posing a significant risk to the public in the manner that it undermines the ability of security services to intercept the communications of terrorist groups and thus prevent attacks. In the wake of the terrorist attack on Paris in January 2015 targeting the satirical magazine *Charlie Hedbo*, which saw 12 people murdered, David Cameron made the following statement referencing the need to close down means of communications for terrorists that the security services could not access:

In extremis, it has been possible to read someone's letter, to listen to someone's call, to mobile communications… The question remains: are we going to allow a means of communications where it simply is not possible to do that? My answer to that question is: no, we must not. The first duty of any government is to keep our country and our people safe. (Cameron in Watt et al., 2015)

The implication of this statement is that encryption, and its use by terrorist groups such as the one responsible for the attack on *Charlie Hedbo*, is a source of insecurity. The technology is, by this statement, framed as the source of a serious threat – serious due to its connection to terrorism – which, unchecked, could result in a repeat of the events in Paris. In this instance, Cameron has taken the facilitating condition of a recent and prominent terrorist attack, highlighted a component of it which relies upon the internet, and then amplified the risk which this component poses to the public.

Acts of rhetorical securitised norm construction such as this were further repeated, in a strikingly similar formula, by Cameron's successor and her Home Secretary. Amber Rudd, who took the position of Home Secretary after her predecessor Theresa May became Prime Minister, once again raised the topic of encryption as a specific risk in the wake of the terrorist attack on Westminster Bridge in London in 2017. Rudd invoked near identical language to Cameron two years earlier, stating that "You can't have a situation where warranted information is needed, perhaps to stop attacks like the one last week, and it can't be accessed" (Jukes, 2017). May further added to this after the June 2017 terrorist attack on London Bridge in a speech delivered on the steps of Downing Street.

> We cannot allow this ideology the safe space it needs to breed – yet that is precisely what the internet, and the big companies that provide internet-based services provide… We need to work with allied democratic governments to reach international agreements to regulate cyberspace to prevent the spread of extremist and terrorism planning. (May in Stone, 2017)

The language and the timing of the statements of these three politicians, directed at a public audience, are almost identical. They are evidence of the knowing construction of encryption and the spectre of *cyber*-terrorism – or at least cyber-enabled terrorism – as a severe threat, directly responsible for acts of terrorism that have resulted in loss of life and physical harm. Cameron, Rudd, and May have all taken what is actually a minor component of what was otherwise a typical act of terrorism and inflated its importance within the public discourse through a rhetorical act of norm securitisation: a speech act. As a part of the creation of a

securitised normative basis for a set of policies directed at the internet companies mentioned by these politicians and seeking to grant greater powers regarding interception of communications data, these allied norm entrepreneurs have engaged in an act of rhetorical norm construction. This process contributes both to the specific norms regarding cyber-surveillance and those of state powers of surveillance, and to the broader state-centric set of norms relating to cyber-terrorism. This amplification of the danger posed by cyber-terrorism is, however, reliant entirely upon there being some form of operationalised norm construction at the hands of a terrorist organisation – an act of terrorism within which some relation to cyber-capability can be found, highlighted, and ultimately used as the driving force for a series of rhetoric-based acts of securitised norm construction which can encompass the intended set of policies.

Offering salvation: security at a cost

As previously noted, states not only engage in a rhetorical act of securitised norm construction through the amplification of risk or damage relating to cyber-terrorism – an intentional contribution to the full cycle of cyber-terrorism norms – but there is also a secondary, unintended contribution which stems out of attempts to inure their preferred norm from potential challenge. While I suggest that this component of the norm construction process is unintentional, that does not mean that it does not have a favourable impact upon the resilience and successful legitimisation of this norm by its intended audience. The amplification of the risk posed by an act of cyber-terrorism is solely intended to justify the shift towards a securitised normative position. However, the cost implicit in the means offered to secure against this new, dangerous form of terrorism are a less explicit rephrasing of the initial amplification of threat. One which occurs as a secondary feature of the imposition of the policies which the entire process of norm securitisation is meant to justify.

The case study I have chosen to employ for this section returns to the analysis found in Chapter 3 of this thesis. The manner in which the UK government, over an extended period, securitised and then reaffirmed the securitisation of norms which allow the digital surveillance of their population provides numerous examples of how the solution offered to mitigate against a source of public fear itself designates a cost and thus reiterates the level of threat. As demonstrated in Chapter 3, the UK's securitisation of digital surveillance has relied heavily upon the presentation of risk to certain groups that there is an implicit moral duty to protect. Most commonly, public fear is directed towards a risk posed to children (HC Deb 29 November 1999, vol 340, col 43; HC Deb 13 March 2000, vol 346, col 10; HC Deb 10 July 2014, col 456; Cm

7586), the nation as a whole (HC Deb 14 January 2015, col 869; HL Deb 19 June 2003, col 275; HL Deb 19 June 2000, col 16), or in some cases the fundamental nature of our society. Linking the threat of cyber-terrorism – even when the cyber component is only minor – to the reason that these groups or issues are threatened amplifies the threat. However, the norm entrepreneurs, in this instance a series of UK governments, engage in a secondary act which aims to fortify this process of securitised norm construction.

The most effective method by which this act of securitisation might be challenged would be to demonstrate that the cost, in regard to the undermining of existing liberties or rights, outweighs the security that will be achieved through the solutions proposed by the securitising norm entrepreneur. With regards to cyber-surveillance as a subsidiary of state-centric cyber-terrorism norms, this could take the form of a competing norm entrepreneur – one in favour of a de-securitised normative position – seeking to demonstrate to the relevant audience the specific implications of allowing legislation such as the Investigatory Powers Act 2016 to come into force. This challenge can be and is often pre-empted by state norm entrepreneurs as part of the cycle of cyber-terrorism norm construction.

In the UK, the announcement of a consultation into codes of practice contained within the draft Investigatory Powers Act 2016 by then Minister for Security Ben Wallace provides an example of this pre-emptive norm-fortifying act of rhetorical norm construction:

> It radically overhauls the way these powers are authorised and overseen. It introduces a 'double-lock' for the most intrusive powers, including interception and all of the bulk capabilities, so that these warrants cannot be issued until the decision to do so has been approved by a Judicial Commissioner. And it creates a new Investigatory Powers Commissioner to oversee how these powers are used…
>
> The Act provides world-leading transparency and privacy protection. It received unprecedented and exceptional scrutiny in Parliament and was passed with cross-party support. There should be no doubt about the necessity of the powers that it contains or the strength of the safeguards that it includes. (HC Deb 23 February 2017, c 38WS)

In this statement Wallace implicitly attaches a cost to the powers being granted through this process of securitisation. Terms such as "double-lock" and references to world-leading privacy protection, when combined with how the necessity of these powers is beyond doubt – again referencing the level of threat they seek to counter – effectively undermine attempts to

counter the securitised norm through alluding to its negative impacts upon the individual. Any attempt to do so can then be met with the pre-supported counter-argument that the cost may be high, but it is one that has already been considered and found to be acceptable when balanced against the risk.

Reported in the *Guardian* newspaper, a further iteration of this component of the norm construction can be noted in a statement on this same Act by Home Secretary Amber Rudd:

> The Investigatory Powers Act is world-leading legislation, that provides unprecedented transparency and substantial privacy protection. The government is clear that, at a time of heightened security threat, it is essential our law enforcement and security and intelligence services have the power they need to keep people safe. The internet presents new opportunities for terrorists and we must ensure we have the capabilities to confront this challenge. But it is also right that these powers are subject to strict safeguards and rigorous oversight. (Rudd in Travis, 2016)

Once again, the language contained in Rudd's support of the Investigatory Powers Act 2016 begins with a reference not to the explicit civil liberties issues arising from its empowerment, but instead implicitly alluding to them while pre-emptively explaining that the Act – itself a product or symptom of the securitised norms which her government supports – has already solved these problems. This is an effective rhetorical act of norm construction that at once furthers the necessity and legitimacy of the normative shift of which the government is in favour, while at the same time further feeding into the public fear of what has been framed as cyber-terrorism. The fact that the powers granted in the Act are such that they must be counter-balanced within the same Act to ensure that it "provides unprecedented transparency and privacy protection" (Rudd in Travis, 2016) further contributes to a cycle of norm construction which relies upon the amplification of both the cyber component and the level of the threat at which it is targeted.

It must lastly be noted that this form of amplification of threat, through the provision of cost – although potentially an unintentional or secondary outcome resulting from attempts to secure the preferred norm – is just as reliant upon the acts of norm construction employed by the terrorist actors themselves as its more definitively augmentative counterpart. Without the actual attacks, complete with whatever level of cyber-capability they employ, the acts of rhetorical norm construction embarked upon by the state would have nothing which they could amplify. They would have no evidence of cyber-terrorism that could be inflated beyond its natural importance, nor would they have a fear on which to build. This suggests that not

only is the state's role in the construction of its own norms of cyber-terrorism reactionary to the material provided by terrorists, but that rhetorical norms themselves suffer the same limitation.

Conclusion: the complementary cycle of cyber-terrorism norm construction and the necessity of operationalised norms

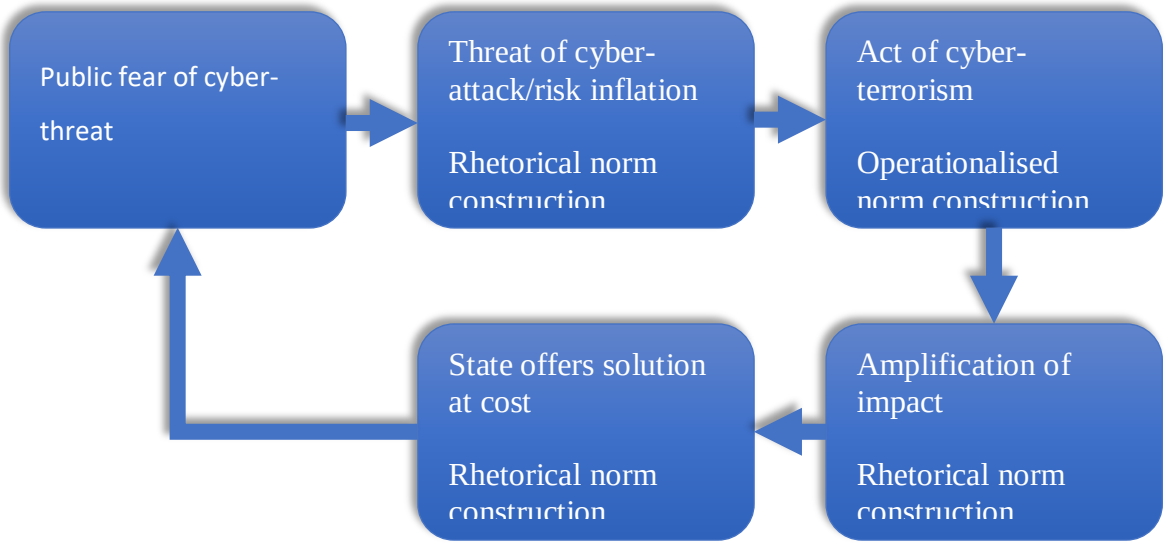


Figure 7: The cycle of complementary cyber-terrorism norm construction.

