Phobic Cartography: a Human-Centred, Communicative Analysis of the Cyber Threat Landscape

Dr Keith Scott
De Montfort University, Leicester, UK
jklscott@dmu.ac.uk

Abstract: This paper outlines the first stages of a research project mapping the cyber threat landscape. The proliferation and interconnection of networked devices and the ever-growing numbers of users able to damage (accidentally or deliberately) the integrity of this system of systems leads to cyber security adopting a reactive and defensive stance, in which we devise policy on the basis of what *has* happened, rather than what *may* happen, or what we pray will *never* happen. Simultaneously, the growth of the domain leads to silo thinking, and a lack of communication between public and private, civilian and military sectors; there is a need for a synoptic examination of the field, pooling the knowledge of practitioners from across the discipline.

This paper will present the development of the initial proof of concept study, outlining:

a. use of a blended methodology, combining automated quantitative analysis (via Corpus Linguistics tools) with qualitative study (via Critical Discourse Analysis);
b. ethical issues involved in obtaining, storing, and handling of the data;
c. a discussion of initial hypotheses;
d. the intended plan of campaign for moving the project from pilot stage to its full scope;
e. proposals as to how this project may act as a driver for innovation and greater resilience in devising effective cyber security policy.

Mediaeval maps often contained blank space, labelled 'Terra Incognita' and 'Here Be Monsters'; this project will develop a more detailed cartography of the threat landscape of the cyber domain, filling in the blanks and identifying the 'monsters' we fear.

This is an innovative project, examining empirical data drawn from respondents across the discipline, and offers a new way of examining the challenges we face. It allows us to develop a more accurate picture of the threat landscape, and to evaluate what risks we may be ignoring.

Keywords: risk/threat perception, corpus linguistics, critical discourse analysis

1. Introduction

AUTHOR'S NOTE: This paper is a description of the early stages of an ongoing research project; given the submission deadline for the conference, what follows does not discuss analysis of empirical data, and will confine itself to the outlining of certain initial hypotheses. By the time of the ICCWS conference, it will be possible to present the first stage of findings and analyses of the pilot study discussed in Section 5 below

By its very nature, the online environment is uniquely vulnerable to harm; before ARPANET had even been switched on, Willis Ware identified the ways in which a networked system is inherently and inevitably open to attack and exfiltration of data (Ware, 1967); in the world as it now is, the situation is all the more perilous. According to a series of recent reports (Hau et al., 2016; Hewlett Packard Enterprise, 2016; ISACA, 2015; NCA Strategic Cyber Industry Group, 2016), both risk and threat are expanding at a frightening rate, as a direct result of the ever-greater embedding of IT in modern life. Attempts to establish even a minimum standard of effective cyber security are further hampered by the reluctance of governments and companies to reveal breaches of their networks out of fear of reputational damage, and the scale of both unreported and unknown events (Barrett 2015). Much research has been devoted towards establishing a clear and precise taxonomy of cyber threat and risk (see Applegate and Stavrou, 2013; Cebula and Young, 2010; CESG, 2016; ENISA, 2016; Gerić and Hutinski, 2007*;* Jouini, Ben Arfa Rabai and Khedri, 2015*;* Marinos, 2016; Simmons et al, 2014; Zhu, Joseph and Sastry, 2011). However, such an approach neglects one key issue; 'risk', 'threat', and 'vulnerability' are not monolithic terms, capable of only one interpretation (TAG, 2010). An action or event may have many different 'meanings', depending on the context in which it occurs. Consider the action of accessing online material and/or websites which are judged 'inappropriate'; the action is the same in both circumstances, but the nature of the risk/threat depends on the specifics of the situation and the actors involved; an employee

accessing Wikileaks clearly requires a very different response from a teenager surfing websites containing material likely to radicalize. Furthermore, those in charge of cyber security at a national level are generally those with the least technical knowledge; as 'Naughton's Law' puts it, "the more senior the cabinet minister, government official, corporate executive or judge – the weaker their understanding of the Internet will be" (Aldrich, 2012).

