RISCS

Policy Briefing

Evaluating Cyber Security Evidence for Policy Advice (ECSEPA)

Cyber security policy making: a framework to assess evidence quality

Cyber security is considered a "Tier 1" risk to National Security. Civil servants across the UK Government are working on policy advice for cyber security – but how they acquire and use evidence to make recommendations is not well understood. This is important as the source and credibility of evidence affects the effectiveness and authority of the judgements made about threats, risks, mitigation and consequences. This briefing sets out findings from research as to how evidence is being incorporated into developing effective cyber security policies across UK Government.

Use of evidence in cyber security policy making

Evidence-informed policy making is intended to reduce uncertainty in decision making by drawing on rigorously collated information to turn policy goals into reasonable, concrete and achievable outcomes.

The quality of evidence used is crucial to the value of advice provided by civil servants to decision makers. The UK hopes to become "the safest place to live and do business online", as outlined in its National Cyber Security Strategy (NCSS),[1] and cyber security is increasingly pervasive across all policy areas. This means it will be ever more important for civil servants to assess, and be confident in the quality of the evidence they are using. The NCSS seeks to make cyber security part of business-as-usual, by embedding it into policy making, regulatory frameworks, business practices, research agendas and institutional structures throughout Government and society.

To achieve this, government departments must work together to share information, views and decision-making processes. The Cabinet Office Strategic Policy Making team described types of evidence with a list of sources reproduced here.[4] Previous research has found that in practice, the UK public sector uses a more limited range of evidence, specifically research and statistics, policy evaluation, economic modelling and expert knowledge. Published research is not always used.[5]

UCL

UKRI Engineering and Physical Sciences Research Council

Coventry University

The project included three primary activities to assess the effectiveness of cyber security decision-making.

Mapping exercise

We worked with the cyber security policy community to create a map of where cyber security policy development is taking place across government, and what evidence is used by policymakers.[2]

Evidence Quality Assessment Model (EQAM)

Our framework rates evidence samples relative to each other based on source and credibility, designed to help policy-makers assess the credibility of their evidence.[3]

Policy crisis games

We brought together the policy community working across government to take part in a simulated 'crisis game'. We observed participants' decision-making processes as they worked in teams to develop solutions to a fictional escalating cyber security crisis.

Cyber security making policy in the UK faces novel challenges:[6]

- The landscape is developing rapidly and cuts across most policy portfolios, whether it concerns maintaining the security of personal health records, defending the national power grid against cyber attacks or preventing online scams and fraud.
- Cyber security is a political issue and evidence can be contradictory, gathered selectively and/or carry specific agendas or goals which could reduce its rigour and reliability. For example, states may prioritise using evidence from within their sovereign borders.
- The stakeholder community involved in meeting the NCSS objectives is vast. They have competing priorities and vested interest in particular policy decisions. For example, preventing online scams and fraud involves financial institutions (such as banks and insurers), law enforcement agencies and cyber threat intelligence companies, which all have different priorities, liabilities and regulatory standards.

Our interviews with civil servants working in cyber security across UK government departments (including Digital, Culture, Media and Sport and the Home Office) and specialist agencies such as the London Mayor's Office for Policing and Crime and the National Crime Agency (NCA) found that they use a wide range of sources. However, the quality of this evidence is not always considered or understood, which has consequences for the quality of advice created based on it.

What makes high quality evidence?

Evidence quality has been discussed and measured in other disciplines. In medicine for example, the presence of randomised control trials is a key measure of evidence quality (the What Works Centre for Local Economic Growth uses the 'Maryland Scientific Method Scale').[7] The Department for International Development aims to help civil servants to understand different types of empirical research evidence, appreciate the principles of high quality evidence, consider how the context of research findings affects the way staff might use them and understand how to make sense of inconsistent or conflicting evidence.[8]

The 'Evidence Quality Assessment Model'

We have come up with a framework to assess evidence quality for cyber security, which we hope will help civil servants to provide the best policy advice based on the available evidence. It is designed for civil servants who provide short-term and long-term policy advice to measure the quality of evidence they use and to express the level of confidence they have in that evidence. It can also be used for reflection on the diversity of evidence sources they rely on. The framework positions evidence samples relative to each other based on two dimensions of evidence quality: source and credibility. There are different quality issues associated with data and human sources of evidence, but data sources may be preferred if they are more objective and tangible. The credibility dimension reflects the point that the method and provider of evidence both underpin the quality of the information.

Types of evidence

- Expert knowledge
- Published research
- Statistics
- Stakeholder consultations
- Previous policy evaluations
- Internet resources
- Outcome of consultations
- Costings of policy options
- Results from statistical and ecological modelling

Evidence used by UK civil servants in cybersecurity

- Research on trends from open source material (such as forums, news articles, and newsletters).
- Threat intelligence reports from academics and think tanks; surveys and case studies received from government sources (restricted and unrestricted), and from businesses.
- Intelligence reports from domestic and overseas sister agencies and restricted government information and the crime survey for England and Wales.
- Action fraud and general policing data from the NCA, cyber security breaches survey and Office of National Statistics (ONS) data sources and reports.
- Classified information from law enforcement agencies and the intelligence community.

