An Evidence Quality Assessment Model for Cyber Security Policymaking

Sneha Dawda, Madeline Carr, Atif Hussain, Siraj Shaikh, Alex Chung

To cite this version:

Sneha Dawda, Madeline Carr, Atif Hussain, Siraj Shaikh, Alex Chung. An Evidence Quality Assessment Model for Cyber Security Policymaking. 12th International Conference on Critical Infrastructure Protection (ICCIP), Mar 2018, Arlington, VA, United States. pp.23-38, 10.1007/978-3-030-04537-1_2 . hal-02076296

HAL Id: hal-02076296
https://hal.science/hal-02076296

Submitted on 22 Mar 2019

Chapter 2

AN EVIDENCE QUALITY ASSESSMENT MODEL FOR CYBER SECURITY POLICYMAKING

Atif Hussain, Siraj Shaikh, Alex Chung, Sneha Dawda and Madeline Carr

Abstract A key factor underpinning a state's capacity to respond to cyber security policy challenges is the quality of evidence that supports decision making. As part of this process, policy advisers, essentially a diverse group that includes everyone from civil servants to elected policy makers, are required to assess evidence from a mix of sources. In time-critical scenarios where relevant expertise is limited or not available, assessing threats, risk and proportionate response based on official briefings, academic sources and industry threat reports can be very challenging. This chapter presents a model for assessing the quality of evidence used in policymaking. The utility of the model is illustrated using a sample of evidence sources and it is demonstrated how different attributes may be used for comparing evidence quality. The ultimate goal is to help resolve potential conflicts and weigh findings and opinions in a systematic manner.

Keywords: Evidence quality assessment, cyber security, policymaking

1. Introduction

Research in cyber security tends to focus on technical factors, vulnerabilities and solutions. Some research focuses on the "human dimension," but these studies look predominantly at end-users. However, regulatory and policy frameworks also have significant implications with regard to cyber security. Policy advisers, sometimes with limited relevant expertise and often in time-critical scenarios, are asked to assess evidence from a mix of sources such as official threat intelligence, academic research and industry threat reports. The diverse evidence base is then used to make judgments about threats, risk, mitigation and consequences, and offer advice that shapes the national regulatory landscape, foreign and domestic security policy and/or various public and private sector initiatives. The research presented in this chapter is motivated by the need to better support decision making in the United Kingdom policy community when interpreting, evaluating and understanding evidence related to cyber security.

The decisions made by policy advisers in many ways shape the landscape and ecosystem within which other actors operate. A better understanding of the influences on such decision making is essential to identifying how the policymaking community can be supported in making sound policy decisions that foster continued innovation and mitigate current and future cyber security threats.

This research is motivated by the following key questions:

- What evidence do U.K. policymakers rely upon?
- What is the quality of the evidence?
- How effective are the judgments about threats, risks, mitigation and consequences based on the evidence?

Understanding how U.K. policymakers select evidence, why they place one source over another and how adeptly they can recognize possible weaknesses or flaws in evidence are central to addressing these research questions.

This chapter presents a simple model that supports the quality assessment of a variety of evidence sources used in cyber security policymaking. Given the diversity of the sources, some of which may be conflicting or contradictory, an evaluation of the quality of the available evidence can help resolve potential divergence. The proposed Evidence Quality Assessment Model (EQAM) is a two-dimensional map that uses a set of attributes to position evidence samples relative to each other. The attributes are derived from the literature and from a series of semi-structured interviews of policy advisers from the U.K. cyber security policy community.

2. Evidence and Policy Challenges

Policymakers use a diverse evidence base to make judgments about threats, risk, mitigation and consequences, and offer advice that shapes the national regulatory landscape, foreign and domestic security policy, and a range of public and private sector initiatives. In this context, evidence assessment for policymaking is a particular problem for three reasons:

- First, some of the evidence is contradictory and/or potentially carries within it specific agendas or goals that may impede its rigor and reliability. The "politicization" of cyber security evidence is increasingly problematic because states may trust threat intelligence based on whether the sources are located within their sovereign borders instead of the quality of the research.

- Second, it is extremely difficult to conclusively attribute cyber attacks and to quantify the costs of cyber insecurity. For policy advisers, the lack of clarity about the concrete financial implications of cyber security vulnerabilities and incidents makes it challenging to develop sound responses. Without clarity about the role of specific communities of perpetrators, policy alternatives can be disconnected from the real threats, targeting individuals or groups who may not, in fact, be the key malicious actors. These challenges mean that existing evidence often only partially supports policy advisers' evaluations of cyber security risks, threats and consequences – and the resulting recommendations.

