Title of Edited Volume (by Springer Nature)
Encyclopedia of Security and Emergency Management

Title of Entry
Cybersecurity: Policy

Authors
Alex Chung[a], Sneha Dawda[a], Atif Hussain[b], Siraj Ahmed Shaikh[b], and Madeline Carr[a]

[a] University College London, Department of Science, Technology, Engineering and Public Policy (UCL STEaPP), UK

[b] Systems Security Group, Institute for Future Transport and Cities (FTC), Coventry University, UK

Keywords
Adaptive policymaking (APM); agile governance; attribution; Budapest Convention; critical infrastructure; cyber; cyberattack; cybercrime; cybersecurity; European Union (EU); evidence-based policymaking; geopolitics; incident response; international relations; Mutual Legal Assistance Treaty (MLAT); UK National Cyber Security Centre (NCSC); national cyber security strategy (NCSS); US National Cyber Strategy (NCS); US National Security Strategy (NSS); polycentric governance; public policy; public-private partnership; socio-technical; Tallinn Manual; United Kingdom (UK); United Nations (UN); United States (US); wicked problem

Definition
Cybersecurity policy refers to a course of action adopted by a state, an organisation, or a set of actors with the aim of ensuring cybersecurity and/or digital competitiveness as well as defining the individual and collective responsibilities in pursuit of that goal.

1. Introduction: What is cybersecurity policy and why does it matter?

Cybersecurity policy refers to a course of action adopted by a state, an organisation, or a set of actors with the aim of ensuring cybersecurity and/or digital competitiveness as well as defining the individual and collective responsibilities in pursuit of that goal. Broadly conceived, this area of public policy concerns complex, multifaceted, and dynamic security and business innovation related to information and communications technology (ICT). Cybersecurity policymaking includes legal, regulatory, technical, organisational, behavioural, international, and other capacity-building areas. Policy dimensions attached to these include information security, network security, cybercrime, and cyber conflict.

Cybersecurity policy can be formulated and implemented domestically at different levels of government or at the international level. The policy scope can range from short to longer term objectives and has implications for a wide range of societal actors. Effective cybersecurity policy can have consequences for public safety, national security, citizens' well-being, and economic prosperity. As became clear in the wake of the alleged interference in the 2016 US elections, it can even have implications for the health and sustainability of democratic processes.

Some governments produce clearly articulated cybersecurity policy goals, objectives and strategies which are publicly accessible. Others struggle to develop these due to a lack of capacity or the weight of more immediately pressing problems. Still other governments develop cybersecurity policies but choose not to share them with their own citizens or other governments. Therefore, the study of cybersecurity policy often focuses on those countries that do publish their plans – countries like (but certainly not limited to) the United States (US), Japan, Australia, Norway, France, Germany, Canada and the United Kingdom (UK; see ccdcoe.org for a list of published national cybersecurity strategy documents).

In these countries, cybersecurity policy tends to coalesce around the promotion of the national interest with security, defence and the resilience of the private sector most often prioritised in government agendas. Specific issues tend to include the protection of critical national infrastructure and critical information infrastructure, continued industrial and business growth and innovation, the prevention of fraud, cybercrime, and child sexual exploitation, as well as defending against state-sponsored misinformation propaganda and other state-sponsored malicious cyber activities.

In a world where the pace of digitalisation is accelerating, a comprehensive and well thought out cybersecurity policy that is based on defined legal and regulatory frameworks is understood to be a cornerstone of prosperous and proper-functioning societies. However, identifying what exactly constitutes 'good' cybersecurity policy is difficult for a number of reasons. This is not a mature area of policymaking and there are some factors which make it particularly challenging. These include coordination problems of any diverse policy issue across portfolios, the close interdependence of government with the private sector for pursuing cybersecurity, and the challenges of jurisdiction which sometimes defy cyber incidents.