The Evidence Quality Assessment Model

Less credible

More credible

Data Sources

Evidence based on open source data and third-party sites, such as blogs or industry sources

Example: *Kaspersky Lab Global Report.*

Kaspersky Lab is a multinational cyber security and anti-virus provider headquartered in Moscow, Russia. The report covers security events from around the globe.

Considerations

- **Industry sources** can be advantageous to the organisations that collect and publish the data: they can use selected evidence to corroborate their findings with the assumption that other sources may not publish their own evidence and that non-technical audiences may not understand how the data are collected. Can be biased for commercial advantage and are not peer reviewed.
- **'Digital evidence'** is subject to easier manipulation.[9] Unlike with analogue evidence such as ridge patterns for fingerprinting or polymarkers for DNA analysis, editing software exists for almost all types of digital information.
- **Data analysis of cyber-attacks** is open to interpretation. For example, evaluating the level of sophistication of a cyber-attack has controversially been used as an indicator of the identity of the attacker.[10]

Evidence based on reliable and regulated sources using rigorous methods

Example: *IBM 2017 report.*

IBM X-Force Research is a team that monitors and analyses security issues and provides threat intelligence content. This report covers IBM X-Force Research's findings.

Considerations

- **Transparency** around how evidence is collected, processed, stored and handled is essential if it is to be used for policy decisions related to legislation or regulation. It is particularly important for non-technical cyber security policymakers who may require further transparency to determine the credibility of the evidence.
- **Digital forensics** (the recovery and investigation of material found in digital devices) is subject to strict chain of custody and preservation procedures.

Human Sources

Testimony obtained through unregulated means, such as media reports and online forums

Example: *BBC article on the main technology events of 2017.*

Considerations

- **Bias** may affect the credibility of testimony. The news article in the example relies heavily on the opinions of political leaders and acknowledged experts. While experts can be trusted to provide sound advice, individuals with strong political, commercial, or ideological views may shape the argument or perspective.

Expert witnesses, subject matter experts, and the intelligence community

Example: *NCSC Password security guidance.*

Considerations

- **The cyber threat intelligence industry** is a major source of information for government agencies and corporations for policy making and decisions about security.
- **Geopolitical affiliations** can cast a shadow on providers.
- **Conflicting evidence** among different providers can occur, for example password advice from leaders in the market differs from that of NCSC.

The next iteration of the framework

The use of a framework to measure evidence quality, combined with the rich stakeholder discussions that this would enable could improve policy makers understanding of, and decision making in field of cyber security. This framework is the first step: we plan to develop this idea further with input from the UK policy-making community experienced in cyber security to help refine the evidence quality criteria and validate the framework.

References

1. National Cyber Security Strategy 2016 – 2021. Available at: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021
2. ECSEPA Map. Available at: https://www.riscs.org.uk/ecsepa-map/
3. Hussain A, Shaikh S, Chung A, Dawda S and Carr M. (2018). 'An Evidence Quality Assessment Model for Cyber security Policymaking'. Critical Infrastructure Protection XII, IFIP.
4. British Cabinet Office (1999). Professional Policymaking in the Twenty-First century. Available at: https://dera.ioe.ac.uk/6320/1/profpolicymaking.pdf
5. Nutley, S., Davies, H., and Walter, I., Evidence based policy and practice: cross sector lessons from the UK (2002). Working Paper 9, Social Policy Research and Evaluation, New Zealand.
6. Chung A, Dawda S, Hussain A, Shaikh S and Carr M. (2018). 'Cyber security: Policy', Encyclopedia of Security and Emergency Management, LR Shapiro and MH Maras eds. Springer Nature.
7. https://whatworksgrowth.org/resources/the-scientific-maryland-scale
8. DFID, 2014. How to Note: Assessing the strength of evidence. Available at: https://www.gov.uk/government/publications/how-to-note-assessing-the-strength-of-evidence
9. Chaikin, D. (2006). Network investigations of cyber-attacks: the limits of digital evidence. Crime Law Soc Change. 46, 239–256.
10. Guitton,C and Korzak, E. (2013). The Sophistication Criterion for Attribution. The RUSI Journal, vol. 158(4), pp. 62-68.

Questions for the policy community

- How could a tool for assessing evidence quality change the way you use evidence?
- How could the next iteration of this framework be improved?
- What are the outstanding barriers and challenges to developing good cybersecurity policy? How can the research community support this?
- The ECSEPA Mapping project identifies where cyber security policy development is taking place across Government, and what evidence is used by policymakers. The map is designed to be used and updated by policymakers. Is this visualisation useful to you? How could it be improved?

We'd love to hear your thoughts on these questions. Please get in touch using the contact details below.

Our research

This briefing was produced in partnership with UCL STEaPP's Policy Impact Unit as part of the work carried out by the ECSEPA project team at UCL and Coventry University. This research has been funded by the Engineering and Physical Science Research Council (EPSRC) as part of the ECSEPA project. This is part of the Research Institute for Sociotechnical Cybersecurity (RISCS).

Contact us

Professor Madeline Carr specialises in Global Politics and Cyber Security at UCL and is Director of RISCS. m.carr@ucl.ac.uk

Professor Siraj Shaikh specialises in Systems Security at the Institute of Future Transport and Cities (IFTC) at Coventry University. s.shaikh@coventry.ac.uk

Further details at: riscs.org.uk