- Third, the cyber security landscape is developing rapidly and spans many areas, including national security, human rights, commercial concerns and infrastructure vulnerabilities. Consequently, policy advisers must balance a range of possibly conflicting interests that compete for attention. Different conceptions of what "cyber security" means to different policy communities raises real impediments to a unified response. Network security, economic security, privacy and identity security, and data security all represent diverse conceptions and priorities that are commonly referred to as "cyber security."

The rise of evidence-based policy making under the Blair government prompted several studies focused on the way U.K. policy advisers engage with and interpret evidence. Early in this process, Solesbury [27] argued for careful critical analysis of what exactly constitutes "evidence," pointing out the relationship between knowledge and power, and the role that selecting and interpreting evidence plays under this approach to policymaking. This leads to several questions. What evidence do U.K. policymakers rely upon in this context? What is the quality of the evidence? How effective are the judgments about threats, risks, mitigation and consequences based on the evidence? Understanding how U.K. policymakers select evidence, why they weight one source over another and how adeptly they can recognize possible weaknesses or flaws in evidence are central to addressing these questions.

Evidence-based policymaking has been a core concept in contemporary U.K. policymaking since the 1990s. However, there is a lack of agreement in the policy community on the level of clarity and definition of evidence, and the academic or scientific standards that should be applied to the evidence. This has resulted in the popularization and politicization of evidence-based policymaking as a catch-phrase instead of a policy process that utilizes rigorous methodology and systematic analysis [6, 16, 17, 21, 34]. In addition, modern technological concerns are increasingly complex and, therefore, render an approach that solely relies on evidence-based policymaking rather simplistic compared with nuanced forms of policymaking where evidence is contextualized within the policy process and objectives. Evidence-based policymaking involves a critical approach based on replicable scientific studies. It responds to the belief that past policy decisions may have relied on the biased selection of evidence. It also seeks to address the influence of untested views of individuals or groups who represent vested interests, tradition, ideology, prejudice and/or speculation [4]. Evidence-based policymaking therefore attempts to reduce uncertainty and increase clarity in decision making by drawing on rigorous information to turn policy goals into concrete, achievable actions [26].

In recent years, the policymaking landscapes in some developed countries have led to innovative governance models for dealing with cyber security instead of relying on evidence-based policymaking or other traditional forms of policymaking such as the rational model, implied model, enlightenment model, knowledge-driven model, political model and tact model [16, 23, 32]. In the United Kingdom, newer systems take the form of adaptive (or agile) policymaking (APM). Adaptive policymaking explicitly accounts for deep uncertainties prompted by the speed with which technologies evolve [13]; this is in direct contrast to classical policymaking approaches that are ill-suited to managing the complexities associated with cyber security [16, 29, 33].

The adaptive paradigm also markedly departs from tradition by incorporating a strategic vision and framework from which policies are derived to prepare for negative eventualities; but it is also sufficiently flexible and dynamic to meet changing circumstances through short-term actions [29]. In order to facilitate this process, the proposed Evidence Quality Assessment Model seeks to validate evidence quality in a timely fashion, enabling policymakers to understand the implications of utilizing evidence and making the best judgments based on the available evidence.

3. Assessing Evidence Quality

The Strategic Policy Making Team at the U.K. Cabinet Office [28] describes evidence as expert knowledge, published research, existing statistics, stakeholder consultations, previous policy evaluations, Internet resources, costing of policy options and results from economic and statistical modeling. Davies [4] has structured different types of evidence into controlled experimental trials and studies, social surveys, econometrics, expert advisory groups, public attitudes, ethical values such as belief and aspirations, and research evidence from relevant sources that have been systematically searched, critically appraised and rigorously analyzed according to explicit and transparent criteria. However, Nutley et al. [22] note that, in practice, the U.K. public sector uses a more limited range of evidence, specifically, research and statistics, policy evaluation, economic modeling and expert knowledge.

3.1 Subject Interviews

As part of this research, sixteen policy advisers and U.K. civil servants were interviewed between November 2017 and February 2018. The subjects were employed across U.K. Government departments, including the Cabinet Office, Department for Digital, Culture, Media and Sport (DCMS), Home Office, Foreign and Commonwealth Office (FCO), Her Majesty's Revenue and Customs (HMRC) and Department of Communities and Local Government (DCLG), along with specialist agencies such as the London Mayor's Office for Policing and Crime, National Crime Agency (NCA) and National Police Chiefs' Council (NPCC).