This paper examines cyber risk and threat in ways which may make certain readers uncomfortable; firstly, it examines human factors, rather than technology (wetware, rather than hardware or software), and secondly, it investigates, not objective data such as event logs, but *subjective* data, in order to determine the extent to which cybersecurity policy is shaped by belief, and whether and at which points 'expert opinion' shades into 'groupthink'. Underlying this study is a blended methodology which enables the objective analysis of such subjective data. This is entirely fitting with the domain, for 'cyber' has been, from its inception in the work of Wiener and above all the multidisciplinary Macy Conferences, a truly blended discipline, concerned with the interaction of Man and machine, of human and artificial intelligence (see Dupuy, 2009; Heims, 1991; Pias, 2016).

Cyber security is practiced by individual actors (licit and illicit), whose perception of events is inevitably framed by their own personal opinions, education and experience. More than this, each actor operates within a particular, highly specific domain - technical, political, national...- and ascribes to a set of values unique to that domain. All areas of human experience are governed by the codes and ethics (often unconscious and unspoken) of what Haas (1992) terms "epistemic communities", the often "unacknowledged legislators" (in Shelley's phrase) which shape our apparently independent thoughts. The key aspects of these epistemic communities are:

(1) a shared set of normative and principled beliefs;
(2) shared causal beliefs;
(3) shared notions of validity
(4) a common policy enterprise (Haas, 1992)

It is entirely reasonable to expect that any group of individuals dealing with similar issues and experiencing similar training and education will come to form an epistemic community; however, over time, such a community can become trapped in ossified thought patterns and practices, and fall prey to the pressures of "groupthink" (Ricciuti, 2014**a** and 2014**b**; Rose, 2011; Whyte, 1952). The dangers of this in a continually expanding and evolving domain such as cyber security are all too evident. What this project seeks to offer is a means of stepping back from firefighting and the enumeration of current risks/threats, and to examine what practitioners in cyber security consider what may lie ahead, as a means of evaluating underlying perceptions in the various epistemic communities that make up the domain.

There will be those who will have difficulty in accepting the utility of studying subjective opinion; however, there is a long-established tradition of empirically-driven and methodologically robust research (*inter alia* Botterill and Mazur, 2004; Deery, 1999; Kahan, Jenkins-Smith and Braman, 2010; Moussaïd, Brighton, and Gaissmaier, 2015; Slovic, 1987 and 1993; Tversky and Kahneman, 1974; Vasvári, 2015; Weber and Hsee, 1998) which demonstrates that the evaluation of risk/threat is inherently a subjective act, resting on preconception, individual knowledge and epistemic values. As Slovic's (1993) landmark paper puts it:

> there is no such thing as 'real risk' or 'objective risk.' The nuclear engineer's probabilistic risk estimate for a nuclear accident or the toxicologist's quantitative estimate of a chemical's carcinogenic risk are both based on theoretical models, whose structure is subjective and assumption-laden, and whose inputs are dependent on judgement.

Human factor research in cyber security must examine the users and the attackers of systems; it must also consider the opinions and attitudes of those who design and administer those systems.

2. Project Overview

> "Our enemies are innovative and resourceful. And so are we. They never stop thinking about new ways to harm our country and our people. And neither do we." (George W. Bush, 5 August 2004).

President Bush's words have been subject to criticism, if not downright ridicule; however, he was in fact completely right. Any effective security policy *must* be driven, not just by what we know to be the case, but by the consideration of what *could* happen. The aim of this project is to gain a clearer picture of the cyber threat/risk landscape as *perceived* by stakeholders, in order to determine the extent to which a commonality of perception exists (or does not exist) across the various sub-domains that make up the cyber security environment. We wish, in effect, to ask stakeholders across the domain: "What keeps you awake at night?" (Some informal responses are given by Hoff, 2015, Roman, 2015, and Stiennon, 2010.) The aim is to construct a database of 'nightmare scenarios' as envisaged by individuals engaged in cyber security in as many fields as possible (academia, government, the military, law enforcement, the emergency services, finance and commerce) in order to determine:

a. whether different fields perceive a differing range of dangers, or if there is a common set of perceived risks/threats
b. whether responses differ according to level of experience in specific domains (in order to determine whether the growth of epistemic communities has in fact led to 'groupthink')
c. whether different sectors can learn from each other in terms of threat/risk mitigation and prevention (professional firewalls may lead to a lack of shared knowledge and good practice)
d. whether significant correlations exist between perceived threat/risk and specific types of stakeholders (e.g. are less experienced actors more or less likely to perceive original dangers)

