Chapter 1

AN EVIDENCE QUALITY ASSESSMENT MODEL FOR CYBERSECURITY POLICYMAKING

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

Abstract One key factor underpinning a state's capacity to respond to policy challenges of cybersecurity is the quality of evidence supporting such decision making. As part of this process, policy advisers, essentially a diverse group including everyone from civil servants to elected policy makers, are asked to assess evidence from a mix of sources. Sometimes with little relevant expertise and often in time-critical scenarios, assessing threat, risk and proportionate response based on a mix of official briefings, academic sources, and industry threat reports is a challenge. The imperative of dealing with such issues in a timely fashion presents novel technical and political challenges for policy advisers. In this paper we present a model to help assess the quality of such evidence. The Evidence Quality Assessment Model (EQAM) is essentially a tool to help assess evidence fitness and credibility for use in such decision making. We illustrate the model with a sample of possible evidence sources to demonstrate how different attributes could be used for a comparison. The ultimate goal here is to help resolve potential conflicts and weigh findings and opinions systematically.

Keywords: Evidence, Quality, Model, Attributes, Cybersecurity, Policymaking

1. Introduction

Research into cybersecurity tends to focus on technical factors, vulnerabilities and solutions. Some work focuses on what is referred to as 'the human dimension' but these studies look predominantly at end user of technology. However, regulatory and policy frameworks also have significant implications for cybersecurity. Policy advisers, sometimes with little relevant expertise and often in time-critical scenarios, are asked

to assess evidence from a mix of sources including official threat intelligence, academic sources, and industry threat reports. Such a diverse evidence base is then used to make judgements on threat, risk, mitigation and consequences, and offer advice shaping the national regulatory landscape, foreign and domestic security policy, and a range of public and private sector initiatives. This paper is motivated by the need to better support decision making in the UK policy community when interpreting, evaluating and understanding evidence about cybersecurity.

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 ways that the policymaking community can be better supported to make sound policy decisions that will both foster continued innovation and also mitigate against the cybersecurity threats that we face now and also those that we will encounter going forward.

Consequently, our research is motivated by the following key research questions: what evidence do UK policymakers rely upon? What is the quality of that evidence? How effective are the judgements about threats, risks, mitigation and consequences based on that evidence? Understanding how UK policymakers select evidence, why they privilege one source over another, and how adept they are at recognising possible weaknesses or flaws in evidence is central to addressing these questions and is the main focus of our research.

This paper sets out to present a simple model to support quality assessment of the range of sources available in this context. Given the diversity of such sources, some of which may conflict and contradict, an evaluation of quality matters to help resolve potential divergences. The model, laid out as an evidence quality assessment model (EQAM), is a simple two-dimensional map where we use a set of attributes to position evidence samples relative to each other. The identification of attributes has been derived from a combination of sources from the literature and a series of 15 semi-structured interviews with policy advisers currently working within the UK cybersecurity policy community.

1.1 Rest of this paper

The rest of this paper is organised as follows. Section 2 discusses the links between cybersecurity evidence and policy challenges. It outlines the rise of Evidence Based Policy Making (EBPM) as a context for current thinking about evidence and policymaking. Section 3 presents the main contribution of this paper. Section 3.1 describes the interviews undertaken with the UK cybersecurity policy community. Section 3.2

and 3.3 detail out the range of quality attributes used by our model. Section 4 analyses a selection of evidence samples using the proposed model as an exercise in such quality assessment. Section 5 concludes the paper and outlines future steps.

2. Cybersecurity Evidence and Policy Challenges

Policymakers use a diverse evidence base to make judgements on threat, risk, mitigation and consequences, and offer advice shaping the national regulatory landscape, foreign and domestic security policy, and a range of public and private sector initiatives. Assessment of evidence is a particular problem for policymaking in this context for three reasons.

- First, some of the evidence is contradictory and/or potentially carries within it particular agendas or goals that may impede upon its rigour and reliability. The 'politicisation' of cybersecurity evidence is increasingly problematic as states sometimes privilege threat intelligence from sources located within their sovereign borders rather than based on the quality of the research they produce.