The interviews revealed that a very wide variety of sources are used as potential evidence for policy analysis. These include research into trends from open-source material, forums, news articles, daily bulletins, media and newsletters; threat intelligence reports from academia and think tanks; intelligence reports from domestic and overseas sister agencies and restricted government information; and crime surveys for England and Wales, action fraud and general policing data from the National Crime Agency (NCA), cyber security breach surveys and Office of National Statistics (ONS) data sources and reports. Threat intelligence reports, surveys, case studies etc. are received from government sources (restricted and unrestricted), as well as from information technology giants such as BAE Systems, IBM, Microsoft, Cisco and FireEye. Policy advisers also access classified information released by law enforcement agencies and the intelligence community.

This study has not reviewed information from the various sources because the proposed model accounts for the use of such evidence. However, while one may assume that the evidence is reliable, it should be considered in the context of multiple (possibly transnational) agencies that may be trusted to varying levels.

With regard to the use of evidence in policymaking, it should be noted that decision making is often based on the best available evidence, although it may not be perfect. If one individual does not offer an informed view, then someone else who is less informed may make the decision; therefore, time is critical for a short-term response. Long-term problems are seen differently because ample time is available to institute the right approaches and gather the necessary evidence. In order to evaluate policy options and identify the options that will genuinely work, it is necessary to validate ideas and understand how to improve the process.

Two dimensions of evidence quality are proposed: (i) evidence sources; and (ii) evidence credibility.

3.2 Evidence Source

The evidence sources include data sources and human sources, both of which pose unique attributes with regard to quality.

Data Sources. Technical and survey data have been used as evidence for a variety of tasks ranging from attributing malware fragments [24] to identifying emerging trends in the technical and social spheres [30]. An artifact of evidence is subject to several considerations:

- The scope of data collection is not always perfect. As such, it may not always be complete to allow inferences. This is particularly problematic when it comes to using industry sources for threat intelligence and technological trends, which tend to increase the commercial advantage to the organizations that collect and publish the data.

- There are questions about the potential volatility of digital sources such as computers and networks [2]. The transient nature of such sources cannot be ignored because of the reliance on digital infrastructures for threat sensing. Additionally, digital forensics is subject to strict chain of custody and preservation procedures, any violation of which could cast doubt on the integrity of data.

- Analysis of data, often abstract and agnostic in nature, is open to interpretation. For example, traces of malware activity may be used to evaluate the sophistication of an attacker, which, in turn, is used as a critical criterion for attribution [7].

The subjects interviewed in the research hailed from a number of organizations. Organizations with a tradition of national data collection and statistical excellence, such as the Office of National Statistics (ONS) in the United Kingdom, are considered to be reliable sources, primarily because of their methodology and objectivity, which bolster confidence when the evidence they provide is cited in reports to ministers.

Human Sources. Human sources, either subjects of interest observed via some channel or knowledgeable experts who offer opinions, are also valuable sources of evidence. With expert knowledge and commentary comes the burden of bias and beliefs, and context and connotation. Indeed this is a substantial challenge because cyber security, as a social construct, takes various forms, including a political discourse that invokes the idea of a cyber "Pearl Harbor" [5]. Objective analysis of information from human sources is sensitive to the credibility of the entity that collects the information and the transparency of its collection method.

3.3 Evidence Credibility

This section discusses credibility in terms of the methodology and provider, both of which ultimately underpin the confidence in the presented evidence.

Methodology. The focus is on published forms of evidence to which some notion of methodology and organization could be attributed. Of course, confidential sources of threat intelligence would follow official protocols; the judgment of their quality would, therefore, be left to the relevant intelligence and policy communities.

A challenge with cyber security is the heightened interest that it attracts due to novel technological aspects. This interest lends itself to hype as well as a lack of balanced technical and broad knowledge to help policy perspectives. Indeed, the level of reporting on cyber security is routinely criticized. Lee and Rid [12] state:

> *"Cynical and overstated reports ultimately lower the quality of bureaucratic procedures and decision making. First, such reports inform decisions at both the strategic and tactical level. Intelligence reports take highly technical data, combine the information with the interpretations of analysts, and give a bottom line to fill knowledge gaps in the government and guide action ... Simply put: many of these reports are incomplete or inaccurate."*

Appropriate methodologies and analyses are key to presenting substantial claims that result from the evidentiary artifacts. These range from empirical analyses of data sets to qualitative and quantitative analyses of socio-technical information.