In Figure 6, above, I have demonstrated how the inputs of both terrorists and states into the construction of their overlapping norms regarding cyber-terrorism complement each other. They serve to create a single cyclical and recursive process which, with the successful completion of each component, both contributes to the public's fear of cyber-terrorism and justifies the normative position of both state and terrorist. For the terrorist, each stage – be it one fulfilled by themselves or the state – furthers their chances of achieving a political goal through the incitement of fear while, in parallel, cementing the normative position that encourages the expansion of the cyber component of their efforts and those of other terrorist actors more generally. Concurrently, for the state, the state of fear which each component of this cyclical process contributes to, and each subsequent completion of the full cycle, provides further justification and legitimisation for the securitised normative position that allows for policies granting powers over emergent technologies, methods of communication, and internet-based industry.

This complete cycle can be separated into two sections, this divide relating both to the norm entrepreneur involved within the components contained in each section and the order in which this cycle operates. This final analysis will consider these two sections in turn before finally examining them as a single entity; beginning with the section which concerns the components in which the norm entrepreneurs contributing are the terrorist actors, before addressing those components wherein the state is a contributing norm entrepreneur.

Terrorists, as norm entrepreneurs regarding cyber-terrorism, are involved in the process in three of the five components which I have extrapolated. They are the sole contributors to the first and second stage and have an equal potential input into the third stage, alongside state norm entrepreneurs. With regards to the methods of norm construction employed, terrorist actors as norm entrepreneurs employ both rhetorical or discursive norm construction as well as operationalised norm construction. The former found – as previously described through the case studies of the SEA, Anonymous, WikiLeaks, and others – in claims of attribution, threat of attack, or statements amplifying acts of terrorism which contained the application of cyber-capability, however limited. The latter is evident in these attacks themselves. The attacks detailed in this chapter, those carried out by the SEA, Anonymous, and al-Qaeda, as well as those simply claimed by WikiLeaks, New World Hackers, or other opportunistic groups, provided one of the two core components upon which the rest of this cycle of securitised norm construction depends.

The discursive or rhetorical acts of norm construction that terrorists contribute to their respective components of this cycle of securitised norm construction rely both upon the natural fear with which humans regard the unknown – with technology itself presenting as an unknown risk – and acts of terrorism which contain an element reflecting this fear of technology. The role of cyber-capability in any given attack need not be, in actuality, central to the target, nature, or success of the attack: it must only have the potential to be framed as such. In a similar vein, attacks which do rely solely upon cyber-capability do not need to be complex or inflict serious damage. The seriousness of these attacks, as measured by the audience towards whom they are directed – this being the general public – is based more upon the efficacy of the amplification of these attacks and the risk posed by whatever element of cyber-capability is employed. There exists, then, within the terrorist related components of this norm construction cycle, a symbiotic relationship between operationalised contributions to the normative process and their rhetorical cousins. However, this relationship still contains a greater reliance upon the operationalised component, without which there would be no foundation upon which discursive or rhetorical acts of amplification could be built.

The amplification component of this cycle differs from those preceding it in that it is contributed to by both terrorist norm entrepreneurs and state norm entrepreneurs. This discursive, rhetorical element of norm construction is engaged in both by terrorist actors and by states. Terrorist actors do so in order to maximise the impact of the operationalised component provided by their or another group's act of cyber-terrorism. States, on the other hand, engage in this rhetorical and discursive act of norm construction in order to maximise the securitising power provided by a facilitating condition – this same act of cyber-terrorism – towards the construction and institutionalisation of the securitised norm set which they champion. The rhetorical, discursive forms of norm construction embarked upon directed towards this component of the cycle could be referred to as *norm multipliers* – comparable to the term force multiplier within military contexts. In effect, within this component, two groups which by their nature would be expected to be in direct competition with each other in fact engage in acts of norm construction that not only bear striking similarities to one another in structure, language, and purpose, but also, in fact, serve to aid in the realisation of each other's goals. The more spectacular and impressive the act of cyber-terrorism and the more central its cyber component, the easier it is for state actors to employ this operationalised act within their own efforts of norm construction. When a terrorist actor employs this norm multiplier, by its nature this act seeks to create a spectacle; theatre where the audience is the general population and the intended response is one of fear and horror. State actors within this securitised norm construction cycle seek the same goal, employ the same methods, and build upon the same operationalised acts; this component then is a complementary stage, with two opposed actors effectively assisting each other in reaching their goals.

Finally, the position and nature of the components of this cycle entirely beholden to state securitising norm entrepreneurs provide further support to the hypothesis that with regards to cyber-terrorism norm construction – and securitised norm construction in general – discursive or rhetorical norms are not only predominantly secondary in terms of their temporal placement within the process, but they are also dependent upon the existence of an operationalised norm construction component within the process. Without this active form of norm construction, the rhetorical or discursive forms upon which states commonly seek to rely in the forming of securitised norms would be severely limited. Both components that fall entirely within the remit of state norm entrepreneurs – amplification and solution offering – employ a discursive form of norm construction. While it might be possible to both create and inflate a threat which does not bear any relation to an actual instance of cyber-terrorism, such an attempt at norm securitisation is far more likely to fail as a result. Without some

component of truth the potential for the target audience to accept the necessity of a shift to securitised norms and their related policy is seriously limited.

In conclusion, the norms of cyber-security with regards to cyber-terrorism are constructed through a shared duality. Both rhetorical discursive acts of securitised norm construction and the operationalised form elucidated by this thesis are in evidence. These two methods of norm construction are complementary to each other, both serving to take advantage of and heighten a pre-existent state of fear in order to enhance the chances of a successful internalisation of the norms that the two groups of norm entrepreneurs involved represent. However, not only do these two sets of norms ultimately seek alternative end goals, each seeking the annulment of the other, but the terrorist actor's position in the normative cycle provides it greater leverage in shaping the end result than the state actor's. Discursive and rhetorical norms, the sole methods employed by states in this process, are not only employed after the operationalised and rhetorical inputs of the terrorist norm entrepreneurs, they are also dependent upon them. Thus, discursive and rhetorical norms – whomever employs them within this cycle of securitised norm construction – are reactive; limited by nature and dependent on the proactive operationalised form of norm construction.

Chapter 7 – Conclusions

Cyber-security: the need for a new approach

The goals of this thesis were to expand upon current literature and discussion through analysis of the nature of international and domestic norms, and how they are constructed in relation to issues arising from cyber-security. This thesis has sought to examine the way that norms are constructed with regards to several issues composite with cyber-security specifically. In doing so it aimed to offer insight into methods of norm construction and the actors involved, focusing on the security component of these norms. My intention in analysing how actors shape cyber-security norms has been to demonstrate the concept of operationalised norm construction which, in spite of being evident in historic examples, has previously been paid little attention in academic literature. Finally, it has been the aim of this work to demonstrate the power vested in securitised norms and the processes of their construction which makes them both more effective and more resilient norms; this in turn explains the popularity of this method of construction by norm entrepreneurs.

Cyber-security is not just a buzz word, popular with new media and politicians seeking to demonstrate their understanding of how rapidly developing technological innovation has impacted social structure and phenomenon. Nor is it merely a subject of abstract academic discussion, with limited contextual relevancy to current affairs and therefore with limited haste attached to the need to increase our understanding of it. The way cyber-security has come to hold such a dominant position in public parlance and the halls of political institutions and academic campuses is symptomatic of its actual relevance. The rapidity with which this field has gained purchase similarly reflective of both its prominence, and rapid acceleration into the security discourse of academics and pertinent actors. Our understanding of this reality is not served by literature and academic analysis which seeks to ascribe its own concepts upon those actors engaging directly with the phenomenon in question. When the literature on cyber-war centres around argument as to whether this form of military activity will or not take place - while the USA is destroying nuclear centrifuges in Iran (Cherepanov and Lipovsky, 2017), the UK is threatening Russia with its arsenal of cyber-weapons (Woodcock, 2017), and the German Bundestag is decrying yet another breach of its networked systems by another state (Murdock, 2017) - this literature is insufficient and cannot offer the understanding such circumstances require.

While this thesis has been directed at a subject specific context, cyber-security, the approach taken, and findings generated contribute to a wider theoretical discourse. In seeking to answer

the more relevant question of *how* various actors will engage with norms and issues of cyber-security rather than the out-dated question of *if* actors will engage with them, this thesis offers a range of contributions to the wider literature, particularly with regards to theories of norm emergence and securitisation. The analysis presented in this thesis has engaged with overlapping theories of constructivism. It has demonstrated how both norm emergence theory as detailed by Finnemore and Sikkink, and securitisation theory as proposed by Buzan and the Copenhagen School can undergo a process of hybridisation to synthesise a single theoretical framework; one which I have titled *securitised norm emergence* or *norm securitisation* theory. This framework has not only provided insight into the key aims of this thesis regarding the nature of cyber-security norms and their construction, it provides a model of analysis which can be applied beyond the narrow subject specificity of this work. The framework developed in this thesis offers potential insight into the actors, methods, and nature of any normative process wherein security can be considered.

Lessons learned: norms securitised and pro-active construction

Despite the thematic separation between the central chapters of this thesis the conclusions that each section has come to serve to contribute to a set of holistic theoretical concepts. The lessons learned from the thematic analysis of cyber-surveillance, cyber-war, and cyber-terrorism norms demonstrates the utility of both the hypothesised concepts of *norm securitisation* and *operationalised* norm construction. Together these can be offer a new mode of understanding the interaction of security and norm construction; covering both domestic and international norms and allowing for the inclusion of a variety of actors into analysis which were under previous models absent. The following sections of this conclusion will summarise these lessons.

<u>Securitised Norm Construction: the appeal to fear in norm construction</u>

One of the core aims of this thesis was to examine the way in which those involved in shaping cyber-security norms – norm entrepreneurs – were contributing to this normative process. Rather than seeking to solely consider the question as to whether governments, institutions or other actors were shaping cyber-security norms, this thesis aimed to demonstrate not only that this process was ongoing but to provide insight as to the means through which these normative positions were being constructed. Through the analysis of debate, political statements, and discourse related to the formation and enacting of digital-surveillance powers in the United Kingdom, several interconnecting conclusions can be reached which together contribute towards this goal.

The first of these conclusions was regarding the relevance of securitisation and its component concepts when considering the contents, structure and intentions of political discourse in the UK around cyber-surveillance norms. The connecting of facilitating conditions – events or external contexts – to the absence of the surveillance powers in question, when these events take the form of violent terrorist attacks, prominent and high level criminal activities, or the abuse of children presents a near perfect example of the means of securitisation which Buzan et al describe in their work. Similarly, the directing of this risk towards a group to which a responsibility to defend from risk is naturally ascribed provides evidence of another component of successful securitisation, the selection of an effective referent object. In the case of the UK and cyber-surveillance, my analysis notes that while the public in general is often used as a referent object to which risk is ascribed the most commonly employed – in political debate and public statements or discourse – is children.

After noting the significant evidence of discourse and political action intended to demonstrate existential threat and thereby justify securitisation, this thesis set out the divided positionality of norm entrepreneurs involved in this process. These could be broadly separated into those in favour of a securitised position, justifying an expansion of government powers of digital-surveillance, and those against this shift. The securitisation of this set of developing norms has had a polarising effect, resulting in a group of norm securitising entrepreneurs and a group seeking to counteract the securitising component which their opposition represents.