Within psychology, much work has been done on developing tools for recording and measuring anxiety in individuals, such as the widely-used Fear Survey Schedule for Children (Revised) or FSSC-R (Ollendick, 1983). However, simply to employ a modified version of this tool is not judged to be appropriate in this case, as the FSSC-R simply lists a series of 80 pre-existing sources of anxiety for selection; this project wants to elicit the respondent's own entirely personal and subjective opinion, as far as possible without priming or leading from the questioner. The method of elicitation used here will hence consist of an anonymous survey, asking the respondent to write a short response within a strictly limited time period (to encourage the respondents to answer without undue reflection, hence reducing the risk of their writing what they calculate to be the 'best' response or 'what they should write'). At this stage, the question to be asked is "In your opinion, what is the greatest danger we face in cyber security?"

It may seem that a project such as this veers into the realm of individual psychology and anxiety; this is of course exactly the point. Cyber security is concerned less with facts that with the ways in which those facts are interpreted and analysed to construct strategy and policy. It is, as Myriam Dunn Cavelty (2008) clearly shows, a human science, shaped by issues of conflicting political and ideological discourses. In order to gain a better understanding of the domain, we must examine what we talk about (or do not talk about), and the ways in which we talk about it.

3. Methodology

This project seeks to elicit from respondents a personal, subjective and unmediated response to the question "In your opinion, what is the greatest danger we face in cyber security?". The question specifically avoids such terms as 'risk', 'threat' or 'vulnerability' to avoid priming respondents to answer in any particular way. Response length will be limited to 100 words maximum (to ensure a rapid, concise answer without overdue reflection) and gathered in the first instance through a paper survey, headed with the necessary ethical caveats and declarations (see (4) below).

The data thus obtained will then be analysed as discussed below in order to determine the 'dangers' identified; these will form a basic taxonomy of actions/events/actors, which will be mapped against the existing taxonomies cited in section (1) above, in order to determine where the perceived dangers map (or do not map) against extant theoretical models. The studies of threat/risk taxonomy cited in section (1) above will be vital in this regard, but the study will also draw on extant databases of real-time contemporary threats, such as the RISI Online Incident Database (http://www.risidata.com/Database), the SYMANTEC listing of threats and risks (https://www.symantec.com/security_response/landing/azlisting.jsp) and - if access is possible - the newly constituted ECB real-time cyber threat database (Arnold, 2016)

It is important to note that this project is not primarily concerned with refining existing taxonomies or developing an entirely new one, but with mapping participant data against these existing models to see the extent to which the two datasets do (not) match. However, a possible further benefit of this study is that it may in fact lead to a more accurate modelling of cyber threat/risk and a more detailed, precise taxonomical model, both through the process of existing taxonomies and the examination of perceived dangers.

This analysis will gain a further level of granularity by examining the responses against the personal data supplied by each respondent, in order to determine whether any meaningful correlations exist between, e.g., nature of threat/risk and respondent's domain of expertise. As stated above, the specific variables the initial project will be recording for each respondent are

a. domain of expertise;
b. level of experience (years in the field);
c. gender.

At a theoretical level, the aim is to subject *subjective*, *qualitative* data to both qualitative *and* quantitative analysis, adopting a blended methodology in order to develop a fuller, more nuanced understanding than would be derived from a unimethodological approach.

The textual material obtained from the survey responses will be subjected to two specific methods of linguistic enquiry. Firstly, *critical discourse analysis (CDA)*, which, as Norman Fairclough (2015) puts it:

> combines *critique* of discourse and explanation of how it figures within and contributes to the existing social reality

CDA offers a way of examining texts as a means of revealing their underlying sociocultural and ideological drivers (such as those which form the underlying presuppositions of an epistemic community), and can be immensely powerful as an analytical tool. However, one of the great dangers of CDA is that it can lead to analyses which are *a priori* and partial, in both senses of the term (incomplete and prejudiced). To be truly valuable, and to defend the activity against accusations of unfounded speculation, CDA must be grounded in empirical data, and base its conclusions on a bedrock of testable evidence.