- Secondly, it has proven to be extremely difficult to conclusively attribute cyber-attacks and to quantify the cost of cyber insecurity. For policy advisers, the lack of clarity about the concrete financial implications of various cybersecurity vulnerabilities or incidents makes developing sound responses challenging. Without clarity about the role of specific communities of perpetrators, policy alternatives can be disconnected from the real threat, targeting individuals or groups that may not, in fact, be the key malicious actor. These challenges mean that existing evidence can often only support policy advisers' evaluation of cybersecurity risks, threats and consequences – and the resulting recommendations – to an extent.

- Finally, the landscape of cybersecurity is developing rapidly and spans many issue areas including national security, human rights, commercial concerns, and related infrastructure vulnerabilities. Consequently, policy advisers must work to balance a range of sometimes conflicting interests that compete for attention. Differing conceptions of what 'cybersecurity' means to different policy communities raises real impediments to a unified response. Network security, economic security, privacy and identity security, data security – all of these represent different conceptions and priorities which are commonly referred to as 'cybersecurity'.

The rise of 'evidence based policy making' under the Blair government prompted several studies into the way UK policy advisers engage with and interpret evidence. Early on in this transition Solesbury argued for careful critical analysis of what exactly constitutes 'evidence' [1], 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 UK policymakers rely upon in this context? What is the quality of that evidence? How effective are the judgements about threats, risks, mitigation and consequences based on that evidence? Understanding how UK policymakers select evidence, why they privilege one source over another, and how adept they are at recognising possible weaknesses or flaws in evidence is central to addressing these questions.

EBPM has been a core concept in contemporary UK policymaking since the 1990s. However, there is a lack of agreement among the policy community as to the level of clarity and definition of evidence, and the academic or scientific standard that should be applied to the evidence. This has resulted in the popularisation and politicisation of EBPM as more of a catch-phrase than a policy process that utilises rigorous methodology and systematic analysis [2][3][4][5][6]. In addition, modern day technological concerns are increasingly complex that they render an approach solely relying on EBPM simplistic, compared to more nuanced forms of policymaking where the evidence is contextualised within the policy process and objectives. Evidence based policy making involves a more critical approach based on scientific and replicable studies. It responds to the belief that past policy decisions may have relied upon the biased selection of evidence. It also seeks to address the influence of untested views of individuals or groups that represent vested interests, tradition, ideology, prejudice and/or speculation [7]. Evidence based policy making therefore attempts to reduce uncertainty and a lack of clarity about decision making by drawing upon rigorous information to turn policy goals into concrete and achievable actions [8].

In recent years, the policymaking landscape of some developed countries have led to innovative governance models in dealing with cybersecurity instead of relying on EBPM or other traditional forms of policymaking such as the rational model, implied model, enlightenment model, knowledge driven model, political model, tact model, and so on [3][9][10]. In the UK, newer systems take the form of adaptive (or agile) policymaking (APM). A concept that explicitly accounts for deep uncertainties prompted by the speed with which technologies evolve [11], APM is in direct contrast to the 'classical approach' to policymaking [3]

[12][13]. It recognises how 'conventional' policymaking mechanisms are ill-suited to manage the complexities associated with cybersecurity.

The adaptive paradigm also markedly departs from traditional form by incorporating a strategic vision and framework from which policies are derived to prepare against negative eventualities, while being sufficiently flexible and dynamic to meet changing circumstances through short-term actions [12]. In order to facilitate this process, the EQAM seeks to validate evidence quality in a timely fashion and inform policymakers on understanding the implications of utilising the evidence and make best judgements from the presented evidence.

3. Assessing Evidence Quality

In relation to the nature of evidence, the Strategic Policy Making Team at Cabinet Office [14] describes evidence as expert knowledge, published research, existing statistics, stakeholder consultations, previous policy evaluations, internet, costing of policy options, output from economic and statistical modelling. Davies [7] has structured different type of evidence into experimental controlled trials and studies, social surveys, econometric, expert advisory groups, public attitudes, ethical values such as belief and aspirations and research evidence from all relevant sources that has been systematically searched, critically appraised and rigorously analysed according to explicit and transparent criteria. However, Nutley et al. [15] note that in practice the public sector in the United Kingdom uses a more limited range of evidence, specifically research and statistics, policy evaluation, economic modelling and expert knowledge.