A secondary insight to be found in this separation of actors along securitised lines is the fact that this division was not only evident in the discourse or public political debate surrounding a single instance of policy, or legal framing contained within a limited period. Indeed, the polarised division of this normative position – in favour of securitisation or opposing it – can be discerned from discourse attached to a variety of policy positions that span the entire, almost two-decade, period at which this analysis was directed.

This conclusion leads on to one of the most notable and unexpected lessons which I have extracted from this analysis of cyber-surveillance and its norm development within the UK. The symptoms of securitisation are evident across this extended period, employed by the party in government to justify the need for the extension, retention or expansion of powers of digital-surveillance to which the British security services have legal recourse. During this same period however, there were numerous exchanged of party position within British government resulting from a series of general elections. The period considered for this analysis begins with a Labour majority government, replaced by a coalition between the Conservatives and the Liberal Democrats before finally transitioning one last time to a Conservative party majority.

This indicates that there is some feature of the position of government that results in the incentivisation of a securitised model of discourse for the justification of digital-surveillance. It is a remarkably stark insight to note that norm entrepreneurs that are one week employing language that equates digital-surveillance with an unjustifiable breach of individual privacy shift the next week, following a general election, to language which conflates the lack of digital-surveillance powers with an existential and often unsupported threat to the nation or its children.

Operationalised Norm Construction: seizing advantage in norm construction

On turning the direction of our analysis towards the issue of cyber-war, a similar series of complementary conclusions arise. These serve not only to support my hypothesis regarding *operationalised* methods of norm construction, but also contribute towards the overarching aims of this thesis by expanding our frame of reference as a result. This insight into the nature, potential use of and impact of operationalised norm construction through the analysis of developing norms of cyber-war is in no way limited to the study of this specific phenomenon. Both the conclusions as to the nature of securitised norm construction which were built out of the findings of the preceding chapter and those concerning *operationalised* methods of norm construction introduced in this fourth chapter can be carried over into examination of cyber-terrorism in the antecedent chapter. However, these conclusions also contribute towards the goal of providing a more complete picture as to the manner of security orientated norm construction of cyber-security issues, and of security centric norms in general.

This chapter began with an attempt to contemporise the definition and conception of war and warfare. This was done with the aim of producing a more accurate understanding of how the norms of cyber-war and cyber-warfare might stand, and how they might have been shaped and continue to be shaped by interested parties. With this goal in mind the fourth chapter of this thesis once again selected a case study, one that might allow for a more deductive picture as to how states view and employ methods of cyber-war and thus offer insight into how war might need to be redefined. Russia provided a great deal of evidence to suggest that, despite their fundamental disagreements regarding the potential existence of cyber-war, both Rid and Stone were wrong in their conclusions. The former's conclusions that cyber-war would not take place (Rid, 2012) failed to consider an expanded concept of violence which was a component of the Clausewitzian conception of war, forming the bases of his analysis. The latter, while concluding that cyber-war could take place, had failed to consider that war as a concept should best be considered through the lens of those actors who go to war.

The first, and perhaps most fundamental finding of this chapter was not that cyber-war will or will not take place based upon an often misinterpreted or misapplied definition of war. Rather it is that the conception of war and its norms, contained and exemplified by international legal frameworks and doctrine with which we have previously used to formulate this definition, have been demonstrably proven to be insufficient. War, quite simply, has changed. Russia's dramatic realisation of the potential of psychological or information warfare, as enabled through the matched pairing of technological dependence and its innate insecurity, act as evidence for the fundamental shifting of the boundaries of what has previously been considered war. Not only are those countries affected by Russian cyber-attacks such as Georgia, Estonia and Ukraine referring to these attacks as symptomatic of a new form of war; states which have fallen victim to non-violent, indirect campaigns of misinformation or psychological warfare directed against their citizenry are making similar assertions. Through the medium of social media and diffuse new online sources, Russia has achieved what Sun Tzu, the ancient Chinese general, would ascribe as a perfect victory; one without any fighting. Russia has redefined war to encompass information or cyber-war; in so doing it has contributed to the construction of a set of norms in direct opposition to those still held by states which continue to define war in a manner now rapidly shown as outdated and falling behind.

These new norms of war and warfare encompass a model of cyber-war which includes cyber-espionage, and the leveraging of social media and misinformation to make pawns of a victim state's own population with the intention of creating a state of political and social instability which is extremely beneficial to the perpetrating state. What the analysis in this chapter highlights is that this normative position, held by Russia and beginning to spread to states with similar goals and capabilities, was not constructed through discursive or rhetorical acts of norm construction. This norm developed and has begun to attract new adherents, more norm entrepreneurs, because of the application of the methods of warfare which it allows. These cyber-attacks and the way the material they gathered were weaponised and deployed, in turn successfully providing Russia with political advantage, were indicative of an *operationalised* process of norm construction. Russia, by acting within the bounds of an expanded norm of war, has at once simultaneously achieved its military and political goals *and* constructed a new normative position which encompasses the methods employed to achieve them.

The utilisation of this method of norm construction and the implicit subversion of the existent norms which results from it is at once understandable thanks to its practical benefits and evidently intentional. The modes of warfare encompassed by this norm allow for significant

gains, comparable to those which historically required military usage of direct force, while simultaneously offsetting the risk of not only failure but international repercussion due to the subversive nature of this method of war and of norm construction. The discourse-oriented efforts towards expanding previous norms of war to encompass cyber-capability were not only undermined by the limited imagination as to what could be achieved through non-violent means, but also because of these norms' legitimacy being undermined by the actions of states which discursively and rhetorically supported them. The use of direct cyber-attacks by states whose status should have been contributing to the legitimacy of these efforts to expand restraining norms of war directly undermined this position they purported to support. Attacks such as Stuxnet, Flame and others effectively weakened this norm and presented an opening; Russia simply wedged the door open.

In so doing, through employing operationalised means of norm construction and in the pursuit of practical goals Russia achieved a normative advantage which easily translates into a political one. By disregarding the fledgling and already undermined discursive and rhetorical attempts to expand the norms of war to include the potential of cyber-war Russia managed to seize a position that allowed them to dictate the fundamentals of the much expanded and much less restrained norm within which their actions fit. The advantages granted to this method of norm construction are not simply its resilience to challenge, the rapidity of its uptake or its ability to grant practical success alongside normative. This analysis also suggests that operationalised norms are pro-active and agenda setting, whereas their discursive cousins are reactive and must either seek to reign in the boundaries from where they are set by operationalised acts of construction or play catch up.

Strange alliances: terrorists as unintentional securitising norm entrepreneurs

The proactive nature of operationalised norm construction was the focus of the final empirical chapter of this thesis, chapter five, examining the norms and norm entrepreneurs relating to cyber-terrorism. This chapter postulated a cycle of cyber-terrorist norm construction and demonstrated three interlinked conclusions, each of which contributes further to our understanding of the nature of security-orientated norm construction.

Firstly, it sought to examine whether terrorist actors themselves should be considered as securitising norm entrepreneurs and, if so, what role they might play in the construction of cyber-terrorism specific norms. Firstly, my analysis sought to examine whether terrorist actors themselves should be considered as securitising norm entrepreneurs and, if they could, what role might they play in the construction of cyber-terrorism specific norms. Terrorists are not terribly dissimilar to states with regards to their motivations for employing force to achieve

their goals. Methods of terrorism, the forms of violence employed, are dependent not just on the political nature of the group in question but the practicalities of capability measured against risk, a comparable trait to that of state actors. Terrorists, it was concluded, rely upon the creation of spectacle or theatre to achieve their desired effect. With regards to cyber-attacks the necessary theatre to induce a significant state of fear in the target audience does not require destruction of the like seen in direct, physical forms of terrorist violence. Cyber-attacks are chosen in part due to the pre-existent and naturally inherent fear of the unknown, which the complexity of technology is well suited to engendering. In parallel with states which engage in cyber-war, cyber-terrorists do so because of the balance between cost, risk and potential gains which can be achieved through this method. Violent terrorists use well established means of creating a significant spectacle and thus a significant impact upon a group's chosen audience, but these methods come with a great deal of risk both regarding potential cost and chance of failure. While cyber-attacks provide perhaps a lesser spectacle the existent fear of technological unknowns *does* provide the capability to induce fear, doing so while presenting a higher chance of success and a lower cost to failure.

Terrorist actors which make themselves cyber-terrorists, through the utilisation of whatever cyber-capability within their reach, engage through their attacks in a form of operationalised norm construction comparable to that noted in the previous chapter regarding Russian application of cyber-warfare. There is, however, one distinct difference; while norm entrepreneurs such as Russia achieve the symbiotic purpose of practical goals and the construction of norms in full knowledge of this duality, the same is not true of terrorist actors. Their motivation for employing cyber-capability is the perceived cost-effectiveness that the approach offers, alongside the ability to create a suitably notable spectacle thanks to the amplifying effect of inherent public technological fear. Cyber-terrorist groups do also play a role in the shaping of cyber-terrorism norms; their success serves to incentivise other groups to follow, while their limited restraint sets some boundaries. However, this is an unintended consequence of a natural drive to maximise impact while minimising risk and cost; terrorists are accidental norm entrepreneurs.

The second of the two central conclusions of this chapter further expands upon the mention of *amplification* mentioned in the previous segment. The majority of cyber-attacks carried out by terrorist actors achieve limited actual damage and result in minimal long-term impact. However, the impression they make upon their target audience is heightened, both by terrorist actors seeking to amplify the impact of these cost-effective methods and thus achieve their required spectacle, and by a concurrent process of amplification by the relevant state

actors seeking to employ these minor attacks as facilitating conditions with which to justify securitisation. This of course links in with the analysis in chapter three regarding cyber-surveillance, and the way the UK government has employed such attacks as material for rhetorical or discursive acts of norm construction seeking to justify these extensions of power.

At this stage in the process of cyber-terrorism norm construction that this chapter formulates, both the state and the terrorist actor are seeking to *amplify* the impact of the operationalised component of this cycle, the terrorist's cyber-attack. Both actors often inflate the risk an attack poses or the damage it caused significantly beyond that which it in fact represented. Norms of cyber-terrorism then are constructed in a cooperative fashion, with the process shared between the inadvertent contributions both operationalised and rhetorical provided by terrorist actors and the intentional securitisation employed in a solely rhetorical fashion by state norm entrepreneurs. This process further demonstrates then a distinct divide between the roles of these two kinds of actor, beyond the question of intentionality. States provide only discursive or rhetorical methods of construction to the overall impetus of this process of norm shaping and emergence. Terrorist actors on the other hand, despite their unintentional role, employ both operationalised *and* discursive acts of norm construction, with the latter being mirrored by the state actors involved.

Finally, the third central conclusion of this chapter, one which serves to build upon those reached in all the preceding empirical chapters, relates to the comparative natures of operationalised versus discursive and rhetorical methods of norm construction. The operationalised input to the cyber-terrorism norm construction cycle, which this chapter demonstrates, rests solely in the hands of terrorist groups. Furthermore, the operationalised component of this process is not only the necessary foundation for terrorist norm entrepreneurs' attempts at amplification, again unintentionally contributing to the shape and legitimacy of the norm. This operationalised component also, at best, provides significant legitimacy to the discursive acts of norm construction employed by state norm entrepreneurs in their attempts to justify securitisation of cyber-terrorist norms. At worst, it can be considered as much a necessary component of state actors' input to the norm construction process. This means that with regards to cyber-terrorism, terrorists are setting standards and states are reacting to them. Simultaneously, states contribute to the state of fear which incentivised this method of attack in the first place. Operationalised norm constructive is pro-active, setting standards and the direction of normative process. However, discursive and rhetorical means of norm construction are reactive, and in the instance of cyber-terrorism

dependent on the existence and nature of an operationalised, implicit act of norm construction.