2. What factors complicate cybersecurity policy?

2.1 Coordination problems

Cybersecurity in one form or another can now be found in many (if not most) policy portfolios. In a health portfolio, cybersecurity might relate to the security of personal health records or to the safety of Internet-enabled equipment and personal health devices. Cybersecurity has implications for international trade as governments vie for lucrative contracts for their own indigenous firms while at the same time, a business development portfolio may be working to attract large multinational corporations by offering tax relief in order to stimulate local jobs. Cybersecurity is central to law enforcement, defence and intelligence communities as it is seen as an important element of national security. It is not surprising that with the breadth of issues, interests, objectives and goals amongst these and the many other policy portfolios engaging with cybersecurity, coordination can be extremely difficult.

Policy areas that pertain to national emergency and incident response cover a vast array of public and private cybersecurity spheres. Some of the relevant sectors include telecommunications, electrical and nuclear power, transportation, energy pipelines, weapons systems, refineries, financial networks, and healthcare systems. The effectiveness of policy is dependent upon the joint implementation between the government and the private sector. National technical authorities such as the National Cyber Security Centre (NCSC) in the UK and the National Cybersecurity and Communications Integration Center (NCCIC) in the US have been established to monitor, collect, and share information with their partner organisations. These coordination efforts have proven particularly challenging during emergency situations due to the complexities of multi-stakeholder involvement. To communicate information in a timely and accurate way, it is important to know where clear lines of communications lie between the private sector and government agencies responsible for intelligence, defence and security, law enforcement, and commerce and finance.

Clearly, a high level of coordination is required to increase the overall effectiveness of national and local policies. At the same time, too much centralised control raises concerns about a lack of flexibility and independent thinking – both qualities understood to be important in cybersecurity. Consequently, there is a persistent tension in many countries about how to balance coordination and autonomy in portfolio level decision making. This leads to questions about the role that public-private partnerships (PPP) play in national cybersecurity policy implementation. This concept has been growing in prominence in recent years and now features as the centrepiece in the strategies of many developed countries.

2.2 Public-Private Partnership

Critical national infrastructures of developed countries have experienced a progressive shift toward a market-led management approach since the turn of the century. In the context of an overall shift to small government, the control over ICT estates as well as related knowledge, skills, and expertise have increasingly been relegated to the private sector rather than being retained by national governments. As a result, there has been a high level of

outsourcing of responsibility, ownership, and capability to private entities. Governments regard this as a means of relieving financial burdens and remaining up to date in a rapidly evolving technological landscape. As a consequence, the PPP has now become a key mechanism for the mitigation of cybersecurity threats. Many states now rely on PPPs as part of their policy implementation plan (Carr 2016a).

PPPs are important to national cybersecurity policy for a number of reasons. In the US, for example, over 85 percent of national critical infrastructure is in private hands. While there is excellence in the military and intelligence communities, commercially available ICT solutions mostly come from the private sector. Governments have an incentive to stimulate and support private sector growth and then draw on its expertise when required. While there are many reasons why the PPP is an important element of national cybersecurity policy planning and implementation, these arrangements are not without problems (*ibid*.).

Several types of specific PPP arrangements have been identified and classified. These include the dichotomy of horizontal, consensual decision-making partnerships which displays the true nature of PPP, versus hierarchical relationships with unipolar power asymmetry. Other PPP arrangements include *partnership as management reform* through the relinquishing of state authority and capability, to *partnership as power sharing* which entails information sharing rather than responsibility sharing. Clearly articulated (and contracted) PPPs can be very effective but NCSSs often refer to this in an amorphous way; 'we are bound together in cyberspace' (Osborne 2015) type of arrangement which fail to specify lines of responsibility and liability for national security issues. As a core responsibility of the government, national security should not be outsourced in principle, especially when the private sector has no interest in accepting it in practice.

In order for PPP to work to maximum advantage, competing agendas between the government and multinationals who own and who wield significant influence over national security concerns need to be spelled out in the PPPs' design. The distinction between the government's duty to protect national security as a necessary public 'good', and profit as the ultimate end for companies, need to be explicit for the middle ground to emerge. To aid this, a shift is required from the normative and 'new management' language, which obfuscates a dysfunctional partnership, to a clear language that acknowledges PPP's weaknesses.

2.3 Jurisdiction and speed

Another set of coordination challenges that complicates cybersecurity policy concerns law enforcement investigatory capacity in response to cyber incidents. Unlike crime in the physical world, cybercrime's unique extraterritorial qualities transcend geographical boundaries. The invisible and non-local nature of cyberattacks create obstacles for the authorities to quickly and effectively investigate and apprehend perpetrators.