3.1 Interviews

Our interviews were carried out with a selection of 16 policy advisers and civil servants from November 2017 to February 2018. The sample was employed across government departments, including the Cabinet Office, Department for Digital, Culture, Media and Sport (DCMS), Home Office, Foreign and Commonwealth Office (FCO), HM Revenue and Customs (HMRC) and Department of Communities and Local Government (DCLG), and specialist agencies including London Mayor's Office for Policing and Crime, National Crime Agency (NCA) and the National Police Chiefs' Council (NPCC).

Through the interviews it was clear that a very wide variety of sources are used as potential evidence for policy analysis including research into trends, open source material, forums, news articles, daily bulletins, media, newsletter; threat intelligence reports, academic research, think

tanks; intelligence reports from domestic and sister agencies overseas, government restricted information; crime survey for England and Wales, action fraud and general policing data from National Crime Agency (NCA), cyber security breaches survey and ONS (Office of National Statistics) data sources and reports. Threat intelligence reports, surveys, case studies etc. are received from government restricted and unrestricted sources, along with many industry technology giants such as BAE Systems, IBM, Microsoft, Cisco and FireEye etc. Policy advisers also access classified information released by law enforcement agencies (LEAs) and the intelligence community. We do not review or address this information in our study, however our model accounts for such evidence to be used; while one assumes such evidence is reliable, it should be considered in the context of multiple (possibly transnational) agencies (each of which may be trusted to varying levels).

In relation to use of evidence and policymaking, it is noted that decision-making is sometimes based on the best available evidence even though it may not be perfect. If one does not offer an informed view then someone else less informed may take the decision; so time is critical for short term response. Long term problems are seen differently because of available time to put in place the right approaches and gather necessary evidence. Evaluating policy options and to identify what genuinely works well, there is a need to validate ideas and understanding how to improve it.

We propose two dimensions of quality. Section 3.2 describes the underlying basis for evidence, either as some form of data, or human sources. Each pose unique attributes relevant to quality. Section 3.3 considers the nature and provenance of evidence in terms of methodology of collection and the provider. Both are key to processing and credibility, which ultimately underpin confidence in the presentation of evidence.

3.2 Source of evidence

3.2.1 Data. Over the years, a range of technical and survey data has been used to present a range of cybersecurity factors, including everything from malware fragments for attribution [16] to emerging trends in the technical and social sphere [17]. Any such artefact of evidence is then subject a number of considerations.

- The scope of data collection is not always perfect. As such it may not always be complete to help with inference. This is particularly problematic when it comes to industry sources for threat intelligence and technological trends, which are typically designed to

magnify effects of commercial advantage to the organisation collection such data.

- There are questions of potential volatility given digital sources such as computers or networks [18]. As we increasingly rely on digital infrastructure for threat sensing, the transient nature of such sources cannot be ignored. In addition to this, digital forensics is subject to strict procedures of digital chain of custody and preservation, any violation of which could cast doubt over the integrity of data.

- Analysis of data, often abstract and agnostic in nature, is often highly open to interpretation, where, for example, traces of malware activity may be used to judge sophistication, which in turn is used as a critical criterion for attribution [19].

Of the subjects interviewed, bodies associated with a tradition of national data collection and statistical excellence such as the Office of National Statistics (ONS) in the UK, is pointed out as a reliable source for its methodology and objectivity giving confidence when cited in reports to ministers.

3.2.2 Human. Human sources, either as subjects of interest observed through some channel or knowledgeable experts offering opinions, are the other valuable source of evidence. With expert knowledge and commentary comes the burden of bias and beliefs, and context and connotation. Indeed this is a substantial challenge as cybersecurity, as a social construct, takes many different forms including a political discourse that invokes the idea of a cyber "Pearl Harbour" [20]. Objective analysis from human sources therefore is sensitive to the credibility of the entity collecting information alongside the transparency of their method of collection.