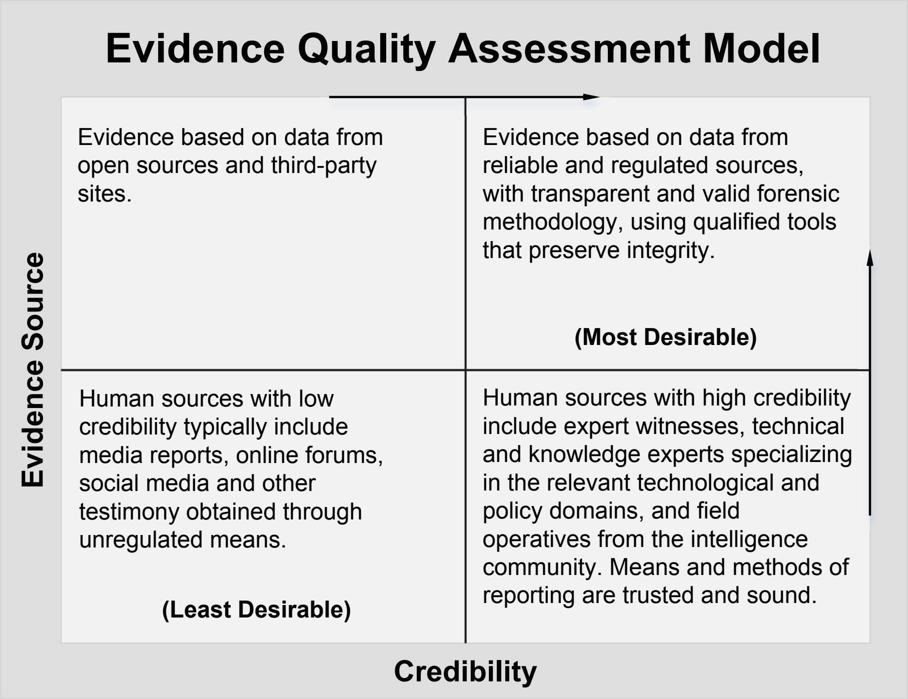
The legal imperative regarding cyber attacks [8] implies that several attributes are important if evidence is to be used for policy decisions related to legislation or regulation, or if a state is to respond under international norms and law. Especially important is transparency with regard to how evidence is collected, processed, stored and handled.

Provider. Over the past two decades, an entire industry dedicated to cyber threat intelligence has emerged. Cyber threat intelligence is an umbrella term that refers to the collection and analysis of threat-related activity from open-source reports, social media and dark web sources. The industry includes major information technology and telecommunications companies, such as IBM and Cisco, and niche operators, such as FireEye, that are focused on advanced threats. The industry is a major source of information for government agencies and corporations for policymaking and for making decisions about security investments.

Geopolitical affiliations have the potential to cast a shadow on providers even when their technical capabilities are acknowledged. Kaspersky Lab, headquartered in Moscow, Russia, is an example of a provider with very well regarded technical capabilities, including its efforts in detecting Stuxnet [10]. However, Kaspersky Lab software is viewed with suspicion because of the potential for its compromise by Russian Government entities. The interviews conducted in this research also revealed that threat intelligence reports from the company are discredited as a result of its reputation.

The situation in industry is paralleled by that for government agencies. An example is the National Cyber Security Centre (NCSC) in the United Kingdom, whose technical mission is to provide advice and guidance on cyber-related threats to public and private sector stakeholders. The National Cyber Security Centre provides products in various formats, from brief weekly threat reports with little transparency or detail [19] to detailed data-driven guidance with clarity on methodological approaches and data provenance, such as analysis of active cyber defense policy [14]. Indeed, the quality challenges when dealing with a complex evidence base are clearly enunciated in the threat report [19]:

> *"[It is] difficult to draw concrete conclusions – especially about causality – from our current analysis of the data. There are also some anomalies in the data that we don't understand yet. We've tried our best to be clear about our confidence in our conclusions in this paper. People will almost*



Evidence based on data from open sources and third-party sites.

Evidence based on data from reliable and regulated sources, with transparent and valid forensic methodology, using qualified tools that preserve integrity.

Human sources with low credibility typically include media reports, online forums, social media and other testimony obtained through unregulated means.

Human sources with high credibility include expert witnesses, technical and knowledge experts specializing in the relevant technological and policy domains, and field operatives from the intelligence community. Means and methods of reporting are trusted and sound.

Figure 1. Evidence Quality Assessment Model.