The sheer volume and scale of potential mass targets for malicious cyber actors render conventional policing strategies ineffective. Police remit in this area includes the investigation of cyber-enabled crimes such as online fraud and child sexual exploitation

imagery, but also cyber-dependent crimes that incapacitate network systems such as Distributed Denial-of-Service (DDoS) and ransomware. From personal networked devices to commercially sensitive information, and from state secrets to critical national infrastructure systems, the expansive coverage of vulnerable digital assets overstretches policing resources. The blurred boundaries between national cybersecurity concerns and civilian targets, due to ever-increasing digital connectedness, also blurs responsibilities.

In general, three characteristics of the virtual domain make cyber investigations extremely demanding: actor's anonymity, speed of activity, and multi-stage action across jurisdictions (BIICL 2014). Rid and Buchanan (2015: 24-25) provide four categories in their explanation of how the speed and phasing of cyberattacks complicate an investigation. A *direct and immediate* attack can reduce uptime of servers, availability of files, or integrity of data and hardware; a *direct and delayed* attack can manipulate critical network systems to stress their components and result in physical breakdown. An *indirect and immediate* attack for cause reputation damage or loss of confidentiality through file leakage; an *indirect and delayed* attack can involve intellectual property theft which may be used to illegally gain a firm's competitiveness.

In addition, cyber attribution is an extremely difficult, if not impossible, exercise. Computer network systems allow criminals to not only conceal their tracks, but also to mislead by falsifying the origin of the attack. Digital forensic evidence in this respect resists any attempts by the investigator to accurately identifying malicious actors. Bartholomew and Gurrero-Saade (2016) contend that there will never be a solid enough attribution claim to convince everyone, but only multiple indicators that may lead to an educated determination as to the trustworthiness of a claim. Without the ability to attribute attacks with sufficient certainty, authorities cannot take appropriate remedial and deterrent actions (or retaliatory measures) in suspected state-sponsored attacks (*ibid*.).

Across jurisdictions both within and beyond a nation's borders, network infrastructure and digital connectivity can differ greatly. This creates varying levels of needs and interests for security due to an uneven distribution in the level of risks and attacks, which in turn leads to different levels of preparedness, amount of resources allocated to law enforcement, and governance methods. Although Western countries have been working on fostering the right environment and processes and to enable cooperation and collaboration on cybersecurity policy, which is discussed below, these issues remain inherently difficult to resolve.

3. How is cybersecurity policy implemented?

While the governance approach for dealing with policy issues is distinct for every government, an increase in the use of a polycentric mode of governance has been observed worldwide. Such governance structure involves multiple centres and levels of decision-making within the policy community (Ostrom 1961). The following discussion exemplifies the profound coordination challenges illustrated above by selectively focusing on three examples of cybersecurity policies in the US, the UK, and internationally. It looks at some key factors

affecting cybersecurity policy within the context of incident response and management. These include determining where responsibility lies and how it is delineated within PPPs, which key actors take the lead in creating and implementing cybersecurity strategies, and what are the institutional remits of the relevant agencies as well as how their work intersects to promote effective collaboration.

3.1 In the United States

In 2003, the US was the first state to develop a National Cyber Security Strategy (NCSS) titled the National Strategy to Secure Cyberspace and has invested heavily in policy innovation and coordination. The US National Cyber Strategy 2018 (NCS) and National Security Strategy 2017 (NSS) contain prescriptive provisions salient to cybersecurity. At the core of the policy ecosystem sits the Department of Homeland Security (DHS). The DHS conducts high-impact cybercrime investigations alongside other federal agencies. It also attempts to work with federal civilian departments and agencies to promote the adoption of common policies and to share cyber response best practices and tools. This includes the US Computer Emergency Readiness Team (US-CERT) which sits within the NCCIC, a round-the-clock awareness and incident response management centre for integrated cross-government communication.