Such evidence can be provided by recourse to the second of the analytical approaches employed here, namely *corpus linguistics (CL)*. This takes a text or texts, which form the *corpus* to be investigated, converts them to a machine –readable form, and analyses them through the use of various tools in order to reveal significant details concerning word frequency, collocation and to create concordances of keyword appearance. What might be termed the "CDA community" has shown a certain reluctance to embrace CL (Fairclough, 2015: 21), but it can and should be seen as more than a starting point for enquiry, rather an invaluable and inescapable part of the process of a data-driven CDA. The approach taken here follows the work of other corpus linguists, as expressed by Baker *et al.* (2008):

> to show that neither CDA nor CL need be subservient to the other […] but that each contributes equally and distinctly to a methodological synergy.

In the first instance, as outlined in (5) below, a pilot study will be conducted in a largely homogenous sample, drawn from a single domain, and the results derived from this exercise will be used:

a. to test the effectiveness and validity of the experimental approach and underlying methodology
b. to establish a baseline set of results/data.

The data obtained in this study will be used to establish a *reference corpus*, against which further studies can be measured, in order to determine whether stakeholders do in fact display domain-specific anxieties. This is where the ability of CL to perform robust analysis of keywords is vital. ("A keyword may be defined as a word which occurs with unusual frequency in a given text. This does not mean high frequency but unusual frequency, by comparison with a reference corpus of some kind." (Scott, 1997) A helpful discussion of the statistical principles underlying calculations of keyness is Gabrielatos and Marchi, 2011).

The blended approach adopted here will, it is believed, allow the researchers to more fully assess the nature of the anxieties driving stakeholders in the cyber domain, and hence lead to a more informed discussion of how to evaluate and assess these concerns. However, in order for the analysis to be truly successful (and in fact in order that the research may actually be carried out) there are a number of key ethical issues that must be addressed.

4. Ethical Concerns

It is of course a *sine qua non* of effective research that it be carried out in an ethical manner, but a project such as this requires close observation of and adherence to a number of pre-existing codes of practice, notably those produced by JISC (the Joint Information Systems Committee), the ESRC (Economic and Social Research Council), and the British Academy. It must also comply with certain key pieces of British legislation (most notably the Data Protection Act 1998). In order to address these issues, the following steps will be taken:

a. Respondent anonymity will be strictly preserved; no respondent will be identifiable by name, and care will be taken to ensure that the personal data collected will not allow the identification of any individual.
b. Right of withdrawal: any respondent will have the right to withdraw from the survey at any time, and in such a case, their data will be destroyed.
c. Respondents will have the right to enter as much or as little personal data as they wish (e.g. they may choose not to give their age, gender, or domain/length of expertise); while this reduces the granularity of the results and the ability to determine significant correlations between response and individual characteristics, it does mitigate against concerns of possible identification.
d. All data will be held securely; data held in electronic form will be encrypted, and access to it will be limited to the researcher.
e. Any published data will undergo a further process of review to ensure that confidentiality and anonymity guidelines are followed scrupulously.

Strict adherence to the existing institutional and legislative guidelines hence ensures that the project is conducted as it should be, and clear signposting of the processes followed (presented to respondents as a cover sheet to the survey) will, it is hoped, help to ensure as full and honest a series of responses as possible.

5. Pilot Study

The initial pilot survey will be run in the first term of the 2016-2017 academic year, at the UK university at which the researcher is employed. The sample group will consist of Undergraduate and Postgraduate students and teaching staff in Computer Science (sample size ≈ 100). This group has been selected for the following reasons:

a. They all have a level of knowledge of the cyber security domain;
b. They have differing levels of experience in the domain (and level of experience is one of the key variables under investigation);
c. There will be both male and female respondents, allowing an initial examination of the effect (if any) of gender on responses;
d. The pilot survey can be run with large groups quickly and effectively within the university teaching schedule.