> *certainly disagree with some of the conclusions we draw here. That's probably a good thing as it starts to engender an evidence-based discussion about what cyber security policy should look like going forward."*

3.4 Evidence Quality Assessment Model

This section presents the Evidence Quality Assessment Model, which reflects the diverse nature of evidence sources and enables the quality of evidence to be characterized despite the diversity. The proposed model is based on the attributes discussed in Sections 3.2 and 3.3.

Figure 1 shows the proposed model. It provides a simple representation of the quality of evidence using a two-dimensional map, where the vertical axis captures the split in evidence sources between data sources and human sources, and the horizontal axis expresses credibility based on the methodology and provider. For example, the vertical axis could place the value of data sources over the value of human sources in establishing the quality of evidence. As a scale, it helps map evidence that combines both data and human sources to a quality measure. The horizontal axis, on the other hand, is a continuum, where credibility is judged on a case by case basis for each piece of evidence.

The division into four quadrants assists in mapping pieces of evidence to a relative quality metric in an intuitively appealing manner.

4. Model Analysis

This section illustrates the application of the Evidence Quality Assessment Model in a typical use case involving the analysis of a collection of evidence.

4.1 Sample Selection

The application of the Evidence Quality Assessment Model is illustrated using an evidence assessment exercise that was performed internally by a subset of the authors of this chapter. The ten pieces of evidence shown in Table 1 were chosen. The selection was deliberately broad and diverse to help understand whether the proposed model helps achieve consensus across varying levels of evidence quality. Given the current focus on the U.K. policymaking community, all the evidence items were mentioned during the interviews or in the U.K. policy discourse.

4.2 Scoring Analysis

A subset of the authors of this chapter, with expertise in technology and policy, assessed the evidence items individually. The assessors scored each item on the Evidence Quality Assessment Model vertical and horizontal scales shown in Figure 1. Similar scores were consolidated and disparate scores were discussed and a common score was negotiated by the assessors. Table 2 shows the consolidated and negotiated source and credibility scores for the ten evidence items.

Figure 2 shows the ten evidence items placed on the Evidence Quality Assessment Model map according to their consolidated and negotiated source and credibility scores listed in Table 2.

The following details pertaining to the ten evidence items provide insights into the consolidated and negotiated source and credibility scores, and their placement on the Evidence Quality Assessment Model map:

- **NCSC Weekly Threat Report (E-1):** This report is broken up into five threat bulletins. Each bulletin has distinct topics and its analysis varies. For example, the first bulletin includes facts from a survey that communicate the risk and support the claims, whereas the last bulletin only states the claims without providing details about the analysis and findings. This makes the overall threat report slightly harder to assess because the same methodology was not applied across the report. Furthermore, in some instances, the sources of evidence were not stated. For example, a Daesh (ISIL) claim was presented without any validation of its sources. Another example is that the data coverage for Android malware left some key questions unanswered: Which phone models were

Table 1. Ten evidence items used to illustrate the proposed model.

Provider	**Description**
NCSC	NCSC provides advice and support to the U.K. public and public sectors for addressing computer security threats. The *NCSC Weekly Threat Report* issued on December 22, 2017 contains evidence on distinct security issues [19]. *NCSC Password Security Guidance* contains advice for administrators on determining password policy; it advocates a dramatic simplification of the current approach at the system level [18].
CVE	Common Vulnerabilities and Exposures (CVE) catalogs cyber security vulnerabilities and exposures related to software and firmware in a free "dictionary" that organizations can use to to improve their security postures. *CVE-2014-0160* refers to the Heartbleed vulnerability found in the OpenSSL software library [20].
BBC	The British Broadcasting Corporation (BBC) is a British public broadcaster. *BBC 2017* highlights the main technology events that occurred in 2017 [3].
Foresight	Foresight projects, produced by the U.K. Government Office for Science, provide evidence to the policy community. The *Future of the Sea: Cyber Security* project report informs the U.K. maritime sector about cyber security response [25].
FireEye	FireEye is a cyber security company that provides products and services that protect against advanced cyber threats. *FireEye Operation Ke3chang* investigates the Ke3chang cyber espionage campaign [31]. Mandiant is a cyber security firm acquired by FireEye in 2013. The *Mandiant APT1* report implicates China in cyber espionage activities [15].
IBM	IBM X-Force Research is a security team that monitors and analyzes security issues, and provides threat intelligence content. *IBM 2017* reports IBM X-Force Research's findings for 2017 [9].
Kaspersky	Kaspersky Lab is a multinational cyber security and anti-virus provider headquartered in Moscow, Russia. The *Kaspersky Global Report* covers security events from around the globe that occurred in 2017 [11]. *Securelist* is a Kaspersky blog; an article in the blog discusses how to survive attacks that seek to access and leak passwords [1].

tested? Are all Android phones at risk? Are there any impacts on Android tablets?

