STRATEGIES OF CYBER CRISIS MANAGEMENT: LESSONS FROM THE APPROACHES OF ESTONIA AND THE UNITED KINGDOM*

Jamie Collier

Department of Politics and International Relations and Centre for Doctoral Training in Cyber Security, University of Oxford

ABSTRACT

This paper compares the cyber crisis management strategies of Estonia and the United Kingdom—two leading nations in the field of cyber security. The two countries' strategies differ significantly. The most important variables influencing these differences are history, size (both demographic and material resources), political philosophy, digital dependence, and the nature of the threats and adversaries each country faces in the cyber domain. Given the importance of these factors in determining Estonia's and the United Kingdom's cyber crisis strategies, it is difficult to draw from these two cases any generalisable recommendations that apply to other states; rather, the main significance of this study is another: it draws attention to the important role that political, historical, and cultural variables play in the definition of a nation's cyber crisis strategy—and, consequently, the need to fit specific policy approaches within the bounds set by these factors. The paper seeks to demonstrate that while cyberattacks may be highly technical in nature, organisational responses to them have crucial political and social determinants that may supersede the significance of technical factors.

1. INTRODUCTION

Cyberspace has played a decisive role in improving and expanding the operations of critical infrastructures in modern society. This is particularly apparent in economically developed and technologically advanced nations, where information technologies are constantly integrated into a growing range of core services across a number of public and private industries. For example, "smart" power grids utilising cloud computing can deliver significant cost savings and maximise energy

---

This paper has been accepted for publication in Mariarosaria Taddeo and Ludovica Glorioso, eds., *Ethics and Policies for Cyber Operations* (Cham: Springer, forthcoming).

This publication is funded by the European Social Fund and the Estonian Government.

efficiency,[1] while electronic health records can optimise hospital services and give impetus to innovative medical research.[2]

Yet alongside these benefits are considerable risks. The increasing reliance of modern society on complex digital systems—particularly in the operations of critical national infrastructures—increases the risks of disruptive or destructive attack in two significant ways. First, digital systems contain a theoretically limitless number of software (and other) vulnerabilities; hence, the number of possible attack sequences available to an aggressor is also limitless. Second, the wide diffusion of cyberspace empowers new threat actors. Compared to conventional security and defence domains, the cyber domain has low barriers to entry; not just states but also non-traditional and militarily weak actors can use cyberspace to cause alarming harm.[3] Cybersecurity, in short, has become a crucial component of national and economic security strategy; it is a central and necessary feature of a modern nation's crisis management strategy.

This paper focuses on cyber crisis management, defined as the cyber security aspects of a crisis situation, which in turn is defined as a situation where a state's citizens are subject to significant danger. Specifically, the paper examines three domains of crisis management: the organisation of the governmental institutions responsible for crisis situations; the role of non-governmental stakeholders; and international cooperative efforts, with a special emphasis on the countries' use of traditional international security mechanisms (such as NATO) to manage crises. The study seeks to identify similarities and differences in the cyber crisis management strategies of two nations—Estonia and the United Kingdom—and to explore the main explanatory variables that shape and constrain each. This comparative study aims to contribute to cyber security scholarship and practice by identifying broad lessons and insights that might be applicable in other national contexts—even if specific national factors are not replicable. The study aims to create new knowledge by demonstrating the analytical usefulness of a comparative approach to the formulation of cyber security policy, while uncovering the broad political, cultural, and historical factors that influence the national strategies of Estonia and

[1] Cedric Clastres, "Smart Grids: Another Step Towards Competition, Energy Security and Climate Change Objectives," *Energy Policy*, Vol. 39, No. 9 (2011), pp. 5399–5408.

[2] David Kotz, Sasikanth Avancha, and Amit Baxi, "A Privacy Framework for Mobile Health and Home-Care Systems," *Proceedings of the First ACM Workshop on Security and Privacy in Medical and Home-care Systems, SPIMACS* (New York, 2009), pp. 1–12; Ulrike Rauer, "Patient Trust in Internet-Based Health Records: An Analysis Across Operator Types and Levels of Patient Involvement in Germany," *Policy and Internet*, Vol. 4, No. 2 (March 2012), pp. 1–42; and Peter Groves, Basel Kayyali, David Knott, and Steve Van Kuiken, "The 'Big Data' Revolution in Healthcare," McKinsey Global Institute (New York: 11 January 2013).

[3] Joseph S. Nye, Jr., *The Future of Power*, chap. 5 (New York: PublicAffairs, 2011), pp. 113–151.

the United Kingdom. Why Estonia and the United Kingdom? These two states were chosen for comparison because they are often regarded as international leaders in cyber security (for example, both are members of the so-called Digital 5—or D5—network of leading digital governments).[4] It is important to note that there are significant similarities and differences between the two states: both are developed European economies as well as European Union and NATO member states and both feature a high degree of dependence on digital systems; yet at the same time they are notably different in size, threat landscape, and other factors.