6. Next Steps

The pilot survey outlined above will allow an initial ability to road-test the underlying methodology, and to fine-tune issues such as question wording. It will also provide a set of data which will be used to establish a reference corpus and initial taxonomy of 'dangers'; this latter point is itself a useful research topic, in that it will allow the project to determine whether the existing taxonomies of risk/threat events matches with the real concerns of respondents. It is entirely possible that this project will identify issues which are not present in existing taxonomies, or which need to be prioritized in the development of strategy and policy. The aim is that

the initial results and analysis will be discussed at the 2017 ICCWS Conference (which will also offer an opportunity to run the survey among a population which is both large and highly diverse).

The next step will be (*mutatis mutandis*) to roll the survey out to a larger and wider range of respondents, and to move from academia to other sub-domains within the field. It is intended that the second run of the survey will be conducted at a workshop in January of 2017 attended by stakeholders in the field drawn from the UK public and private sectors. This group will be smaller than that in the pilot survey (≈ 50) but will offer a diversity of age and experience across differing domains.

The project will give a clearer picture of perceived threats/risks across the cyber domain, and determine areas of vulnerability which are as yet under-protected. The true challenge is not conducting the research, but finding ways for disseminating the findings as widely as possible to stakeholders. It is believed that this research is of value not just in itself, but as a way of driving innovation in the future development of effective strategic cyber security policy. While the first step in disseminating the findings will be through academic publishing, the ultimate aim is to determine the best ways of sharing the data with as many practitioners as possible.

7. Initial Hypotheses

> "The great tragedy of science—the slaying of a beautiful hypothesis by an ugly fact". (Huxley, 1901).

These are highly provisional, interim hypotheses, but they mark out the initial areas of interest. As with all research, they are constructed, not to be *proved*, but to be *tested*.

a. The *null hypothesis* (H_0) is that there will be no significant differences in the responses, and that a common series of risks/threats will be identified.
b. There will be a correlation between level of experience and technical detail of the 'danger' identified (i.e. greater experience will lead to a greater fixation on technicalities)
c. Respondents with a greater degree of experience will display a greater commonality of response (the more one identifies with the epistemic community, the greater the 'groupthink')
d. Respondents with lower levels of experience will display a greater degree of originality of response ('groupthink' has not set in)
e. Gender of respondents will correlate with nature of threat/risk identified (allowing initial discussion of the nature of Computer Science as a 'masculine' subject area; see Sax et al, 2015, Stepulevage and Plumeridge, 1998)

These hypotheses set out the starting point for the project; it is expected that analysis of the actual data will identify many further avenues for research. The blended methodology outlined here is portable, and can be applied in fields such as textual attribution, while the *analytical* tools also hold out the possibility of *generating* precisely targeted, linguistically, epistemically and culturally appropriate tools of information warfare and counter-radicalization. These are, however, outside the current realm of enquiry.

8. Conclusion

As stated at the outset of this paper, the cyber realm is dangerous, and becoming ever more so; no one project can hope to produce a completely safe world. What is presented here is a first step to examining what it is that stakeholders in the field actually fear, as a means of identifying possible areas that we are as yet not engaging with. This project is an exercise in mapping the cyber landscape, and identifying the zones marked 'Here Be Monsters'. By the end of even the pilot stage of the research, it is believed that we will have helped to reduce the areas of the map consisting of blank space and the legend 'Terra Incognita'.

Bibliography

Aldrich, R. (2012) "James Bond, "Skyfall" and GCHQ", [online], *warwick.ac.uk*, 18 November, www2.warwick.ac.uk/fac/soc/pais/people/aldrich/vigilant/lectures/gchq/skyfall/.