Table 2. Consolidated and negotiated scores for the ten evidence items.

Quality Criteria	**E-1**	**E-2**	**E-3**	**E-4**	**E-5**	**E-6**	**E-7**	**E-8**	**E-9**	**E-10**
Source	8	15	6	12	7	13	17	6	12	2
Credibility	53	65	33	49	47	52	56	63	27	17

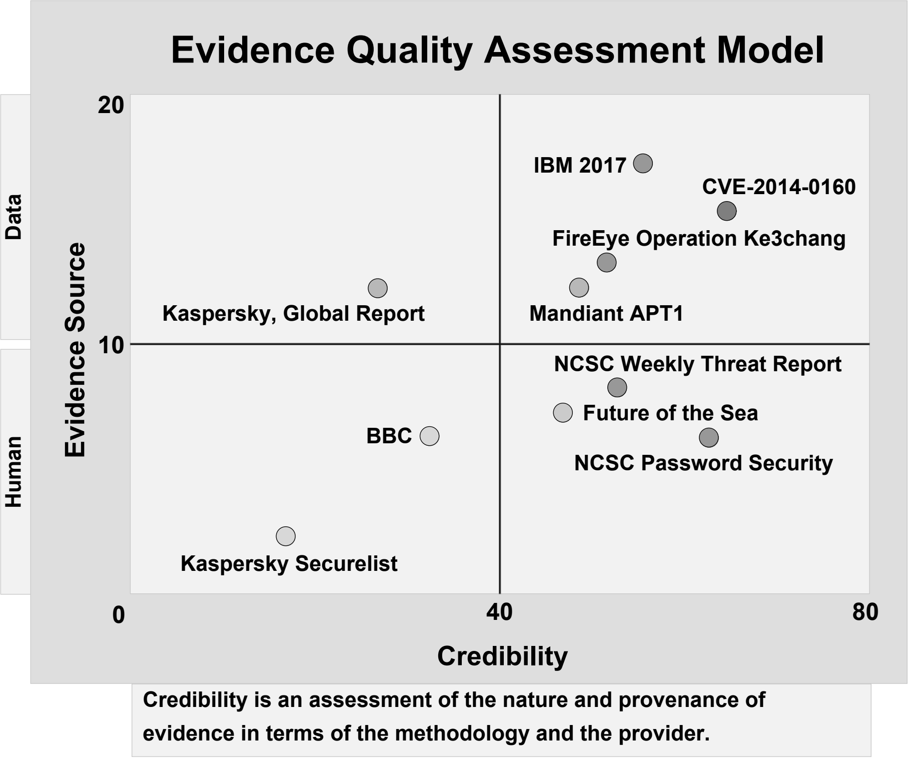


Figure 2. Placement of the ten evidence items on the EQAM map.

- **CVE-2014-0160 (E-2):** This evidence item is slightly obscure to a non-technical cyber security analyst, but the explanation of the threat and potential breadth of attacks are explained very well. A more accessible explanation would be more appropriate for non-technical consumers.

- **BBC 2017 (E-3)** This news article relies heavily on the opinions of political leaders and acknowledged experts. While the experts can be trusted to provide sound advice, individuals with strong political views may be biased.

- **Future of the Sea: Cyber Security (E-4):** This project report heavily relies on expert knowledge to provide a detailed scientific review of the topic. Such a review is subject to considerable scrutiny in terms of the scientific evidence selected and the corresponding inferences. However, the scientific evidence includes a very broad mix of research studies and technical artifacts and reports. These provide confidence in the methodology, but the evidence is drawn largely from human sources (of course, in some other cases, the evidence could be purely data-driven).

- **FireEye Operation Ke3chang (E-5):** This report was found to be much too technical for the assessors. While it is clear that ample quantitative evidence is provided, the methodology is somewhat vague at times. Perhaps a clearer link with the context is needed at the beginning, especially related to Syria. The inferences are problematic and could undermine a good data source when making policy decisions.

- **Mandiant APT1 (E-6):** The appendices to this report assist in understanding the methodology employed by Mandiant. Of note is the clarity with which the evidence is used to state the findings – myriad charts, photographs and empirical evidence. These are particularly useful in explaining the threat and the actor to a non-technical audience. Clear explanations of the artifacts in the report enable readers to assess the sources and credibility, but this makes for a long and detailed document, which negatively affects readability.