3.3 Credibility

3.3.1 Methodology. We focus our attention here on published forms of evidence to which some notion of methodology and organisation could be attributed to. We acknowledge that confidential sources of threat intelligence would follow official protocol; the judgement of their quality therefore is left to knowledge and limitation known within the relevant intelligence and policy communities.

One challenge with cybersecurity is the nature of heightened interest it attracts due to novel technological aspects. Such interest lends itself to both hype, and a lack of balanced technical and broader knowledge to help policy perspectives. Indeed the level of reporting of cybersecurity is

particularly criticised as such where *"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"* [21].

Appropriate methodology and analysis is key to argue substantial claims that result from the artefacts. This ranges from empirical analysis over data sets to appropriate qualitative and quantitative analysis over socio-technical input.

Moreover, the legal imperative around cyber attacks [22] means that a number of attributes are key if evidence is to be used for policy decisions that are to do with any aspect of legislation or regulation, or if a state is to respond under international norms and law. This makes transparency of how any artefact of evidence is collected, processed, stored and handled important.

3.3.2 Provider. There is an entire industry that has emerged over the last two decades dedicated to cyber threat intelligence, which is essentially an umbrella term to refer to collection and analysis of threat-related activity from a mixed of open sourced, social media and dark web sources. The industry is structured so as to be a mix of major IT and telecommunication companies, such as IBM and Cisco, to a set of specialised niche operators focused on advanced threats such as FireEye. The sector has become a major source of information supplier to government and corporate agencies making use of such information for better security enforcement to policymaking.

Geopolitical affiliations have the potential to cast a shadow over industry sources however even if technical capability is acknowledged. Kaspersky Labs is one example which has the highly credible reputation around its technical capability, including it's efforts in early detection of Stuxnet [23]. The Russian company's software has been warned against given the potential for its compromise from the state. Our interview findings also suggest threat intelligence from the company have been discredited given the reputation.

Industry is paralleled by government agencies, such as the National Cyber Security Centre (NCSC) in the UK, which have adopted the technical mission of advisory and guidance on cyber-related threats to a range of official and private stakeholders.

NCSC, as an example, provisions such advice in various formats for public consumption, from brief weekly threat reports with little trans-

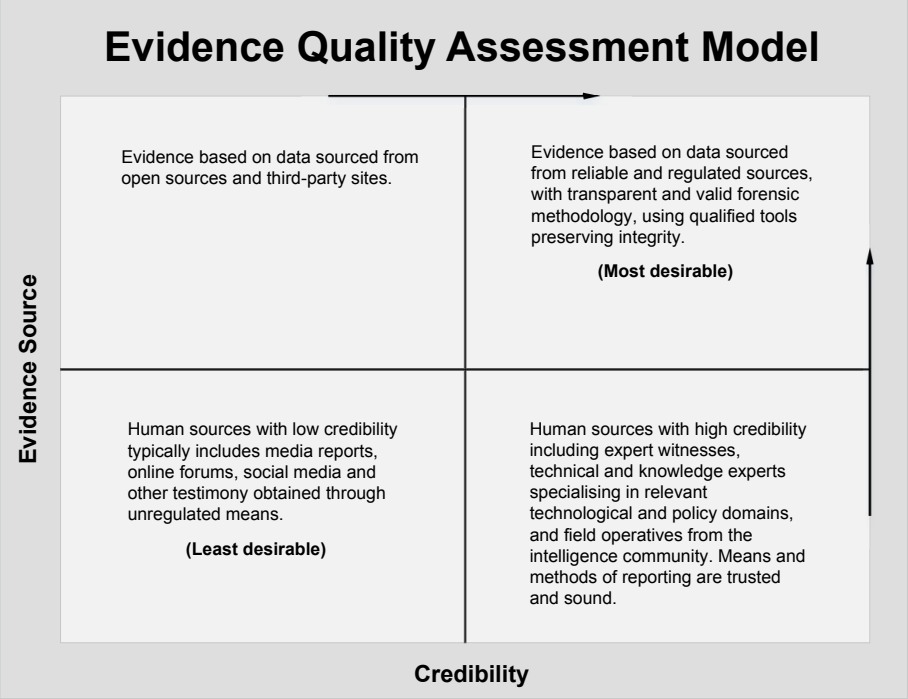

Figure 1. Our model is a simple representation of the quality of evidence using a two dimensional map where the vertical axis demonstrates the split between data and human, and the horizontal axis represents credibility assessed over methodology and provider. The four quadrants are simply to help with relative assessment of pieces of evidence.