Applegate, S. and Stavrou, A. (2013) "Towards a Cyber Conflict Taxonomy", *5th International Conference on Cyber Conflict*, K. Podins, J Stinissen, M.Maybaum (Eds), NATO/CCD/COE Publications, Tallinn.
Arnold, M. (2016) "European Central Bank creates cyber attack real-time alert system", [online], *Financial Times*, 12 May, https://www.ft.com/content/5113afae-1833-11e6-bb7d-ee563a5a1cc1.
Baker, P. et al (2008) "A useful methodological synergy? Combining critical discourse analysis and corpus linguistics to examine discourses of refugees and asylum seekers in the UK press", *Discourse and Society,* 19, pp. 273-306.
Barrett, D. (2015) "Frauds worth £12bn go unreported, says report", [online], *Daily Telegraph*, 19 March, www.telegraph.co.uk/news/uknews/crime/11480715/Frauds-worth-12bn-go-unreported-says-report.html.
Botterill, L., and Mazur, D. (2004) *Risk & risk perception: A literature review*, Rural Industries Research and Development Corporation, Canberra.
Cebula, J. J. and Young, L. R. (2010) *A Taxonomy of Operational Cyber Security Risks*, CMU/Software Engineering Institute, Pittsburgh, PA.
CESG (2016) *Common Cyber Attacks: Reducing The Impact*, CESG, London.
Deery, H. A. (1999) "Hazard and Risk Perception among Young Novice Drivers", *Journal of Safety Research*, Vol. 30, No. 4, pp 225–36.
Dunn Cavelty, M. (2008) *Cyber-Security and Threat Politics*, Routledge, London.
Dupuy, J-P, tr. M.B DeBevoise (2009) *On the Origins of Cognitive Science: The Mechanization of Mind*, MIT Press, Cambridge Mass.
ENISA (2016) "Existing taxonomies", [online], www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies.
Fairclough, N. (2015) *Language and Power,* 3rd ed., Routledge, London.
Gabrielatos, C. and Marchi, A. (2011) "Keyness: Matching metrics to definitions", Paper read at Corpus Linguistics in the South Conference, University of Portsmouth, 2011. Available at: eprints.lancs.ac.uk/51449/4/Gabrielatos_Marchi_Keyness.pdf.
Gerić, S. and Hutinski, *Ž. (2007) "*Information System Security Threats Classifications", *Journal of Information and Organizational Sciences,* Vol. 31, No. 1, pp 51-61.
Haas, P. M. (1992) "Introduction: Epistemic Communities and International Policy Coordination", *International Organization*, Vol. 46, No. 1, pp 1-35.
Hau, B. et al. (2016) *M-Trends Emea Edition 2016*, Mandiant Consulting/FireEye, Alexandria, VA.
Heims, S.J. (1991) *The Cybernetics Group*, MIT Press, Cambridge, Mass.
Hewlett Packard Enterprise (2016) *HPE Security Research: Cyber Risk Report 2016*, Hewlett Packard Enterprise Security Research, Bracknell, UK.
Hoff, K. (2015) "Cybersecurity and Things that Keep Us Awake at Night", *linkedin*, 11 August**,** www.linkedin.com/pulse/cybersecurity-things-keep-us-awake-night-knut-hoff.
Huxley, T.H. (1901) "President's Address to the British Association for the Advancement of Science, Liverpool Meeting, 14 Sep 1870", *The Scientific Memoirs of Thomas Henry Huxley*, Vol. 3, D. Appleton & Co., London, p 580.
ISACA (2015) "ISACA Identifies Five Cyber Risk Trends for 2016", [online], *ISACA*, 16 December, www.isaca.org/About-ISACA/Press-room/News-Releases/2015/Pages/ISACA-Identifies-Five-Cyber-Risk-Trends-for-2016.aspx.
Jouini, M., Ben Arfa Rabai, L., and Khedri, R. (2015) "A Multidimensional Approach Towards a Quantitative Assessment of Security Threats", *Procedia Computer Science* 52, pp 507 – 514.
Kahan, D. M., Hank Jenkins-Smith, H., and Braman, D. (2010) "Cultural cognition of scientific consensus", *Journal of Risk Research*, Vol. 14, No. 2, pp 147-74.
Marinos, L. (2016) *ENISA Threat Taxonomy: A tool for structuring threat information*, ENISA, Heraklion.
Moussaïd, M, Brighton, H., and Gaissmaier, W. (2015) "The amplification of risk in experimental diffusion chains", *Proceedings of the National Academy of Sciences*, Vol. 112, No. 18, pp 5631-6.
NCA Strategic Cyber Industry Group (2016) *Cyber Crime Assessment 2016*, National Crime Agency, London.
Ollendick, T.H. (1983) "Reliability and Validity of the Revised Fear Survey Schedule for Children (FSSC-R)", *Behaviour, Research and Therapy*, 21, pp 685–692.
Pias, C. ed. (2016) *Cybernetics - The Macy Conferences 1946-1953. The Complete Transactions*, University of Chicago Press, Chicago.
Ricciuti, J. E. (2014**a**) *Groupthink: A Significant Threat to the Homeland Security of the United States*, Master's Thesis, Naval Postgraduate School, Monterey, CA.