In addition, the DHS also promotes cybersecurity on several fronts through engagements with its partnering organisations. These include public awareness campaigns, cyber insurance market, research and development, jobs and training, and skills and education. Apart from the DHS, a number of US government bodies are also charged with mandates relevant to cybersecurity policymaking. For instance, the Departments of Commerce (USDC), Defense (DOD), Treasury (USDT), Energy (DoE), Health and Human Services (HHS), and Justice (DoJ) all work in conjunction with the DHS to safeguard different areas of the US cybersecurity ecosystem by jointly executing policy plans.

Notwithstanding the roles government actors take on to shape and direct cybersecurity policy at the federal level, implementation is far from a straightforward process. While the DHS's coordination role is meant to be supported by a wide range of public and private partners who are operators and co-owners of most of the government critical national infrastructures, policy delivery and outcome are often contested. Although PPP cooperation and collaboration are vital to the implementation of cybersecurity policies (which includes the NCS 2018 and NSS 2017) at the federal level, non-federal influences are seriously impeding the effective coordination of critical infrastructure policies that aim to protect national security and facilitate cyber risk communications.

The decentralised US federalism system gives rise to simultaneous decision-making and guarding of assets and rights by different institutional actors. For instance, the US Congress, state and local governments, and private companies may choose not to share information with the federal government or adhere to federal level cyber risk guidance if doing so conflicts with their economic interests (Mussington 2018). These obstacles present significant challenges to the country's ability to carry out and maintain coherent cybersecurity policies and operational response structures that ought to align with executive orders and legislation.

3.2 In the United Kingdom

As one of the most digitally ambitious countries in Europe, the UK's stated goal is to be 'the safest place to live and do business online' (NCSS 2016-2021). Since 2011, cybersecurity has been nominated as a 'Tier 1' threat to UK national security (NCSS 2011-2016). The UK has the largest digital economy of the G20, which accounts for 12.4% of the country's GDP, more than double that of the US at 5.4% (techUK 2015). Substantial resources and efforts are allocated by the UK government to ensure that the country's capabilities are at the forefront of this field.

The policy terrain of UK cybersecurity is centrally administered and funded through the Cabinet Office. Similar to the US and other developed countries, the UK relies on the National Cyber Security Strategy 2016-2021 (NCSS) as the overarching policy document that sets out the strategic direction of, and approach to, ensuring cybersecurity. For the years 2016 to 2021, the Cabinet Office oversees a budget of £1.9 billion to support the delivery of the NCSS, though they provide minimal top-down operational directives to ministerial departments involved this area.

Remaining behind the scenes, the GCHQ is the primary player leading the effort to ensure the cybersecurity of national information network and communications systems. As the technical authority within the government and the public-facing organisation under the GCHQ, the NCSC supports, implements, and coordinates top-level policies. The Incident Response Management team within the NCSC is responsible for assessing and responding to emerging incidents. If the crisis is deemed to pose an immediate threat or a rapidly escalating threat to national security, a Cabinet Office Briefing Room (COBR) meeting is convened where actors such as the National Crime Agency (NCA) may take part in a law enforcement and investigatory capacity. During emergency situations, the central government (HMG) takes action with the assistance of the NCSC to provide points of effective coordination that quickly work to deploy defensive (and offensive) measures against adversaries.

Compared to the US, the implementation and delivery of the NCSS in the UK is functionally more distributed amongst HMG ministerial departments, the lead charge for which resides with the Home Office and the DCMS. The former is tasked with operational and strategic foci on cybercrime and cyber threats, while the latter is mandated with cyber growth, innovation and security. Akin to the US, the challenge of delivering national policy objectives means public and private institutions are required necessarily to work collaboratively across government and industry sectors.

3.3 Internationally

Instead of a single policy framework, the international policy landscape consists of multilateral efforts to jointly agree on rules and harmonise national laws. These comprise of clusters of binding and non-binding instruments reached by states sometimes with the help of international organisations. Binding instruments include conventions, directives, and regulations. Non-binding instruments include declarations, recommendations, and guidelines. Intergovernmental and supranational entities also work together to facilitate the

implementation process in the name of global order and security, but mixed results have been obtained so far.