Norm Securitisation and Operationalised Norm Construction

In combining the insights gained through analysis of these separate issues of cyber-security, the way the norms relating to them are constructed and the actors involved in this construction, a more complete and universal set of conclusions as to the nature of these processes can be identified. The central concepts which have been unpacked throughout this analysis are those of securitised norm emergence and operationalised norm construction. Through the analysis of cyber-surveillance norms within the UK we have noted the prevalence of securitised norm emergence, employed by the government independent of whichever political party is currently in power. This suggests that the heightened chance of successful norm construction using securitised means is not only recognised across the political establishment, but they are such that their deployment is all but assured as a result.

The fourth and fifth chapters of this thesis, on war and terrorism, first introduced and then fit the concept of operationalised methods of norm construction into frame, alongside norm securitisation and its impact on domestic orientated norms. In concluding that operationalised norms possess a proactive quality, with discursive and rhetorical methods in contrast being either dependent or reactive, this in turn suggests that domestically focussed securitised norm construction is entirely reactive. The means of securitised norm construction employed by the state - their use of facilitating conditions, emotive referent objects, the failings of functional actors, and the assertion and amplification of their being an existential threat - are all discursive or rhetorical forms of norm construction. Ergo, they are reactive. States are in effect not the trend setters with regards to the shape and direction of securitised norms. It is instead those actors who provide the operationalised component of norm construction which states seek to restrain, use or counteract through their own reactive, discursive and rhetorical means of securitised norm construction.

This leads on to the final conclusion of this thesis. When states do employ operationalised norm construction as opposed to rhetorical or discursive means, they do so intentionally *and* in recognition of the proactive and trend setting capability that this method of norm construction grants. This suggests that states turn to operationalised acts of norm construction when the status quo, the current norm governing the issue with which they actively engage, either represents a disadvantage to that state or serves to restrain the state from gaining an advantage which they have recognised. In short, states engage in operationalised norm

construction when the existent state of the international system of values and normative controls inhibits them from employing policy or applications of power in the manner which they wish. States therefore expand the boundaries of acceptable inter-state behaviour when it suits them, and when the current limitations placed upon them begin to chafe. The USA and Israel demonstrated this with Stuxnet, and the UK by threatening cyber-retaliation against Russian attributed poisonings. Russia simply went one step further. In doing so, they pushed the boundaries of the normative values of cyber-war, subverting the discursive normative process just as these other states had and, at the same time, reshaping the concept of war without anyone realising it.

Applications and implications

These conclusions, and the analysis which has led to them, are intended to be employed not only in an academic sense of furthering the understanding of theoretical concepts and phenomenon. The purpose of this work is also to inform and potentially shape the policy and efforts of those actors or groups whose work or lives might be influenced by the issues raised.

From the perspective of the average state citizen, this analysis allows for a more objective interpretation of the speech acts and political discourse employed by their governments regarding issues concerning cyber-security and also more general securitised policy. This contribution could also further benefit or in fact be taken up by NGOs such as the Open Rights Group or the Electronic Frontier Foundation. An analysis that concludes that states not only over-emphasise the risk posed from technological developments and their misuse, but that this in many instances serves as part of a complimentary process where terrorists and states entrench the same state of fear provides the provides the ammunition for a counter-narrative supported by appropriate evidence. This could be employed to effectively seek to counter this process of securitisation.

From the perspective of international politics and international institutions, the conclusions reached by this thesis regarding the use of operationalised methods of construction to purposefully undermine normative constraints that have become seen as too restrictive should be treated as evidence for a need to respond differently to these acts. If we recognise the potential harm that cyber-capability could cause in the hands of a determined and well-resourced state actor, both to infrastructure and to domestic political and social cohesion, then the direction in which the norms of cyber-war are being pushed by actors who seek to gain advantage must be curtailed. This will require further research, the dedication of

resources, the cessation of activities that would further undermine the legitimacy and efficacy of the more restrained normative position, and most notably a joint effort across the spectrum of norm entrepreneurs. Pandora's box may be open, and the threat of cyber-attack released upon a global audience, but that does not mean it too late for those who had a hand in its opening to mitigate their error and minimise the potential for misuse and harm.

Methodological limitations: more data and more access

While the central aims of this thesis have been met, with my hypothesis examined and found to hold weight, there were still limitations as to the methodology and scope which have been employed. Many of these feed into the final section of this conclusion, in which I suggest future avenues of research that could compliment and further expand upon the work contained within this body of research. The most notable issues that arose through the research and analysis carried out for the purposes of this thesis can be categorised as issues relating to limited scope, and restricted access.

Taking the latter of these into consideration first, an example can be found in the initial intention of this research to contain interview data. Specifically, I set out to target politicians who might represent individual norm entrepreneurs belonging to either a securitising block or a standard normative position. When this was attempted the issue that arose was one of access; politicians approached within the UK, with the intention of collecting data for use in chapter three on cyber-surveillance, were disinclined to acquiesce to my request. My conclusions as to the reason behind this relate in part to the relatively limited access granted by own position as a very early career researcher. However, considering the conclusions of this same chapter regarding the cross-party utilisation of securitising methods of norm construction I believe this unwillingness to engage on the subject to also be likely explained by the potential for hypocritical comparisons.

Access issues obviously expand beyond those regarding the difficulty in arranging interviews with the potential actors involved. When studying security issues, especially when attempting to employ a form of analysis that relies upon the ability to study documents, the issue of access once again arises. The analysis of state action contained within this thesis would be significantly aided by access to internal documents such as policy impact assessments and reports from the security services or military which assess the actual threat posed by different methods or instances of cyber-attack from states and terrorists. These documents are not ever intended for public perusal and thus are unlikely to be made available to academic study. This is especially the case when that study proposes a process of norm construction regarding

cyber-terrorism in which the state cooperates with terrorist actors to maximise the state of fear within its own citizenry to justify the requirement for powers of digital-surveillance.

Regarding scope there are several limitations related to restricted scope within this thesis. This thesis employed a great deal of case study analysis which directed attention towards a range of states and non-state actors. Predominantly however the greatest attention was paid to the UK, the USA and Russia. While these examples provided ample evidence to test my hypothesis the analysis and the theories I propose fit within a wider, international context. It would be ideal, therefore, if the depth of analysis applied to these examples could be directed toward an expanded range of actors and institutions. Many of the potential candidates have been mentioned briefly within the preceding chapters: Israel, Germany, North Korea, and Iran. Each of these states has engaged to some extent and in some format with both internal domestic securitisation, and external operationalised processes of securitised norm construction. It would be unlikely in the extreme that across these states, and the many other examples to which this thesis' theories could be turned, there would be no evidence of variation or no room for further addition and nuance to be gathered.

The final scope related limitation of this thesis is regarding the limited analysis of another potential securitising norm entrepreneur. This thesis fails to fully engage with analysis of the role of those groups or bodies which could be described as functional actors; these are directly involved with the issue which is in the process of being securitised, or are having the norms under which it operates reshaped. While states can, in some regards be considered functional actors, particularly in relation to the international norms surrounding cyber-war, so too could international business interests or institutions. The role of companies such as Facebook and Google, as well as that of internet service providers such as Verizon and AT&T, and those of international institutions and NGOs such as the European Court of Justice, the Electronic Frontier Foundation and the Open Rights Group, are notable in their absence from this analysis. These limitations lead this conclusion well into the assessment of opportunities to expand this research in future projects.

Questions that remain

The aim of this research, and indeed of my own continuing academic interests, is to expand our concept of how norms and security interact; engaging in them as a singular, conjoined phenomenon rather than separate entities. A significant component of this frame of reference relies upon the consideration and matching expansion of this framing to include an accurate and complete range of norm entrepreneurs and actors. This thesis has initiated this effort,

considering the impact of non-state groups such as terrorists alongside the role of states and institutions, but it remains incomplete. A future avenue of research that I propose aims to broaden this list, directing its analysis at the role and the impact of functional actors such as social media companies, internet service providers, and international institutions and NGOs in the process of cyber-security norm construction. Seeking to understand the input companies such as Facebook make in the process of securitised norm construction would not only expand the utility of the theoretical model that this thesis has contributed but would potentially result in real world policy recommendations. Potential impact could include the implementation of recommendations by these same groups, in seeking to shape norms in a manner more beneficial to their users and to the societies in which they operate.

In a parallel effort to expand upon the foundations set by this thesis in a manner that could present findings to inform policy for a variety of actors, another avenue for further study might be to focus upon the comparative strength of different processes of norm construction. This is of relevance with regards to the concept of cyber-war for states and international institutions, but also to NGOs regarding civil rights issues that might benefit from further research into the nature of operationalised norms. Greater understanding of the reasons behind their selection and comparative resilience analysis might provide insight into how actors who wish to maintain or affirm non-securitised or more restrained forms of securitised norm might seek to fortify against, or counteract the advantages implicit in, operationalised methods of norm construction. Such research might include the examination of the efficacy of counter-narratives as a manner of declawing the power of operationalised instances of information warfare, or whether efforts to clarify the sources or purpose of information provided by internet sources can act as a buffer between the actor employing information warfare and their target group. Further research could also explore whether technological solutions such as algorithmic censorship and gatekeepers can have an immunising effect upon this emergent form of cyber-warfare.

A final area for further research arises from the scope-based limitations which I discussed in the previous section of this conclusion. While there are numerous examples of states used as case studies and context, for the purposes of this thesis only a small selection of them were engaged with in significant detail. To further test the hypothesis posed in this thesis, with the hope of adding further nuance and added utility to the frameworks I have proposed, a more expansive look at the methods and impacts of securitised norm construction in a wider variety of states is required. Applying the same analytical tools as employed against the UK, the USA and Russia for this thesis towards states such as Germany, Israel, North Korea and Iran would

serve to both demonstrate the broad utility of the concepts of operationalised norm construction and securitised norm emergence, while allowing for expansion of these same concepts through a broader range of contexts.

Bibliography

Ackerman, S. and Roberts, D. (2013) *US Lawmakers Call for Review of Patriot Act after NSA Surveillance Revelations* [online]. *Guardian*. Available from: www.theguardian.com/world/2013/jun/10/patriot-act-nsa-surveillance-review [Accessed 6 March 2018].

Alperovitch, D. (2015) *The Latest on Chinese-Affiliated Intrusions* [online]. CrowdStrike Blog. Available from: www.crowdstrike.com/blog/the-latest-on-chinese-affiliated-intrusions-into-commercial-companies/ [Accessed 22 January 2018].

Anon (2016) *EU data ruling goes against UK government* [online]. BBC. Available from: www.bbc.co.uk/news/uk-politics-38390150 [Accessed 20 March 2018].

Anti-terrorism Act, c 41 (2001). Available from http://canlii.ca/t/j0x6 [Accessed 26 July 2013].

Arendt, H. (1970) *On Violence*. London: Allen Lane The Penguin Press.

Arquilla, J. and Ronfeldt, D. (1995) 'Cyberwar is Coming!', *Comparative Strategy,* 12 (2), 141–165.