parency or detail [24], to more data-driven detailed guidance with clarity on methodological approach and data provenance, such as the analysis on an assessment of the Active Cyber Defence policy [25]. Indeed, the quality challenges around a complex evidence base as such are acknowledged clearly by the authors who are clear that *"it's 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 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."* [25].

3.4 Evidence Quality Assessment Model (EQAM)

We present a model to reflect the diverse nature of the sources of evidence, and how we can characterise quality across this diverse space. Our model (EQAM) is based on a range of attributes from sections 3.2 and 3.3.

The proposed model as shown in Figure 1, is divided into four quadrants with evidence credibility on the horizontal axis and evidence sources on the vertical axis. We proposition the value of data in establishing quality over the value of human sources on the vertical axis. As a scale it helps to map sources that combine both types of input.

Over the horizontal axis we acknowledge that it has to serve as a continuum where credibility has to be judged on a case by case basis for each piece of evidence. The division over four quadrants is simply to help map evidence sources in relative position to each other.

4. EQAM Analysis

We present a simple illustration of the EQAM model to run through what would be a typical use to analyse a given selection of evidence.

4.1 Sample Selection

To illustrate the model we have performed an evidence assessment exercise internally within the team. A selection of ten pieces of evidence were chosen. The choice has been deliberately broad and diverse to help understand whether the model helps consensus across varying levels of evidence quality. Given our current focus on the UK policymaking community, the shortlist reflects items that have either been mentioned during our interviews or in the local policy discourse. Table 1 below shows details of the various providers we have used in our samples and the exact items of evidence.

4.2 Scoring Analysis

A subset of the authors, with a background a mix of technology and policy, assessed the evidence individually to score it on EQAM vertical and horizontal scales as per Figure 1. Table 2 shows the results of this exercise. Following on from this, the assessors translated the scores on to the map to discuss similarities and disparities in scores.

Similar scores were consolidated and disparate scores were discussed to negotiate to a common score. Figure 2 shows the consolidated EQAM map for the entire shortlist of evidence items.

Table 1. A selection of ten evidence items to help illustrate our model. These are deliberately chosen from a broad and diverse set to help understand whether the model helps consensus across varying levels of evidence quality. The shortlist reflects items that have been mentioned during our interviews or in the UK policy discourse.

Provider	**Description**
NCSC	NCSC provides advice and support for the public and private sector in how to avoid computer security threats in the UK. **NCSC Weekly Threat Report** issued on 22nd December 2017 contains evidence on distinct security issues [24]. **NCSC Password Security Guidance** contains advice for system owners responsible for determining password policy, advocating a dramatic simplification of the current approach at a system level [26].
CVE	Common Vulnerabilities and Exposures (CVE) is a list of information security vulnerabilities and exposures that aims to identify and catalogue vulnerabilities in software or firmware into a free "dictionary" for organisations to improve their security. **CVE-2014-0160** is a Heartbleed vulnerability found in OpenSSL software library [27].
BBC	The British Broadcasting Corporation (BBC) is a British public service broadcaster. **BBC 2017** highlights technology events from the year 2017 [28].
Foresight	Foresight projects, produced by the Government Office for Science, provide evidence to the policy community in the UK. **Foresight, Future of Sea** is a review of science to inform the UK's cybersecurity response for the maritime sector [29].
FireEye	FireEye is an enterprise cybersecurity company that provides products and services to protect against advanced cyber threats. **FireEye Operation ke3chang** investigates cyber espionage campaign, called "Ke3chang" [30]. Mandiant is a cybersecurity firm acquired by FireEye in 2013. Mandiant issued **Mandiant APT1** reports implicating China in cyber espionage [31].
IBM	IBM X-Force Research is a team of security professionals that monitor and analyse security issues from a variety of sources, providing threat intelligence content. **IBM 2017** evidence is an annual report presenting their findings from the year 2017 [32].
Kaspersky	Kaspersky Lab is a multinational cybersecurity and anti-virus provider headquartered in Moscow, Russia. **Kaspersky Global Report** is an annual report for 2017 covering security events from around the globe [33]. **SECURELIST** is an official blog from Kaspersky and the evidence is to survive attacks that result in password leaks [34].