- **IBM 2017 (E-7):** This is the most comprehensive report of the ten evidence items analyzed in this research. It benefits from a clear description of the underlying methodology, including the systematic integration of qualitative and quantitative sources. However, this may be because IBM is in a position to comment on cyber security statistics – as outlined in the report, thousands of customers use IBM products, which enables the company to acquire statistics. The report is also accessible to non-specialists because it uses clear language and provides definitions where needed.

- **NCSC Password Security Guidance (E-8):** This guidance is clear in its intent: it provides readers with a visual representation of the potential threat and risks, and how to mitigate them. While there are only two instances of quantitative evidence, the qualitative advice comes from a position of authority on the topic; also, the risks are communicated very well.

- **Kaspersky Global Report (E-9):** This report is very poorly written, which distracts from the overall credibility of the report. Nevertheless, qualitative and quantitative evidence are used thoroughly, and the methodology is very clear. Kaspersky Lab suffers from a severe lack of trust as an evidence provider as far as the U.K. policymaking community is concerned. This is reflected in the low ranking of the evidence item in Figure 2.

- **Kaspersky Securelist (E-10):** This article makes sparse use of quantitative data when discussing how to survive attacks that access and leak passwords. No statistics related to prevention are presented, nor is the efficacy of prevention discussed. The data coverage is adequate to communicate the associated risk, but not enough to support the claims made in the article. For example, the guidance on using 23-character passwords is not substantiated. As before, Kaspersky Lab suffers from a severe lack of trust as an evidence provider.

5. Conclusions

It is imperative to assess the quality of the evidence base used for cyber security policymaking. The Evidence Quality Assessment Model presented in this chapter is a simple two-dimensional map that positions evidence samples relative to each other based on source and credibility. As such, it represents the first step towards a tool for assessing the fitness of evidence used in cyber security decision making. The use case involving representative items of evidence demonstrates how multiple attributes may be used to compare and contrast evidence items. The soft validation of the model also demonstrates its potential to resolve conflicts and achieve consensus when assessing evidence quality.

Future research will draw on senior members of the U.K. policymaking community who are well-versed in cyber security to help refine the evidence quality criteria and formally validate the model. The effort will leverage a repository containing a wide variety of evidence sources identified through stakeholder engagement.

Acknowledgement

This research was funded by the Engineering and Physical Science Research Council (EPSRC) as part of the project, Evaluating Cyber Security Evidence for Policy Advice: The Other Human Dimension (EP/P01156X/1), under the Human Dimensions of Cyber Security.

References

[1] D. Bestuzhev, How to survive attacks that result in password leaks? *Securelist*, Kaspersky Lab, Moscow, Russia, July 13, 2012.

[2] D. Chaikin, Network investigations of cyber attacks: The limits of digital evidence, *Crime, Law and Social Change*, vol. 46(4-5), pp. 239–256, 2006.

[3] G. Corera, If 2017 could be described as "cyber-geddon," what will 2018 bring? *BBC News*, December 30, 2017.

[4] P. Davies, Is evidence-based government possible? presented at the *Fourth Annual Campbell Collaboration Colloquium*, 2004.

[5] E. Gartzke, The myth of cyberwar: Bringing war in cyberspace back down to Earth, *International Security*, vol. 38(2), pp. 41–73, 2013.

[6] A. Glees, Evidence-based policy or policy-based evidence? Hutton and the government's use of secret intelligence, *Parliamentary Affairs*, vol. 58(1), pp. 138–155, 2005.

[7] C. Guitton and E. Korzak, The sophistication criterion for attribution: Identifying the perpetrators of cyber attacks, *The RUSI Journal*, vol. 158(4), pp. 62–68, 2013.

[8] O. Hathaway, R. Crootof, P. Levitz, H. Nix, A. Nowlan, W. Perdue and J. Spiegel, The law of cyber attack, *California Law Review*, vol. 100(4), pp. 817–886, 2012.

[9] IBM Security, IBM X-Force Threat Intelligence Index 2017, The Year of the Mega Breach, Somers, New York, 2017.

[10] E. Kaspersky, The man who found Stuxnet – Sergey Ulasen in the spotlight, *Security Matters*, Kaspersky Lab, Moscow, Russia (`www.eugene.kaspersky.com/2011/11/02/the-man-who-found-stuxnet-sergey-ulasen-in-the-spotlight`), November 2, 2011.

[11] Kaspersky Lab and Business Advantage, The State of Industrial Cybersecurity – Global Report, Woburn, Massachusetts and San Francisco, California, 2017.