Arthur, C. (2014) *EU Court of Justice Overturns Law That Would Enable 'Snoopers' Charter* [online]. *Guardian*. Available from: www.theguardian.com/technology/2014/apr/08/eu-court-overturns-law-snoopers-charter-data-phones-isps [Accessed 20 March 2018].

Arquilla, J., Ronfeldt, D., & Zanini, M. (2000). Information-age terrorism. *Current History, 99*, 179. Retrieved from https://search.proquest.com/docview/1309783168?accountid=11862

Associated Press (2016) *Nice Truck Attack: French Police Arrest Eight More Suspects* [online]. Available from: www.theguardian.com/world/2016/sep/20/nice-truck-attack-french-police-arrest-eight-new-suspects [Accessed 12 March 2018].

BAE Systems Detica (2011) *The Cost of Cyber Crime.* London: Detica.

Balzacq, T. (2005). The Three Faces of Securitization: Political Agency, Audience and Context. European Journal of International Relations, 11(2), 171–201. https://doi.org/10.1177/1354066105052960

Ball, K., Snider, L. 2013, *The Surveillance-Industrial Complex: A Political Economy Of Surveillance,*Routledge, New York

Bartlett, J. (2014). Dark net markets: the eBay of drug dealing. *The Observer*.

Bendrath, R. (2001). The Cyberwar Debate: Perception and Politics In US Critical Infrastructure Protection. *Special Issue of Information & Security*, 65.

Bendrath, R. (2003). The American Cyber-Angst and the Real World—Any Link? In

Bombs and Bandwidth: The Emerging Relationship between IT and Security, edited by Latham R., New York: The New Press.

Berkman, F. (2013) *Syrian Hackers Target Obama's Twitter, Facebook Posts* [online]. Mashable. Available from: https://mashable.com/2013/10/28/syrian-electronic-army-obama/ [Accessed 10 March 2018].

Bertram, L. (2016) Terrorism, the Internet and the Social Media Advantage: Exploring How Terrorist Organizations Exploit Aspects of the Internet, Social Media and How These Same Platforms Could be Used to Counter-Violent Extremism, *Journal for Deradicalization*, Summer (7), 225–252.

Bertram, S. (2017) ''Close Enough' – The Link Between the Syrian Electronic Army and the Bashar al-Assad regime, and Implications for the Future Development of Nation-State Cyber Counter-Insurgency Strategies', *Contemporary Voices: St Andrews Journal of International Relations* [online], 8 (1). Available from: https://cvir.st-andrews.ac.uk//articles/10.15664/jtr.1294/ [Accessed 10 March 2018].

Bodkin, H. et al. (2017) *Government Under Pressure After NHS Crippled in Global Cyber Attack As Weekend Of Chaos Looms* [online]. *Telegraph*. Available from: www.telegraph.co.uk/news/2017/05/12/nhs-hit-major-cyber-attack-hackers-demanding-ransom/ [Accessed 1 March 2018].

Boffey, D. and Rankin, J. (2017) *EU Escalates its Campaign Against Russian Propaganda*. *Guardian*. 23 January. [online]. Available from: www.theguardian.com/world/2017/jan/23/eu-escalates-campaign-russian-propaganda [Accessed 6 November 2017].

Booth, R. et al. (2017) *Russia Used 419 Fake Accounts to Tweet About Brexit, Data Shows* [online]. *Guardian*. Available from: www.theguardian.com/world/2017/nov/14/how-400-russia-run-fake-accounts-posted-bogus-brexit-tweets [Accessed 14 November 2017].

Borger, J. (2017) *As France Becomes Latest Target, are Election Hacks the New Normal?* [online]. *Guardian*. Available from: www.theguardian.com/world/2017/may/05/french-election-hack-emmanuel-macron [Accessed 6 November 2017].

Borger, J. et al. (2013) *Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security* [online]. *Guardian*. Available from: www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security [Accessed 19 March 2018].

Bossert, T. P. (2017) *It's Official: North Korea is Behind WannaCry* [online]. *Wall Street Journal*. Available from: www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537 [Accessed 1 March 2018].

Brunner, E. M. and Cavelty, M. D. (2009) 'The Formation of In-formation by the US Military: Articulation and Enactment of Infomanic Threat Imaginaries on the Immaterial Battlefield of Perception', *Cambridge Review of International Affairs* [online], 22 (4), 629–646.

Burden, K. and Palmer, C. (2003) 'Cyber Crime – A New Breed of Criminal?', *Computer Law and Security Report*, 222–227.

Burgess, M. (2017) *Here's the First Evidence Russia Used Twitter to Influence Brexit* [online]. Wired. Available from: www.wired.co.uk/article/brexit-russia-influence-twitter-bots-internet-research-agency [Accessed 26 February 2018].

Buzan, B. et al. (1997) *Security: A New Framework for Analysis*. London: Lynne Reinner Publishing.

Byers, D. (2017) *Facebook Estimates 126 Million People Were Served Content From Russia-Linked Pages* [online]. CNN. Available from: http://money.cnn.com/2017/10/30/media/russia-facebook-126-million-users/index.html [Accessed 2 February 2018].

Cameron, D. (2009) 'Giving Power Back to the People'. Speech at Imperial College London, 25 June.

Cavallaro, L. (2013). *Malicious Software: Should We Care?* Lecture given at Royal Holloway, University of London, 20 November.

Cavelty, M. D. (2008) 'Cyber-Terror – Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate', *Journal of Information Technology and Politics* [online], 4 (1), 19–36.

Cavelty, M. D. (2012) 'The Militarisation of Cyberspace: Why Less May be Better', in *4th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications, pp.141–153.

Chakrabarti, S. (2018) *Hard Questions: What Effect Does Social Media Have on Democracy?* [online]. Facebook Newsroom. Available from: https://newsroom.fb.com/news/2018/01/effect-social-media-democracy/ [Accessed 24 January 2018].

Cherepanov, A. and Lipovsky, R. (2017) *Industroyer: Biggest Threat to Industrial Control Systems Since Stuxnet* [online]. Welivesecurity. Available from: www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/ [Accessed 28 February 2018].

Chirgwin, R. (2018) *IT 'Heroes' Saved Maersk From Notpetya With Ten-Day Reinstallation Bliz* [online]. The Register. Available from: www.theregister.co.uk/2018/01/25/after_notpetya_maersk_replaced_everything/ [Accessed 28 February 2018].

Chokshi, N. (2016) *Trump Accuses Clinton of Guiding Global Elite Against U.S. Working Class* [online]. *New York Times*. Available from: www.nytimes.com/2016/10/14/us/politics/trump-comments-linked-to-antisemitism.html [Accessed 28 February 2018].

Clarke, Richard, A,. and Knake, Robert, K. (2010). Cyber war: the next threat to national security and what to do about it, New York, Ecco

Clausewitz, C. V. (2008) *On War.* Princeton: Princeton University Press.

CNN (2010) *New Issue of Magazine Offers Jihadists Terror Tips* [online]. CNN. Available from: www.cnn.com/2010/WORLD/meast/10/12/mideast.jihadi.magazine/index.html [Accessed 12 March 2018].

CNN (2016) *Full Transcript: CNN Democratic Debate* [online]. CNN. Available from: www.cnn.com/2016/04/14/politics/transcript-democratic-debate-hillary-clinton-bernie-sanders/index.html [Accessed 28 February 2018].

Coker, C. (2013-02-01). (Ed.), Warrior Geeks: How 21st Century Technology is Changing the Way We Fight and Think About War. : Oxford University Press,. Retrieved 24 Feb. 2019, from http://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780199327898.001.0001/acprof-9780199327898.

Coleman, G. (2015) Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous. London: Verso.

Conway, M. (2008) 'Media, Fear and the Hyperreal: The Construction of Cyberterrorism as the Ultimate Threat to Critical Infrastructures', *Working Papers in International Studies*, 1–38.

Conway, M., (2012) Introduction: terrorism and contemporary mediascapes – reanimating research on media and terrorism, Critical Studies on Terrorism,5:3, 445-453, DOI: 10.1080/17539153.2012.725979

Conway, M. (2013) 'Three Arguments Against Cyberterrorism'. Paper presented at A Multidisciplinary Conference on Cyberterrorism, Birmingham.

Cornish, P., Livingstone, D., Clemente, D. and Yorke, C. (2011) *Cyber Security and the UK's Critical National Infrastructure.* London: Chatham House.

Council of Europe (2001) Convention on Cyber Crime. Budapest.

Court of Justice of the European Union (2014) The Court of Justice Declares the Data Retention Directive to be Invalid. No. 54/14

Couzigou, I. (2013) 'The Use of Force as a Response to Cyberterrorism'. Paper presented at A Multidisciplinary Conference on Cyber Terrorism, Birmingham.

Cox, J. (2017) *Facebook, Google and Twitter Respond to May's Comments That Tech Companies Need to do More to Stamp Out Extremism* [online]. *Independent*. Available from: www.independent.co.uk/news/business/news/facebook-google-twitter-london-attack-terror-tech-companies-do-more-surveillance-privacy-a7773026.html [Accessed 27 January 2018].

Davis, B. R. (2006) 'Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet with the Rule of Law and Improved Tools for Cyber Governance: Comment', *CommLaw Conspectus: Journal of Communications Law and Policy*, 15, 119–186.

Davis, J. (2007) *Hackers Take Down the Most Wired Country in Europe* [online]. Wired. Available from: www.wired.com/2007/08/ff-estonia/ [Accessed 28 January 2018].

Dearden, L. (2017) *French Media Ordered Not to Publish Macron's Hacked Emails* [online]. *Independent*. Available from: www.independent.co.uk/news/world/europe/emmanuel-macron-email-hack-leaks-election-marine-le-pen-russia-media-ordered-not-publish-commission-a7721111.html [Accessed 23 January 2018].

Delcker, J. (2017) *Germany Fears Russia Stole Information to Disrupt Election* [online]. Politico. Available from: www.politico.eu/article/hacked-information-bomb-under-germanys-election/ [Accessed 22 January 2018].

Department of Homeland Security and Office of the Director of National Intelligence (2016) Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security [online]. US Department of Homeland Security. Available from: www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national [Accessed 20 March 2018].

Department of the Army (2005) *Field Manual 3-05.30.* [online]. Federation of American Scientists. Available from: https://fas.org/irp/doddir/army/fm3-05-30.pdf [Accessed 8 January 2018)

Der Spiegel (2013) *Interview with Whistleblower Edward Snowden on Global Spying* [online]. Spiegel Online. Available from: www.spiegel.de/international/world/interview-with-whistleblower-edward-snowden-on-global-spying-a-910006.html [Accessed 19 March 2018].

Digital Rights Ireland (2004) *DRI Brings Legal Action Over Mass Surveillance* [online]. Digital Rights Ireland. Available from: www.digitalrights.ie/dri-brings-legal-action-over-mass-surveillance/ [Accessed 6 March 2018].

Dinniss, H. H. (2012) *Cyber Warfare and the Laws of War.* Cambridge: Cambridge University Press.

Dunn Cavelty, M. (2008) Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate, Journal of Information Technology & Politics, 4:1, 19-36, DOI: 10.1300/J516v04n01_03

Dunn Cavelty, M., From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse, *International Studies Review*, Volume 15, Issue 1, 1 March 2013, Pages 105–122, https://doi.org/10.1111/misr.12023

Elliott, F. and Haynes, D. (2017) *GCHQ: British Cyberweapons Could Paralyse Hostile States* [online]. *The Times*. Available from: https://www.thetimes.co.uk/article/gchq-british-cyberweapons-could-paralyse-hostile-states-zbcm3mdbt [Accessed 21 March 2018].