Launched in 2001 and came into force that year, the Convention on Cybercrime of the Council of Europe (Budapest Convention) is the first binding international treaty on crimes committed via the Internet and computer networks. Developed in consultation with the US, Canada, Japan, and South Africa, it is open to signature by any state and at the time of writing had been ratified by 61 states. To ratify the treaty, states are required to outlaw five actions and authorise their domestic law enforcement agencies to investigate them: unauthorised access, unauthorised interception, data interference, system interference, and misuse of devices (Carr 2016b).

Predominantly an instrument for aligning states' criminal codes to facilitate faster and more effective cooperation between law enforcement bodies, its uptake has been slow and limited mainly due to technical capability, legal factors, and a lack of political will. The addition of new protocols since 2006 has also led to widespread disagreement among states over the value of their inclusion due to inconsistencies with the public policies and security priorities of states (*ibid*.). The main legal mechanism upon which treaties such as the Budapest Convention can rely for cross-jurisdictional law enforcement is the Mutual Legal Assistance Treaties. Signatories of MLATs have an obligation to reciprocate in all types of criminal investigations and prosecutions Including those with a cyber dimension. Together, MLATs and the Budapest Convention significantly minimises barriers to international cooperation in the enforcement of rules and regulations stemming from cybersecurity policies.

While intergovernmental cybersecurity framework developments can be traced back to the 1990s, there has been a strong push for new policies since the early 2010s due to the novel forms of insecurity and threats that are arising in cyberspace. The 'Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations' contains a comprehensive analysis of how existing international law applies to cyberspace, based on the first 2013 edition. Authored by 19 international law experts led by the North Atlantic Treaty Organization (NATO), the Manual's intended audience is global policymakers. According to the authors, its main contributions are that it captures the disagreements between countries on issues of cyber conflict and highlights the need to move away from an offensive posture in cyberspace to a defensive one. It acknowledges, for the first time, the lack of understanding of legal grey areas in cyberspace which creates contentions in the interpretation and application of international law.

At the UN level, states have worked together through the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) to negotiate some common understanding and agreement about responsible state behaviour in cyberspace. In 2012, all participating states (including Russia, China and the US) agreed that international law does apply in cyberspace. Exactly *how* it applies has been the source of ongoing debate. In 2016, the UN GGE produced a consensus report on 11 proposed 'norms' of responsible state behaviour but the subsequent meeting in 2017 was dominated by deeply divergent views. The controversies surrounding the politicisation of the International Telecommunications Union's (ITU) is another example, where states' different political and belief systems in the amount of

control exerted over the Internet have led to the creation of internal factions which have marred its governance effort. Moreover, geopolitical rivalry is reflected in the trend towards regionalism, which impedes wider international cooperation. Different views on cyberspace governance and cyber norms are manifested in the policy stance of regional security groupings.

Notably, the Shanghai Cooperation Organisation (SCO) established in 2001 - comprised of China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan - emphasised the importance of cyber sovereignty and the creation of a new cybercrime treaty in addition to the Budapest Convention. European Union (EU) led frameworks such as the Network and Information Security Directive (NISD) and the General Data Protection Regulation (GDPR) tend to focus on self-regulation and compliance measures aimed at managing unavoidable cyber risks and incidents. Despite high-level dialogues between the US, the UK, the EU Member States, Russia, and China on these issues, common ground has not been reached

4. Future thinking

In the 21st century, the pervasiveness of software and communications systems allows cyber insecurity to permeate through every facet of citizens' lives (Tanczer *et al*. 2018). This presents tremendous challenges to policymaking due to the myriad of ways in which it poses potential and real harm to public interest and safety. Policymakers need to make informed decisions based on accurate assessment of the risks, vulnerabilities, and threats, and harm emanating from cybersecurity ecosystem. Yet, they are struggling to achieve this in a cohesive, joined up way because the cyber domain is a highly dispersed issue with complex interdependencies across portfolios, and it is in constant flux.

This combination of two factors produce what are referred to as 'wicked problems' and they render policymaking especially challenging. These kinds of 'wicked problems' need to be tackled through cross-governmental departments and intergovernmental agencies that have coexisting roles and overlapping functions. The coordination of collaborative efforts to counter these policy issues from multiple centres and levels of a policy network simultaneously, as illustrated in the examples of the US and the UK, are key organisational features of a polycentric governance structure.