Table 2. Ten evidence items from Table 1 are each ranked by the assessors. Scores below show consolidated and negotiated final scores for source and credibility criteria.

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

NCSC Weekly Threat Report (E-1) is broken up into five distinct threat bulletins. Each bulletin has distinct topics and its analysis varies e.g. the first bulletin includes facts from the survey to communicate the risk and support the claims while last bulletin only states the claims without providing any details of the analysis or findings. This makes the overall threat report slightly harder to assess as the same methodology was not applied across the report. Furthermore, in some instances, the sources of evidence were not stated such as the Daesh claim is presented with no validation of its sources. The data coverage for Android malware leaves questions unanswered such as what phone models were tested? Does it put all Android phones at risk? Does it have any impact on tablets running Android?

CVE-2014-0160 (E-2) is slightly obscure to a non-technical cyber-security analyst but the explanation of threat and potential breadth for attacks is very well explained. Perhaps a more accessible explanation would be more appropriate for a non-technical consumer.

BBC 2017 (E-3) news article relies heavily on the opinions of political leaders and those acknowledged as experts. Whilst such experts can be trusted on sound advice, others with known strong political views may not always be unbiased.

Foresight, Future of Sea (E-4) heavily relies on expert knowledge to conduct a detailed scientific review on the allocated topic. Such reviews are subject to detailed scrutiny in terms of the choice of scientific evidence selected and inferred on. Such scientific evidence however is a very broad mix of studies and technical artefacts and reporting. While as such it offers confidence in terms of methodology, it largely remains in the realm of human source of evidence for policymaking; unless in some particular cases such reviews are purely data-driven.

FireEye Operation ke3chang (E-5) was found to be far too technical for the assessor team in general. Whilst it is clear that quantitative evidence is ample, the methodology is somewhat vague at times. Perhaps a clearer link with the context is needed at the beginning as the