Ellis, R. (2016) *Erdogan's Turkey Has Reached New Levels of Hysteria* [online]. *Independent*. Available from: www.independent.co.uk/voices/turkey-has-reached-new-levels-of-journalist-repression-yet-the-eu-willingly-lets-itself-be-fooled-a6944501.html [Accessed 6 March 2018].

Embar-Seddon, A. (2002) 'Cyberterrorism: Are We Under Siege?', *American Behavioral Scientist* [online], 45 (6), 1033–1043.

Eriksson, J. (2001). Cyberplagues, IT, and security: Threat politics in the information age. *Journal of Contingencies and Crisis Management*, *9*(4), 200-210.

European Commission (2012) Special Eurobarometer 390: Cyber Security. European Commission.

Fabbrini, F. (2015). Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States. *Harvard Human Rights Journal* 28, 65-96.

Finnemore, M. (2017) *Cybersecurity and the Concept of Norms* [online]. Carnegie Endowment for International Peace. Available from: http://carnegieendowment.org/2017/11/30/cybersecurity-and-concept-of-norms-pub-74870 [Accessed 1 December 2017].

Finnemore, M. and Sikkink, K. (1998) 'International Norm Dynamics and Political Change', *International Organization*, 52 (4), 887–917.

FireEye (2017) *Senate Intelligence Committee: Russia and 2016 Election* [online]. FireEye. Available from: www.fireeye.com/content/dam/fireeye-www/solutions/pdfs/st-senate-intel-committee-russia-election.pdf [Accessed 4 March 2018].

Fisher, M. (2013) *Syrian Hackers Claim AP Hack That Tipped Stock Market by $136 Billion. Is it Terrorism?* [online]. *Washington Post*. Available from: www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/ [Accessed 20 March 2018].

Foster, P. (2013) *'Bogus' AP Tweet About Explosion at the White House Wipes Billions off US Markets* [online]. *Telegraph.* Available from: www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html [Accessed 10 March 2018].

Futter, A. (2018). 'Cyber'semantics: why we should retire the latest buzzword in security studies. *Journal of Cyber Policy*, *3*(2), 201-216.

Gallagher, S. (2018) *Twitter "Bot" Purge Causes Outcry from Trollerati as Follower Counts Fall* [online]. ars technica. Available from: https://arstechnica.com/tech-policy/2018/02/twitter-suspends-thousands-of-accounts-for-bot-behavior-some-cry-censorship/ [Accessed 26 February 2018].

Geers, K. (2009) 'The Cyber Threat to National Critical Infrastructures: Beyond Theory', *Information Security Journal: A Global Perspective* [online], 18 (1), 1–7.

Geers, K. and Alqartah, A. (2013) *Syrian Electronic Army Hacks Major Communications Websites* [online]. FireEye. Available from: www.fireeye.com/blog/threat-research/2013/07/syrian-electronic-army-hacks-major-communications-websites.html [Accessed 12 March 2018].

Gill, P. et al. (2017) ‘Terrorist Use of the Internet by the Numbers’, *Criminology and Public Policy* [online], 16 (1), 99–117.

Gisel, L. (2013) *The Law of War Imposes Limits on Cyber Attacks Too* [online]. ICRC. Available from: www.icrc.org/eng/resources/documents/interview/2013/06-27-cyber-warfare-ihl.htm [Accessed 21 March 2018].

Gogolin, G. (2010) ‘The Digital Crime Tsunami’, *Digital Investigation*, 3–8.

Gold, S. (2012) 'Virtual Jihad: How Real is the Threat?', *Network Security* [online], (12), 15–18.

Gorodnichenko, Y. et al. (2017) *Social Media, Sentiment and Public Opinions: Evidence From #Brexit and #USElection* [online]. Swansea University. Available from: https://rahwebdav.swan.ac.uk/repec/pdf/WP2018-01.pdf [Accessed 26 February 2018].

GReAT (2017) *Wannacry and Lazarus Group – The Missing Link?* [online]. SecureList. Available from: https://securelist.com/wannacry-and-lazarus-group-the-missing-link/78431/ [Accessed 1 March 2018].

Greenberg, A. (2017a) *Hackers Gain Direct Access to US Power Grid Controls* [online]. Wired. Available from: www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/ [Accessed 28 February 2018].

Greenberg, A. (2017b) *Hackers Hit Macron with Huge Email Leak Ahead of French Election* [online]. Wired. Available from: www.wired.com/2017/05/macron-email-hack-french-election/ [Accessed 23 January 2018].

Grierson, J. (2017) *UK Hit by 188 High-Level Cyber-Attacks in Three Months* [online]. *Guardian*. Available from: www.theguardian.com/world/2017/feb/12/uk-cyber-attacks-ncsc-russia-china-ciaran-martin [Accessed 6 November 2017].

Griffith, E. (2018) *Pro-Gun Russian Bots Flood Twitter After Parkland Shooting* [online]. Wired. Available from: www.wired.com/story/pro-gun-russian-bots-flood-twitter-after-parkland-shooting/ [Accessed 26 February 2018].

Hamilton68 (n.d.) *Hamilton 68: Tracking Putin’s Propaganda Push... to America* [online]. GMF. Available from: http://dashboard.securingdemocracy.org/ [Accessed 28 February 2018].

Hansard HC Deb, vol. 340, cols. 45, 29 November 1999

Hansard HC Deb, vol. 346, cols. 768, 6 March 2000

Hansard HC Deb, vol. 346, cols. 10, 13 March 2000

Hansard HC Deb, cols. 105, 10 April 2000

Hansard HC Deb, vol. 349, cols. 543, 8 May 2000

Hansard HC Deb, vol. 351, cols. 601, 12 June 2000

Hansard HC Deb, cols. 112W, 12 March 2007

Hansard HC Deb, cols. 1059W, 16 November 2009

Hansard HC Deb, cols. 1048W, 28 January 2010

Hansard HC Deb, cols. 151WH, 28 October 2010

Hansard HC Deb, cols. 813W, 17 November 2010

Hansard HC Deb, cols. 38WS, 11 May 2011

Hansard HC Deb, cols. 34WS, 19 May 2011

Hansard HC Deb, cols. 468W, 16 January 2012

Hansard HC Deb, cols. 1453W, 1 May 2012

Hansard HC Deb, cols. 33, 9 May 2012

Hansard HC Deb, cols. 18W, 10 September 2012

Hansard HC Deb, cols. 19W, 10 September 2012

Hansard HC Deb, cols. 90WS, 13 July 2012

Hansard HC Deb, cols. 456, 10 July 2014

Hansard HC Deb, cols. 704, 15 July 2014

Hansard HC Deb, cols. 1011, 17 July 2014

Hansard HC Deb, cols. W, 24 October 2014

Hansard HC Deb, cols. 869, 14 January 2015

Hansard HL Deb, cols. 1404, 12 June 2000

Hansard HL Deb, cols. 16, 19 June 2000

Hansard HL Deb, cols. 275, 19 June 2003

Hansard HL Deb, cols. 1, 9 May 2012

Hansard HL Deb, cols. 23, 17 November 2015

Hansen, L. (2006). Security as Practice: Discourse Analysis and the Bosnian War. London: Routledge.

Harris, P. (2013) *Chinese Army Hackers are the Tip of the Cyberwarfare Iceberg* [online]. *Guardian*. Available from: www.theguardian.com/technology/2013/feb/23/mandiant-unit-61398-china-hacking [Accessed 21 March 2018].

Healey, J. (2011) *Bringing a Gun to a Knife Fight: Striking Back in Cyber Conflict* [online]. Atlantic Council. Available from: www.atlanticcouncil.org/blogs/new-atlanticist/bringing-a-gun-to-a-knife-fight-striking-back-in-cyber-conflict [Accessed 4 March 2018].

Heickerö, R. (2014) 'Cyber Terrorism: Electronic Jihad', *Strategic Analysis* [online], 38 (4), 554–565.

Hern, A. (2015) *Google Says Non to French Demand to Expand Right to be Forgotten Worldwide* [online]. *Guardian*. Available from: www.theguardian.com/technology/2015/jul/30/google-rejects-france-expand-right-to-be-forgotten-worldwide [Accessed 27 January 2018].

Higgins, A. (2017) *Maybe Private Russian Hackers Meddled in Election, Putin Says* [online]. *New York Times*. Available from: www.nytimes.com/2017/06/01/world/europe/vladimir-putin-donald-trump-hacking.html [Accessed 4 March 2018].

Hoffman, B. (2002) *Lessons of 9/11* [online]. Rand Corporation. Available from: www.rand.org/pubs/testimonies/CT201.html [Accessed 10 March 2018].

Home Office (2000) Regulation of Investigatory Powers Act (c23). London: The Stationary Office.

Home Office (2009a) *Protecting the Public in a Changing Communications Environment* (Cm. 7568). London: The Stationary Office.

Home Office (2009b) *Strategic Defence and Security Review* (Cm. 9748). London: The Stationary Office.

Home Office (2015) Draft Communications Data Bill (Cm. 9152). London: The Stationary Office.

Home Office (2016) Investigatory Powers Act (c. 25). London: The Stationary Office.

Hooge, L. (2005) 'Several Roads Lead to International Norms, but Few via International Socialization: A Case Study of the European Commission', *International Organization*, 58 (4), 861–898.

Hope, C. (2013) *David Cameron Challenges China Over Cyber Spying* [online]. *Telegraph*. Available from: www.telegraph.co.uk/news/politics/david-cameron/10493018/David-Cameron-challenges-China-over-cyber-spying.html [Accessed 4 March 2018].

Huysmans, J. (2011). What's in an act? On security speech acts and little security nothings. Security Dialogue, 42(4–5), 371–383. https://doi.org/10.1177/0967010611418713

Intelligence and Security Committee (2017) *Annual Report 2016–2017* (HC 2016–17, 655).

International Committee of the Red Cross (ICRC) (1977) Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I). ICRC.

Ivanov, A. and Mamedov, O. (2017) *ExPetr/Petya/NotPetya is a Wiper, Not Ransomware* [online]. SecureList. Available from: https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/ [Accessed 28 February 2018].

Jenkins, B. (1975) *Will Terrorists Go Nuclear?* The Rand Paper Series. Santa Monica: The Rand Corporation.

Jenkins, B. M. (2012) 'The New Age of Terrorism', in *The McGraw-Hill Homeland Security Handbook*. New York: McGraw-Hill Professional, pp.117–130 [online]. Rand Corporation. Available from: www.rand.org/pubs/reprints/RP1215.html [Accessed 12 March 2018].

Jukes, L. (2017) Amber Rudd on Westminster Terror Attack. *The Andrew Marr Show* [online]. BBC. Available from: www.bbc.co.uk/programmes/p04y2cnh [Accessed 17 March 2018].

Kaspersky Labs (2017a) *Spam and Phishing in 2016* [online]. SecureList. Available from: https://securelist.com/kaspersky-security-bulletin-spam-and-phishing-in-2016/77483/ [Accessed 21 January 2018].

Kaspersky Labs (2017b) *Spam and Phishing in Q2 2017* [online]. Available from: https://securelist.com/spam-and-phishing-in-q2-2017/81537/ [Accessed 21 January 2018].