Further, adaptive policymaking (APM) and agile governance have also been on the rise globally, which are now reflected in various national cybersecurity strategies. Agile governance entails adaptive, inclusive and sustainable policymaking that accounts for not only input from the government but emphasises collaborative efforts by multi-stakeholders. APM explicitly accounts for deep uncertainties prompted by the speed with which technologies evolve, in contrast to the 'classical approach' such as evidence-based policymaking (Haasnoot *et al.* 2013). APM incorporates a strategic vision and framework from which policies are derived to prepare for negative eventualities, while being sufficiently flexible and dynamic to meet changing circumstances through short-term actions (Tanczer *et al.* 2018).

While the UK and the US have not clarified the methodological approach behind the design, formulation, and implementation of their NCSSs, agile governance and APM models have come to be recognised as an important tool by the government, industry, and academia of the respective countries (Parcell and Holden 2013). Research on cutting edge tools and decision-making frameworks that focus on robust evidence uptake and rigorous evidence evaluation is currently being developed to assist the policy process (Hussain *et al*. 2018).

In the UK, collaborative projects in partnership with government bodies such as the Cabinet Office, the Department of Work and Pensions, the Department of Health, the Ministry of Justice, and the Ministry of Defence are under way to investigate new ways of developing and incorporating agile principles in their policy work. In the US, organisations such as NIST in the Department of Commerce, American Institute of Aeronautics and Astronautics (AIAA), and Federal Government infrastructure suppliers are employing an adaptive approach to policy implementation at the Federal level.

These approaches are further encouraged for countries working toward common international digital development goals such as the United Nations Sustainable Development Goals. A gradual shift toward an open and inclusive model of multi-stakeholderism is advocated to account for the varied stages of digitalisation of each country (Clemente 2013). Despite ongoing development in these areas, much work remains ahead. Commentators have been calling for further research into innovative APM and agile governance models on both national and international fronts, and to implement their application more widely and effectively in the realm of digital policymaking.

5. Conclusion

The complexities of cybersecurity policy are shown through the coordination challenges, PPP obscurities, and jurisdictional issues facing the national and international policy communities. The cyber domain is throwing up uncertainties around issues of national security and national interest, which make it difficult for policy actors to make informed decisions on domestic matters or reach consensus on international concerns. These problems become particularly pronounced when decisive action is needed to respond to cybersecurity incidents and emergencies.

Although governments and private entities have devoted significant resources to better understand and address the inadequacies, clearer terms of reference are required for effective collaboration in the policy process, and wider international cooperation is needed to resolve geopolitical roadblocks and impasse. To this end, polycentric governance appears to be the preferred approach in the US and the UK based on how policy design and implementation are organised between the respective governments and the relevant private sector stakeholders. In recent years, research into different modes of agile governance and APM have made headway in addressing the limitations inherent to this socio-technical area of policymaking. Continued refinement of research in the areas of decision-making processes and evidence evaluation frameworks holds promise for a future that is better equipped to deal with the challenges posed by cybersecurity policymaking.

Cross-References

Criminals: Cybercriminals; Critical infrastructure: Information technology sector; Critical infrastructure: Critical manufacturing sector; Critical infrastructure: Transportation systems sector; Cybersecurity: Cybercrime and prevention strategies; Data; Data Protection; Emergency management: Major incidents that contributed to changes in EM; Industrial control systems; Insider threat; Intrusion detection system; Internet (include deep web); Internet of Things; Public-private partnerships: Cybersecurity; Risk analysis: National and international standards (that lead to difference in policy/procedures)

References

Ansley, R. (2017). 'Tallinn Manual 2.0: Defending Cyberspace.' *Atlantic Council Blog*, February 15.

Bartholomew, B. and Gurrero-Saade, J. A. (2016). 'Wave your false flags! Deception tactics muddying attribution in targeted attacks.' Virus Bulletin Conference, October.

BIICL (2014). 'State Responsibility for Cyber Operations: International Law Issues: Event Report.' British Institute of International and Comparative Law. October 9.

Carr, M. (2016a). 'Public-private partnerships in national cyber security strategies.' *International Affairs*, 92/1: 43-62.

—— (2016b). 'Crossed Wires: International Cooperation on Cyber Security.' *Journal of International Affairs*, 2015/2016, No. 2; 1-2.