[12] R. Lee and T. Rid, OMG Cyber! *The RUSI Journal*, vol. 159(5), pp. 4–12, 2014.

[13] G. Leicester, Viewpoint: The seven enemies of evidence-based policy, *Public Money and Management*, vol. 19(1), pp. 5–7, 1999.

[14] I. Levy, Active Cyber Defense – One Year On, National Cyber Security Centre, London, United Kingdom (`www.ncsc.gov.uk/information/active-cyber-defence-one-year`), 2018.

[15] Mandiant, APT1: Exposing One of China's Cyber Espionage Units, Alexandria, Virginia (`www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf`), 2013.

[16] M. Monaghan, Appreciating cannabis: The paradox of evidence in evidence-based policy making, *Evidence and Policy: A Journal of Research, Debate and Practice*, vol. 4(2), pp. 209–231, 2008.

[17] G. Mulgan, Government, knowledge and the business of policy-making: The potential and limits of evidence-based policy, *Evidence and Policy: A Journal of Research, Debate and Practice*, vol. 1(2), pp. 215–226, 2005.

[18] National Cyber Security Centre, Password Guidance: Simplifying Your Approach, Guidance, London, United Kingdom (`ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach`), 2016.

[19] National Cyber Security Centre, Weekly Threat Report, 22nd December 2017, Report, London, United Kingdom (`www.ncsc.gov.uk/report/weekly-threat-report-22nd-december-2017`), 2017.

[20] National Institute of Standards and Technology, CVE-2014-0160 Detail, National Vulnerability Database, Gaithersburg, Maryland (`nvd.nist.gov/vuln/detail/CVE-2014-0160`), 2014.

[21] M. Naughton, "Evidence-based policy" and the government of the criminal justice system – Only if the evidence fits! *Critical Social Policy*, vol. 25(1), pp. 47–69, 2005.

[22] S. Nutley, H. Davies and I. Walter, Evidence-Based Policy and Practice: Cross Sector Lessons from the UK, Working Paper 9, ESRC UK Centre for Evidence Based Policy and Practice, University of St. Andrews, St. Andrews, Scotland, United Kingdom, 2002.

[23] S. Nutley and J. Webb, Evidence and the policy process, in *What Works? Evidence-Based Policy and Practice in Public Services*, H. Davies, S. Nutley and P. Smith (Eds.), Policy Press, Bristol, United Kingdom, pp. 13–41, 2000.

[24] T. Rid and B. Buchanan, Attributing cyber attacks, *The Journal of Strategic Studies*, vol. 38(1-2), pp. 4–37, 2015.

[25] S. Shaikh, Future of the Sea: Cyber Security, Foresight, Government Office for Science, London, United Kingdom, 2017.

[26] L. Shaxson, Is your evidence robust enough? Questions for policy makers and practitioners, *Evidence and Policy: A Journal of Research, Debate and Practice*, vol. 1(1), pp. 101–112, 2005.

[27] W. Solesbury, Evidence Based Policy: Whence it Came and Where it's Going, Working Paper No. 1, ESRC UK Centre for Evidence Based Policy and Practice, Queen Mary, University of London, London, United Kingdom, 2001.

[28] Strategic Policy Making Team, Professional Policy Making for the Twenty-First Century, Version 2.0, Cabinet Office, London, United Kingdom, 1999.

[29] L. Tanczer, I. Brass, M. Carr, J. Blackstock and M. Elsden, The United Kingdom's emerging Internet of Things (IoT) policy landscape, to appear in *Rewired: Cybersecurity Governance*, R. Ellis and V. Mohan (Eds.), Wiley, Hoboken, New Jersey.

[30] A. Venables, S. Shaikh and J. Shuttleworth, The projection and measurement of cyberpower, *Security Journal*, vol. 30(3), pp. 1000–1011, 2017.

[31] N. Villeneuve, J. Bennett, N. Moran, T. Haq, M. Scott and K. Geers, Operation "Ke3chang:" Targeted Attacks against Ministries of Foreign Affairs, FireEye, Milpitas, California (`www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-ke3chang.pdf`), 2014.

[32] C. Weiss, The many meanings of research utilization, *Public Administration Review*, vol. 39(5), pp. 426–431, 1979.

[33] R. Whitt, Adaptive policy-making: Evolving and applying emergent solutions for U.S. communications policy, *Federal Communications Law Journal*, vol. 61(3), pp. 483–590, 2009.

[34] K. Young, D. Ashby, A. Boaz and L. Grayson, Social science and the evidence-based policy movement, *Social Policy and Society*, vol. 1(3), pp. 215–224, 2002.