Kettle, M. (2015) *Security v Privacy: Anderson Offers the Balance We've Been Seeking Since 9/11* [online]. *Guardian*. Available from: www.theguardian.com/commentisfree/2015/jun/11/security-privacy-anderson-september-11-gamechanger-thersa-may [Accessed 19 March 2018].

Krogstad, J. M. and Lopez, M. H. (2017) *Black Voter Turnout Fell in 2016, Even as a Record Number of Americans Cast Ballots* [online]. Pew Research Center. Available from:

www.pewresearch.org/fact-tank/2017/05/12/black-voter-turnout-fell-in-2016-even-as-a-record-number-of-americans-cast-ballots/ [Accessed 2 February 2018].

Lee, R. (2017) *CRASHOVERRIDE - Analysis of the Threat to Electric Grid Operations* [online]. Dragos. Available from: https://dragos.com/blog/crashoverride/index.html [Accessed 28 February 2018].

Lee, R. M. and Rid, T. (2014) 'OMG Cyber!' *The RUSI Journal* [online], 159 (5), 4–12.

Legro, J. (1997) 'Which Norms Matter? Revisiting the "Failure" of Internationalism', *International Organization,* 51 (1), 31–63.

Leistert, O. (2012). Resistance against cyber-surveillance within social movements and how surveillance adapts. *Surveillance & Society, 9*(4), 441-456. doi:http://dx.doi.org/10.24908/ss.v9i4.4345

Lesser, I., Arquilla, J., Hoffman, B., Ronfeldt, D. F., & Zanini, M. (1999). *Countering the new terrorism*. RAND corporation.

Lewis, J. A. (2002). *Assessing the risks of cyber terrorism, cyber war and other cyber threats*. Washington, DC: Center for Strategic & International Studies.

Lewis, J. A. (2004). Assessing the risk of cyber terrorism, cyber war and other cyber threats, 2002. *Center for Strategic amd International Studies, http://www. csis. org/tech/0211lewis. pdf, stan z dnia*, *27*.

Lewis, J. (2003). Cyber terror: Missing in action. *Knowledge, Technology & Policy*, *16*(2), 34-41.

Lipovsky, R. and Cherepanov, A. (2016) *BlackEnergy Trojan Strikes Again: Attacks Ukrainian Electric Power Industry* [online]. Welivesecurity. Available from: www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/ [Accessed 28 February 2018].

Lipton, J. D. (2010). Digital multi-media and the limits of privacy law. *Case Western Reserve Journal of International Law* 42(3), 551-572.

Lomas, N. (2015) *Facebook Wins Court Challenge in Germany Against its Real Names Policy* [online]. TechCrunch. Available from: http://social.techcrunch.com/2013/02/15/facebook-wins-court-challenge-in-germany-against-its-real-names-policy/ [Accessed 27 January 2018].

Lynn, W. (2010) 'Defending a New Domain: The Pentagon's Cyberstrategy', *Foreign Affairs*, 89 (5), 97–109.

MacDonald, S. (2013) 'Preventing Cyber Terrorism: The Criminalisation of Preparatory Activities'. Paper presented at A Multidisciplinary Conference on Cyberterrorism, Birmingham, UK.

Mason, R. (2015) *Xi Jinping State Visit: UK and China Sign Cybersecurity Pact* [online]. *Guardian*. Available from: www.theguardian.com/politics/2015/oct/21/uk-china-cybersecurity-pact-xi-jinping-david-cameron [Accessed 22 January 2018].

May, T. (2017) *PM Speech to the Lord Mayor's Banquet 2017* [online]. Gov.uk. Available from: www.gov.uk/government/speeches/pm-speech-to-the-lord-mayors-banquet-2017 [Accessed 22 January 2018].

McAfee (2005) McAfee Virtual Criminology Report. McAfee.

McAfee Labs (2013) *2013 Threat Predictions.* Santa Clara: McAfee.

McAfee Labs (2017) *McAfee Labs Threat Report* [online]. McAfee. Available from: www.mcafee.com/uk/resources/reports/rp-quarterly-threats-jun-2017.pdf [Accessed 21 January 2018)

McGoogan, C. (2017) *Hackers Targeting UK Energy Grid, GCHQ Warns* [online]. *Telegraph*. Available from: www.telegraph.co.uk/technology/2017/07/18/hackers-targeting-uk-energy-grid-gchq-warns/ [Accessed 28 February 2018].

Melki, J. and Jabado, M. (2016) 'Mediated Public Diplomacy of the Islamic State in Iraq and Syria: The Synergistic Use of Terrorism, Social Media and Branding', *Media and Communication*, 4 (2), 92–103.

Moore, H. and Roberts, D. (2013) *AP Twitter Hack Causes Panic on Wall Street and Sends Dow Plunging* [online]. *Guardian*. Available from: www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall [Accessed 20 March 2018].

Morris, N. (2011) *Al-Qa'ida threatens cyber-jihad* [online]. *Independent*. Available from: www.independent.co.uk/news/uk/crime/al-qaida-threatens-cyber-jihad-2312651.html [Accessed 10 March 2018].

Mortimer, C. (2017) *Man Who Posted Infamous Image of Muslim Woman 'Ignoring Terror Attack Victims' Was Russian Troll* [online]. *Independent*. Available from: www.independent.co.uk/news/uk/politics/man-muslim-woman-london-terror-attack-phone-russian-troll-identity-a8052961.html [Accessed 5 February 2018].

Musil, S. (2013) *Anonymous Targets Israel in Another Cyberattack* [online]. Cnet. Available from: www.cnet.com/news/anonymous-targets-israel-in-another-cyberattack/ [Accessed 13 March 2018].

Nakashima, E. and Rucker, P. (2017) *U.S. Declares North Korea Carried Out Massive WannaCry Cyberattack* [online]. *Washington Post*. Available from: www.washingtonpost.com/world/national-security/us-set-to-declare-north-korea-carried-out-massive-wannacry-cyber-attack/2017/12/18/509deb1c-e446-11e7-a65d-1ac0fd7f097e_story.html [Accessed 1 March 2018].

NATO Cooperative Cyber Defence Centre of Excellence (2017) *NotPetya and WannaCry Call for a Joint Response from International Community* [online]. NATO Cooperative Cyber Defence Centre of Excellence. Available from: www.ccdcoe.org/notpetya-and-wannacry-call-joint-response-international-community [Accessed 2 March 2018].

NCSC (2018) *Russian Military 'Almost Certainly' Responsible for Destructive 2017 Cyber Attack* [online]. NCSC. Available from: www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack [Accessed 28 February 2018].

Nissenbaum, H. 2004, *Privacy As Contextual Integrity,* Washington Law Review, 79 (2004) 1, pp. 119-158

Nixon, A. et al. (2016) *Flashpoint - An After-Action Analysis of the Mirai Botnet Attacks on Dyn* [online]. Flashpoint. Available from: www.flashpoint-intel.com/blog/cybercrime/action-analysis-mirai-botnet-attacks-dyn/ [Accessed 12 March 2018].

O'Sullivan, D. (2018) *Russian Trolls Created Facebook Events Seen by More Than 300,000 Users* [online]. CNN. Available from: http://money.cnn.com/2018/01/26/media/russia-trolls-facebook-events/index.html [Accessed 5 February 2018].

Oliphant, R. and Esnor, J. (2014) *Ukraine Crisis: Victor Yanukovych Blames Protestors for Violence* [online]. *Telegraph*. Available from: www.telegraph.co.uk/news/worldnews/europe/ukraine/10648066/Ukraine-crisis-Viktor-Yanukovych-blames-protesters-for-violence.html [Accessed 24 March 2014].

Palasinski, M. & Bowman-Grieve, L. Secur J (2017) 30: 556. https://doi.org/10.1057/sj.2014.19

Pallister, D. (2007) *Three Jailed for Engaging in 'Cyber Jihad' for al-Qaida* [online]. *Guardian*. Available from: www.theguardian.com/technology/2007/jul/06/news.terrorism [Accessed 10 March 2018].

Parliament of the United Kingdom (1990) Computer Misuse Act 1990 [online]. Gov.uk. Available from: www.legislation.gov.uk/ukpga/1990/18/contents [Accessed 10 February 2012].

Parliament of the United Kingdom (2000) Terrorism Act 2000 [online]. Gov.uk. Available from: www.legislation.gov.uk/ukpga/2000/11/section/1 [Accessed 15 February 2012].

Parliament of the United Kingdom (2006) Terrorism Act 2006. London: The Stationary Office.

Patterson, T. (2010) *U.S. Electricity Blackouts Skyrocketing* [online]. CNN. Available from: www.cnn.com/2010/TECH/innovation/08/09/smart.grid/index.html [Accessed 29 August 2017].

Porche, I. R. (2016) *Emerging Cyber Threats and Implications*. [online]. Rand Corporation. Available from: www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT453/RAND_CT453.pdf [Accessed 2 September 2017)

Poulsen, K. (1999) *Info War or Electronic Saber Rattling?* [online]. ZDNet. Available from: www.zdnet.com/article/info-war-or-electronic-saber-rattling-5000103202/ [Accessed 10 March 2018].

Primoratz, I. (1990) 'What is Terrorism?' *Journal of Applied Philosophy*, 7 (2), 129–130.

Putnam, R. (1988) 'Diplomacy and Domestic Politics: the Logic of Two-Level Games', *International Organization*, 42 (3), 427–460.

Rankin, J. (2017) *Catalan Independence: EU Experts Detect Rise in Pro-Kremlin False Claims* [online]. *Guardian*. Available from: www.theguardian.com/world/2017/nov/13/catalan-independence-eu-experts-detect-rise-in-pro-kremlin-false-claims [Accessed 14 November 2017].

Realm v Gold and Schifreen AC 1063 (House of Lords, 21 April 1988).

Regulation of Investigatory Powers HC Deb. 14 March 2000.

Reuters (2016) *German Court Rules Facebook May Prevent its Users from Using Fake Names* [online]. *Guardian*. Available from: www.theguardian.com/technology/2016/mar/03/facebook-pseudonym-case-german-court-privacy [Accessed 27 January 2018].

Reuters (2018) *Egypt to Extend State of Emergency for Three Months: MENA* [online]. Reuters. Available from: www.reuters.com/article/us-egypt-security/egypt-to-extend-state-of-emergency-for-three-months-mena-idUSKBN1ER1B0 [Accessed 6 March 2018].

Rid, T. (2011) 'Cyber War Will Not Take Place', *Journal of Strategic Studies* [online], 35 (1), 5–32.

Robhat Labs (2017) *An Analysis of Propaganda Bots on Twitter* [online]. Robhat Labs. Available from: https://medium.com/@robhat/an-analysis-of-propaganda-bots-on-twitter-7b7ec57256ae [Accessed 28 February 2018].

Rocha, J. et al. (2006) *Suspect Says he Meant To kill* [online]. Web Archive. Available from: https://web.archive.org/web/20080502132128/http://www.newsobserver.com/102/story/415421.html [Accessed 12 March 2018].

Rodriguez, M., (2013). Representative of Cuba, at the final session of group of governmental experts on developments in the field of information and telecommunications in the context of international security, New York.