Clemente, D. (2013). 'Adaptive Internet Governance: Persuading the Swing States.' *Internet Governance Papers*, No. 5, October.

Haasnoot, M. Kwakkel, J. H., Walker, W. E, and ter Maat, J. (2013). 'Dynamic adaptive policy pathways: A method for crafting robust decisions for a deeply uncertain world.' *Global Environmental Change*, 23/2: 485-498.

Hussain, A., Shaikh, S. A., Chung, A., Dawda, S., Carr, M. (2018). 'An Evidence Quality Assessment Model for Cybersecurity Policymaking.' *Technical Proceedings: International Federation for Information Processing (IFIP) Conference*, 13 March, Arlington, Virginia, USA.

Mussington, D. (2018). 'Governing Cyber Security in Canada, Australia and the United States.' Christian Leuprect and Stephanie MacLellan eds*., Centre for International Governance Innovation*: Special Report, April.

Osborne, G. (2015). 'Chancellor's Speech to GCHQ on Cyber Security.' *UK HM Treasury online*.

Ostrom, V., Tiebour, C. M., and Warren, R. (1961). 'The Organization of Government in Metropolitan Areas: A Theoretical Inquiry.' *American Political Science Review*. 55/4: 831-842.

Parcell, J. and Holden, S. H. (2013). 'Agile policy development for digital government: An exploratory case study.' Conference: Proceedings of the 14th Annual International Conference on Digital Government Research.

Rid, T. and Buchanan, T. (2015). 'Attributing Cyber Attacks.' *Journal of Strategic Studies*, 38, 1/2: 4-37.

Tanczer, L., Brass, I., Elsden, M., Carr, M., and Blackstock, J. (forthcoming). 'The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape.' In: R., Ellis & V., Mohan, *Rewired: Cybersecurity Governance.* Wiley.

techUK (2015). 'UK's digital economy is world leading in terms of proportion of GDP.' 1 May.

Further Reading

Her Majesty's Government (2016). National Cyber Security Strategy 2016-2021 (cited as NCSS).

NCS (2018). 'National Cyber Strategy of the United States of America.' The White House, Washing D. C., September.

NSS (2017). 'National Security Strategy of the United States of America.' The White House, Washington D. C., December.

Page 2: [1] Deleted	**Madeline Carr**	**7/30/18 7:38:00 PM**

Page 2: [2] Deleted	**Madeline Carr**	**7/30/18 7:37:00 PM**

Page 2: [3] Deleted	**Madeline Carr**	**7/30/18 7:47:00 PM**

Page 3: [4] Deleted	**Madeline Carr**	**7/30/18 7:48:00 PM**

Page 3: [5] Formatted	**Chung, Alex**	**8/15/18 1:43:00 AM**

Justified, Space Before: 0 pt, After: 0 pt, Pattern: Clear (Background 1)

Page 3: [6] Formatted	**Chung, Alex**	**8/15/18 1:43:00 AM**

Justified, Space Before: 0 pt, After: 0 pt, Pattern: Clear (Background 1)

Page 3: [7] Formatted	**Chung, Alex**	**8/15/18 1:43:00 AM**

Justified, Space Before: 0 pt, After: 0 pt, Pattern: Clear (Background 1)

Page 3: [8] Formatted	**Chung, Alex**	**8/15/18 1:43:00 AM**

Justified, Space Before: 0 pt, After: 0 pt, Pattern: Clear (Background 1)

Page 3: [9] Formatted	**Chung, Alex**	**8/15/18 1:43:00 AM**

Justified, Space Before: 0 pt, After: 0 pt, Pattern: Clear (Background 1)

Page 3: [10] Deleted	**Madeline Carr**	**8/13/18 5:48:00 AM**

Page 3: [11] Formatted	**Chung, Alex**	**8/15/18 1:43:00 AM**

Justified, Space Before: 0 pt, After: 0 pt, Pattern: Clear (Background 1)

Page 3: [12] Formatted	**Chung, Alex**	**8/15/18 1:43:00 AM**

Justified, Space Before: 0 pt, After: 0 pt, Pattern: Clear (Background 1)