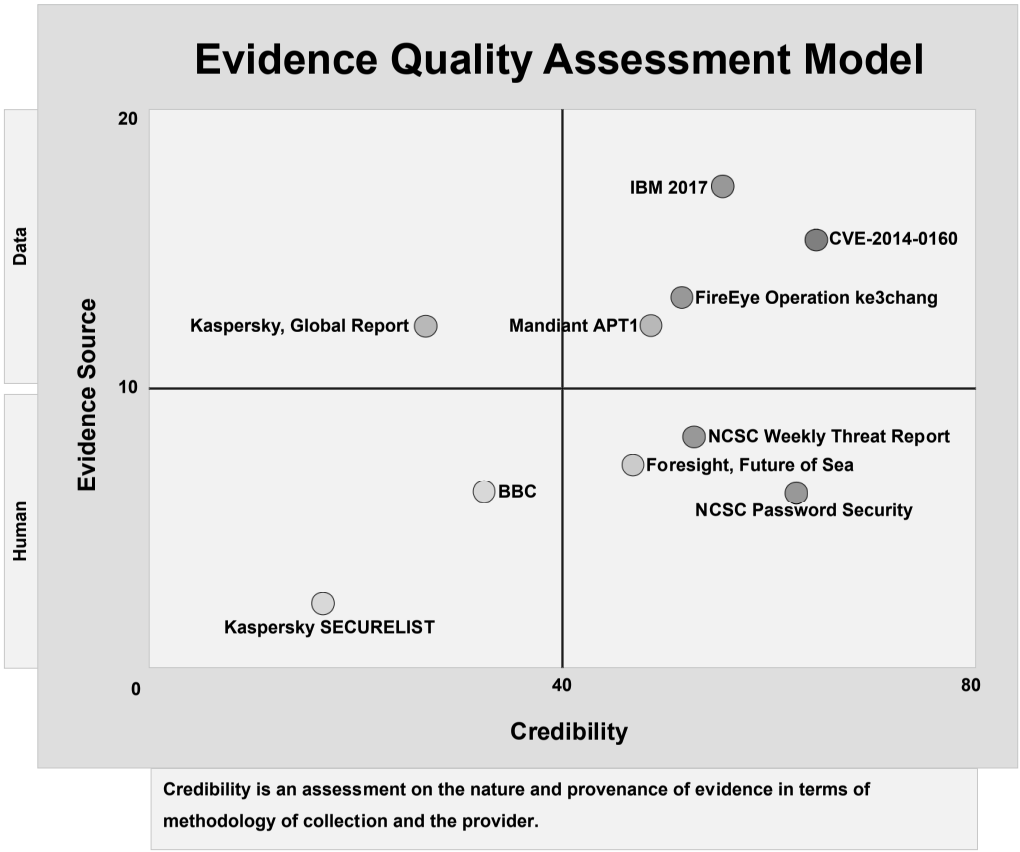

Figure 2. The final scores from Table 2 are shown in this consolidated EQAM map for the entire shortlist of evidence items. The model helps to map out relative positioning of evidence items across both scales to give a final of a quality assessment.

links to Syria are vague. Such inference is problematic and could also often undermine a good data source for policymaking purposes.

Mandiant APT1 (E-6) appendices particularly aid in understanding the methodology employed by Mandiant. Of note is the clarity with which they use the evidence to state their findings, using a myriad of charts, photos, and empirical evidence. This is particularly useful in explaining the threat and the actor to a non-technical audience. By clearly explaining each artefact of the report, the reader can better identify credibility, sources, and so forth; albeit this makes for a very long detailed document not helping readability.

IBM 2017 (E-7) is the most comprehensive report of the shortlist. It benefits from outlining clearly the underlying methodology, including a systematic integration of both quantitative and qualitative sources. However, this may be a result of the beneficial position that IBM is in to comment on cybersecurity statistics, as was outlined in the report given they have thousands of customers using their products and can acquire these statistics without needing to venture too far. The report also clearly outlines any technical elements for a non-specialist audience by using clear language and providing definitions where needed.

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

Kaspersky Global Report (E-9) has very poor quality writing which does distract from the overall credibility of the report. This said, quantitative evidence is used thoroughly, as well as qualitative. Methodology is very clear. Kaspersky as an evidence provider however suffers from a severe lack of trust in the UK policy context, which is reflected in the low ranking in Figure 2.

Kaspersky SECURELIST (E-10) makes sparse use of quantitative data, whilst arguing passwords are stolen; otherwise not providing any statistics on prevention and the efficacy of doing so. Data coverage is enough to communicate the associated risk but not enough to support claims in the guidance. The guidance on 23 character passwords is not substantiated. Lack of trust in the provider remains.

5. Conclusion and Future Work

We are driven to help assess the quality of the evidence base for cybersecurity policymaking. This paper presents a first step towards essentially a tool to help assess evidence fitness and credibility of evidence

for use in such decision making in the form of EQAM. We have illustrated the model with a sample of evidence sources to demonstrate how different attributes could be used for a comparison. The soft validation attempted as part of this paper has shown the model's potential to help resolve conflicts in such quality assessment. As next steps, we plan to conduct formal validation of the model through UK policymaking representatives with a wider variety of evidence sources identified through stakeholder engagement. Senior members of the policymaking community, well-versed with the problem domain, would be invited to validate the findings to help further refine the quality criteria used.

Acknowledgement

This research has been funded by 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 "Human Dimensions of Cyber Security".

References

[1] W. Solesbury, Evidence Based Policy: Whence it Came and Where it's Going, Working Paper No. 1 London: ERSC UK Centre for Evidence Based Policy and Practice, Queen Mary, University of London, UK (`www.kcl.ac.uk/sspp/departments/politicaleconomy/research/cep/pubs/papers/assets/wp1.pdf`), 2001.