Roe, P. (2012). Is securitization a 'negative' concept? Revisiting the normative debate over normal versus extraordinary politics. Security Dialogue, 43(3), 249–266. https://doi.org/10.1177/0967010612443723

Rubin, A. J. (2014) *Jail Sentence in France Over 'Cyber Jihad*' [online]. *New York Times*. Available from: www.nytimes.com/2014/03/06/world/europe/jail-sentence-in-france-over-cyber-jihad.html [Accessed 10 March 2018].

Ruddick, G. (2017) *UK Government Considers Classifying Google and Facebook as Publishers* [online]. *Guardian*. Available from: www.theguardian.com/technology/2017/oct/11/government-considers-classifying-google-facebook-publishers [Accessed 27 January 2018].

Ryan, J. (2011). CIA Director Leon Panetta Warns of Possible Cyber-Pearl Harbor. *ABC News*, *11*.

Sanger, D. E. (2016) *U.S. Cyberattacks Target ISIS in a New Line of Combat* [online]. *New York Times*. Available from: www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html [Accessed 8 May 2016).

Sarkar, A. (2013) *Anonymous and RedHack Breached Israeli Intelligence Agency 'Mossad' Leaked Personal Data of 35K Officials* [online]. Voice of Grey Hat. Available from: www.voiceofgreyhat.com/2013/03/OpIsrael-Anonymous-RedHack-Hacked-Mossad.html [Accessed 10 March 2018].

Satter, R. (2017) *Inside Story: How Russians Hacked the Democrats' Emails* [online]. AP News. Available from: www.apnews.com/dea73efc01594839957c3c9a6c962b8a [Accessed 21 January 2018].

Schultz, E. (2002) 'Security Views', *Computers and Security* [online], 21 (2), 101–112.

Schrage, E. (2017) *Hard Questions: Russian Ads Delivered to Congress* [online]. Facebook Newsroom. Available from: https://newsroom.fb.com/news/2017/10/hard-questions-russian-ads-delivered-to-congress/ [Accessed 1 November 2017)

Schwartau, W., & Foreword By-Draper, J. (2000). Cybershock: Surviving hackers, phreakers, identity thieves, internet terrorists, and weapons of mass disruption. Avalon Publishing Group.

Shachtman, N. (2010) *Cyber Command: We Don't Wanna Defend the Internet (We Just Might Have To)* [online]. Wired. Available from: https://www.wired.com/2010/05/cyber-command-we-dont-wanna-defend-the-internet-but-we-just-might-have-to/ [Accessed 21 March 2018].

Shinkman, P. D. (2013). Former CIA Director: Cyber Attack Game-Changers Comparable to Hiroshima. *US News and World Report*.

Simpson, E. (2012) *War from the Ground Up: Twenty-First-Century Combat as Politics*. Crises in World Politics. London: C. Hurst & Co. (Publishers) Ltd.

Solon, O. (2017a) *US Government Bans Agencies from Using Kaspersky Software Over Spying Fears* [online]. *Guardian*. Available from: www.theguardian.com/technology/2017/sep/13/us-government-bans-kaspersky-lab-russian-spying [Accessed 21 January 2018].

Solon, O. (2017b) *WannaCry Ransomware has Links to North Korea, Cybersecurity Experts Say* [online]. *Guardian*. Available from: www.theguardian.com/technology/2017/may/15/wannacry-ransomware-north-korea-lazarus-group [Accessed 1 March 2018].

Sood, A. K. and Enbody, R. J. (2013) 'Crimeware-as-a-service – A Survey of Commoditized Crimeware in the Underground Market', *International Journal of Critical Infrastructure Protection*, 6, 28–38.

Stavridis, J. (2017) *The United States is Not Ready for a Cyber-Pearl Harbor* [online]. Foreign Policy. Available from: https://foreignpolicy.com/2017/05/15/the-united-states-is-not-ready-for-cyber-pearl-harbor-ransomware-hackers-wannacry/ [Accessed 21 January 2018].

Stevens, T. (2012) 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace', *Contemporary Security Policy* [online], 33 (1), 148–170.

Stohl, M. (2007) 'Cyber Terrorism: A Clear and Present Danger, the Sum of All Fears, Breaking Point or Patriot Games?', *Crime, Law and Social Change* [online], 46 (4–5), 223–238.

Stone-Gross, B., Cova, M., Cavallaro, L., Gilbert, B., Szydlowski, M., Kemmerer, R., Kruegel, C. and Vigna, G. (2009) 'Your Botnet is my Botnet: Analysis of a Botnet Takeover'. Paper presented at ACM Conference on Computer and Communications Security, Chicago, Illinois, 9–13 November.

Stone, J. (2013) 'Cyber War *Will* Take Place!', *Journal of Strategic Studies* [online], 36 (1), 101–108.

Stone, J. (2017) *Theresa May Says the Internet Must Now be Regulated Following London Bridge Terror Attack* [online]. *Independent*. Available from: www.independent.co.uk/news/uk/politics/theresa-may-internet-regulated-london-bridge-terror-attack-google-facebook-whatsapp-borough-security-a7771896.html [Accessed 17 March 2018].

Suiche, M. (2017) *Petya.2017 is a Wiper Not a Ransomware* [online]. Medium. Available from: https://blog.comae.io/petya-2017-is-a-wiper-not-a-ransomware-9ea1d8961d3b [Accessed 28 February 2018].

Swaine, J. (2018) *Twitter Admits Far More Russian Bots Posted on Election Than It Had Disclosed* [online]. *Guardian*. Available from: www.theguardian.com/technology/2018/jan/19/twitter-admits-far-more-russian-bots-posted-on-election-than-it-had-disclosed [Accessed 26 February 2018].

Symantec (2008) *Symantec Report on the Underground Economy* [online]. Symantec. Available from: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf [Accessed 24 March 2018].

Symantec (2017a) *Dragonfly: Western Energy Sector Targeted by Sophisticated Attack Group* [online]. Symantec. Available from: www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks [Accessed 28 February 2018].

Symantec (2017b) *Internet Security Threat Report: Government* [online]. Symantec. Available from: www.symantec.com/content/dam/symantec/docs/reports/gistr22-government-report.pdf [Accessed 28 August 2017].

Symantec (2017c) *WannaCry Ransomware* [online]. Symantec. Available from: www.symantec.com/outbreak/?id=wannacry [Accessed 1 March 2018].

Tait, R. (2017) *Russia's Alleged Interference in Elections Under Spotlight at Prague Summit* [online]. *Guardian*. Available from: www.theguardian.com/technology/2017/may/15/nato-stages-summit-to-counter-alleged-russian-interference-in-elections [Accessed 4 March 2018].

Tamkin, E. (2017) *10 Years After the Landmark Attack on Estonia, is the World Better Prepared for Cyber Threats?* [online]. Foreign Policy. Available from: https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/ [Accessed 28 January 2018].

Times of Israel (2013) *Israel Braces for Massive Cyber-Offensive* [online]. *Times of Israel.* Available from: www.timesofisrael.com/israel-braces-for-massive-cyber-offensive/ [Accessed 10 March 2018].

Toor, A. (2015) *Facebook Ordered to Allow Fake User Names in Germany* [online]. The Verge. Available from: www.theverge.com/2015/7/30/9072257/facebook-real-name-policy-germany [Accessed 27 January 2018].

Travis, A. (2016) *'Snooper's Charter' Bill Becomes Law, Extending UK State Surveillance* [online]. *Guardian*. Available from: www.theguardian.com/world/2016/nov/29/snoopers-charter-bill-becomes-law-extending-uk-state-surveillance [Accessed 18 March 2018].

Traynor, I. (2007) *Russia Accused of Unleashing Cyberwar to Disable Estonia* [online]. *Guardian*. Available from: www.theguardian.com/world/2007/may/17/topstories3.russia [Accessed 28 January 2018].

Trend Micro (2016) *Pawn Storm Targets German Christian Democratic Union* [online]. Trend Micro. Available from: https://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-targets-german-christian-democratic-union/ [Accessed 24 January 2018].

Trend Micro (2017) *Pawn Storm: Back with a Vengeance to Target French Presidential Hopeful Macron* [online]. Trend Micro. Available from: http://blog.trendmicro.co.uk/pawn-storm-back-with-a-vengeance-to-target-french-presidential-hopeful-macron/ [Accessed 24 January 2018)

United Nations (1999) International Convention for the Suppression of the Financing of Terrorism*.* New York: UN General Assembly.

Valeriano, B. and Maness, R. C. (2014) 'The Dynamics of Cyber Conflict Between Rival Antagonists, 2001–11', *Journal of Peace Research* [online], 51 (3), 347–360.

Valeriano, B. and Maness, R. C. (2015) Cyber War Versus Cyber Realities: Cyber Conflict in the International System. Oxford: Oxford University Press.

Waltz, K. N. (2010) *Theory of International Politics*. Long Grove, Illinois: Waveland Press.

Watt, N. et al. (2015) *David Cameron Pledges Anti-Terror Law for Internet After Paris Attacks* [online]. *Guardian*. Available from: www.theguardian.com/uk-news/2015/jan/12/david-cameron-pledges-anti-terror-law-internet-paris-attacks-nick-clegg [Accessed 17 March 2018].

Weimann, G. (2004). Cyberterrorism–How real is the threat? (United States Institute of Peace, Special Report 119). Washington, DC: United States Institute of Peace

Weldes, J., & Saco, D. (1996). Making State Action Possible: The United States and the Discursive Construction of "The Cuban Problem", 1960-1994. Millennium, 25(2), 361–395. https://doi.org/10.1177/03058298960250020601

WikiLeaks (n.d.) *What is WikiLeaks* [online]. WikiLeaks. Available from: https://wikileaks.org/What-is-Wikileaks.html [Accessed 26 February 2018].

WikiLeaks (n.d.) *WikiLeaks – The Podesta Emails* [online]. WikiLeaks. Available from: www.wikileaks.org/podesta-emails/ [Accessed 28 February 2018].

Wilhoit, K. and Haq, T. (2014) *Connecting the Dots: Syrian Malware Team Uses BlackWorm for Attacks* [online]. FireEye. Available from: www.fireeye.com/blog/threat-research/2014/08/connecting-the-dots-syrian-malware-team-uses-blackworm-for-attacks.html [Accessed 12 March 2018].

Winn, Schwartau. (2000), Asymmetrical adversaries, Orbis, Volume 44, Issue 2, 197-205

Withnall, A. et al. (2017) *Five Dead Including Policeman and Attacker in London Terror Incident* [online]. *Independent*. Available from: www.independent.co.uk/news/uk/politics/parliament-shooting-latest-news-man-shot-explosions-heard-westminster-london-a7643686.html [Accessed 12 March 2018].

Woodcock, A. (2017) *Boris Johnson Tells Russia to Halt Cyber Attacks on the West* [online]. *Independent*. Available from: www.independent.co.uk/news/uk/politics/boris-johnson-russia-latest-cyber-attacks-putin-moscow-a8123681.html [Accessed 22 January 2018].

Woolf, N. (2016) *DDoS Attack that Disrupted Internet was Largest of its Kind in History, Experts Say* [online]. *Guardian*. Available from: www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet [Accessed 15 March 2018].

Wright Mills, C. (1956). *The Power Elite.* New York: Oxford University.

Zavrsnik, A.; Levicnik, P. (2015). The public perception of cyber-surveillance before and after edward snowden's surveillance revelations. *Masaryk University Journal of Law and Technology* 9(2), 33-60.