--- (2014**b**) "Groupthink: A Significant Threat to the Homeland Security of the United States - Executive Summary", [online], *Homeland Security Affairs: The Journal of the NPS Center for Homeland Defense and Security*, Vol. xii, www.hsaj.org/articles/3570.
Roman, D. (2015) "5 Things That Keep Cyber Security Pros Awake At Night", [online], *Wall Street Journal*, 30 April, blogs.wsj.com/briefly/2015/04/30/5-things-that-keep-cyber-security-pros-awake-at-night/
Rose, J.D. (2011) "Diverse Perspectives on the Groupthink Theory – A Literary Review", *Emerging Leadership Journeys*, Vol.4, no. 1, pp 37-57.
Sax, L. J. et al (2015) "Anatomy of an Enduring Gender Gap: The Evolution of Women's Participation in Computer Science". Paper read at the 2015 Annual Meeting of the American Educational Research Association. Chicago, IL.
Scott, M (1996) *WordSmith Tools Manual*, Oxford University Press, Oxford.
Simmons, C. B. et al (2014) "AVOIDIT: A Cyber Attack Taxonomy", *Proceedings of the 9th Annual Symposium on Information Assurance (Asia '14),* June, Albany, NY, pp 2-12.
Slovic, P. (1993) "Perceived risk, trust, and democracy", *Risk Analysis,* Vol. 13, No. 6, pp 675–82.
Slovic, P. (1987) "Perception of risk", *Science*, Vol. 236, No. 4799, pp 280–5.
Stepulevage, L and Plumeridge, S (1998) "Women Taking Positions within Computer Science", *Gender and Education*, Vol. 10, No. 3, pp 313-326.
Stiennon, R. (2010), "Seven Cyber Scenarios To Keep You Awake At Night", [online], *forbes.com*, 29 April, www.forbes.com/sites/firewall/2010/04/29/seven-cyber-scenarios-to-keep-you-awake-at-night/#4dd2d62a5e6e.
TAG (2010) "Threat, vulnerability, risk – commonly mixed up terms", [online], *threatanalysisgroup.com*, 3 May, www.threatanalysis.com/2010/05/03/threat-vulnerability-risk-commonly-mixed-up-terms/.
Tversky, A., and Kahneman, D. (1974) "Judgment under Uncertainty: Heuristics and Biases", *Science*, Vol. 185, No. 4157, pp 1124-31.
Vasvári, T. (2015) "Risk, Risk Perception, Risk Management", *Public Finance Quarterly*, Vol. 60, No. 1, pp 29-48.
Ware, W.H. (1967) "Security and privacy in computer systems", *AFIPS '67 (Spring) Proceedings of the April 18-20, 1967, Spring Joint Computer Conference*, ACM, New York, pp 279-82.
Weber, E.U. and Hsee, C. (1998) "Cross-Cultural Differences in Risk Perception, but Cross-Cultural Similarities in Attitudes towards Perceived Risk", *Management Science,* Vol. 44, No. 9 (Sep., 1998), pp 1205-17.
Whyte, W.H. (1952) "Groupthink", *Fortune*, March, pp 114-17, 142, 146.
Zhu, B., Joseph, A., and Sastry, S. (2011) "A Taxonomy of Cyber Attacks on SCADA Systems", *ITHINGSCPSCOM '11 Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, pp 380-88.