[2] 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.

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

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

[5] 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.

[6] 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.

[7] P. Davies, *Is evidence-based government possible?*, 4th Campbell Collaboration Colloquium, Washington DC, 2004.

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

[9] S. Nutley, J. Webb, *Evidence and the policy process*, What works?: Evidence-based policy and practice in public services, 13–41, 2000.

[10] C. H. Weiss, *The Many Meanings of Research Utilization.*, Public Administration Review, vol. 39(5), pp. 426–431, 1979.

[11] G. Leicester, *Viewpoint: The Seven Enemies of Evidence-Based Policy*, Public Money & Management, vol. 19(1), pp. 5–7, 1999.

[12] L. M. Tanczer, I. Brass, M. Elsden, M. Carr, J. Blackstock, *The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape*, Rewired: Cybersecurity Governance, 2018.

[13] R. S. Whitt, *Adaptive Policymaking : Evolving and Applying Emergent Solutions for U.S. Communications Policy*, Federal Communications Law Journal, vol. 61(3), pp. 483–590, 2009.

[14] UK Cabinet Office, *Professional Policy Making For The Twenty First Century Report*, Strategic Policy Making Team (`dera.ioe.ac.uk/6320/1/profpolicymaking.pdf`), pp. 33, 1999

[15] S. Nutley, H. Davies and I. Walter, *Evidence based policy and practice: cross sector lessons from the UK*, Working Paper 9, Social Policy Research and Evaluation, Wellington, New Zealand, 2002.

[16] T. Rid, B. Buchanan, *Attributing Cyber Attacks*, Journal of Strategic Studies, vol. 38(1-2), pp. 4–37, 2014.

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

[18] 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.

[19] C. Guitton, E. Korzak, *The Sophistication Criterion for Attribution*, The RUSI Journal, vol. 158(4), pp. 62–68, 2013.

[20] E. Gartzke, *The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth*, International Security, vol. 38(2), pp. 41–73, 2013.

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

[22] O. A. Hathaway, C. Rebecca, P. Levitz, H. Nix, A Nowlan, W. Perdue and J. Spiegel, *The Law of Cyber-Attack*, Faculty Scholarship Series, pp. 38–52, 2012.

[23] Kaspersky Labs: The Man Who Found Stuxnet Sergey Ulasen in the Spotlight, (www.eugene.kaspersky.com/2011/11/02/the-man-who-found-stuxnet-sergey-ulasen-in-the-spotlight/).

[24] National Cyber Security Centre, Weekly Threat Report 22nd December 2017, UK (www.ncsc.gov.uk/report/weekly-threat-report-22nd-december-2017), 2017.

[25] I. Levy, Active Cyber Defence one year on, National Cyber Security Centre, UK (www.ncsc.gov.uk/information/active-cyber-defence-one-year), 2018.

[26] National Cyber Security Centre, Password Guidance: Simplifying Your Approach, UK (www.ncsc.gov.uk/content/files/protected_files/guidance_files/NCSC\%20Password\%20Security.pdf).

[27] The MITRE Corporation, CVE-2014-0160, USA (nvd.nist.gov/vuln/detail/CVE-2014-0160), 2014.

[28] C. Gordon, 30 December 2017, BBC News, UK (www.bbc.co.uk/news/technology-42338716?intlink_from_url=http://www.bbc.co.uk/news/topics/cz4pr2gd85qt/cyber-security&link_location=live-reporting-correspondent), 2017.

[29] Foresight, Future of Sea - Cyber Security, Government Office for Science, UK (www.gov.uk/government/uploads/system/uploads/attachment_data/file/671824/Future_of_the_Sea_-_Cyber_Security_Final.pdf), 2018.

[30] FireEye, Operation ke3chang, (www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-ke3chang.pdf).

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

[32] IBM Security, IBM X-Force Threat Intelligence Index 2017, 2017

[33] Kaspersky, The State of Industrial Cybersecurity - Global Report, 2017.

[34] SECURELIST, How to survive attacks that result in password leaks?, (securelist.com/how-to-survive-attacks-that-result-in-password-leaks-2/31304).