The paper argues that Estonia and the United Kingdom differ, at times significantly, in their strategic responses to cyber crisis situations because of a combination of political, historical, and cultural variables. These variables include history, size (referring to both demographic and material resources), political philosophy, digital dependence, and the threats and adversaries that each nation faces in the cyber domain. Both case studies demonstrate the importance of non-technical variables in the development of national cyber strategy. Indeed, if Estonia and the United Kingdom differ in their cyber crisis strategies, then other more disparate nations are likely to differ even more significantly—thus highlighting again the importance of a customised and context-specific approach to the study of national strategies. Thus although states caught in a cyber crisis situation are likely to face many similar policy and technical challenges, responses to these challenges at the *strategic* level may vary enormously. Therein lies an important insight for scholarship and practice: because non-technical variables can significantly affect a state's cyber crisis management strategy, these variables require serious attention in assessing the adequateness of national responses. Of course, some features of national strategy—such as the need to define clear and coherent defensive priorities—can be applied broadly. But given the importance of non-technical and country-specific factors in shaping a cyber crisis management strategies, such generalisable lessons are likely to be limited. A strategy or policy that is successful in Estonia might not work effectively in the United Kingdom and vice-versa.

In sum, this paper will seek to demonstrate that given the importance of political, historical, and cultural variables, there can be no "one-size-fits-all" approach to cyber crisis management. Rather, the best crisis response strategy is that which most effectively integrates the strengths and limitations of each nation's respective political and cultural circumstances.

[4] Oscar Williams-Grut, "London Launch for 'D5' Alliance of Digital Nations," *The Independent*, 8 December 2014), http://www.independent.co.uk/news/business/news/london-launch-for-d5-alliance-of-digital-nations-9909374.html.

The remainder of the paper is organised into five sections. Section two describes the scope of analysis and research methods. Section three examines the cyber crisis management strategy of Estonia. Section four reviews the strategy of the United Kingdom. Section five identifies the main explanatory variables that shape and constrain the two nations' strategies. Section six discusses the broader policy implications of the study.

2. SCOPE AND METHODS

A few words on the paper's scope and key terms are in order. In considering responses to cyber threats, the paper focuses on indirect cyber attacks—specifically, attacks on critical national infrastructure. Many security analysts have claimed that cyber attacks are only indirect in nature; that is, they do not produce direct effects on a target.[5] Others, however, have argued that direct forms of cyber attack are possible (for example, digital manipulation of electronic pacemakers) and should not be dismissed. In addition, as new types of devices increasingly become connected to cyberspace—and indeed the Internet—the possibility of direct damage by cyber attack will only increase. But it is true that the vast majority of cyber attacks are indirect; they damage digital systems that run vital services or critical functions that reside outside cyberspace, with the intent of indirectly harming, or at least disrupting, these services. By focusing on indirect attacks, the paper does not mean to downplay the danger of direct attacks. But because academic and policy understandings of such direct attacks is still rudimentary, policy reaction to them has been limited; consequently, it is difficult to meaningfully examine the national strategies dealing with direct attacks—but for this same reason, the development of such strategies should be a key government priority. Third, the paper focuses on strategic—not technical—responses to a crisis. Although cyberattacks are highly technical in nature, the response required in a crisis often has clear political and other non-technical components, for example the question of how government departments work with civilian stakeholders and foreign allies. Non-technical factors may, in fact, be the more important in determining the nature, scope, and success of a crisis response.

Methodologically, the paper draws on a diverse range of sources that includes the secondary academic literature and primary data such as publicly available governmental and business reports. Fieldwork was conducted in both Estonia and the United Kingdom and involved a number of semi-structured field interviews with leading practitioners in the field of cyber security and defence, including

[5] Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst, 2013).

officials at the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE). The analysis also draws from a number of conversations with individuals working within critical national infrastructure as well as academics and researchers specialising in relevant fields. The paper encountered a few notable methodological obstacles. For one thing, the paper is unable to identify interview participants owing to the sensitivity of the topic and in order to elicit open and frank responses from them. For another, Estonia's and the United Kingdom's cyber crisis strategies are largely hypothetical. That is, the paucity of cyber crises available for empirical investigation renders—inevitably—any analysis of this subject speculative to a degree. It cannot be guaranteed that during an actual crisis situation a state will execute its intended crisis strategy; indeed, as discussed below, crisis situations have previously led to extemporaneous responses. Moreover, important procedural details of Estonian and UK strategies remain unclear or unknown because neither country has outlined its cyber crisis management strategy in one single document or because the data remains at least partly classified. This may be because governments are naturally reluctant to disclose the full details of their crisis management, since disclosure may reveal weaknesses that an opportunistic assailant could exploit. Nevertheless, the qualitative data and sources of this study have made possible a rich empirical analysis on which future studies may build.

3. ESTONIA

Estonia's digital infrastructure has grown significantly since the nation regained independence in 1991. It has progressed from a country where only half the population had telephone lines to one that is a recognised global leader in information technology and e-government. In 1992, Estonia decided to orient its developmental strategy to the development of superior digital systems.[6] Starting with a blank slate, it was able to leapfrog previous types of infrastructure—for example, Estonia was able to develop a sophisticated digital land registry system soon after it's re-independence.[7] The state also launched an innovative digital ID-card system. Technology has therefore played a large role in Estonia's attempt to overcome the legacy of Soviet occupation. With the limited resources and budget constraints faced by a small state, technological solutions and innovative approaches in its public sector services have been vital to the country's development. This trend has continued through 2015, with Estonia becoming one of the most connected nations in the world: Estonians pay taxes and vote online; their health records are stored digitally; and concerned parents can access their children's

[6] Mart Laar, *Estonia: Little Country That Could* (London: Centre for Research into Post-Communist Economies, 2002).
[7] "How Did Estonia Become a Leader in Technology?" *The Economist*, 30 July 2013.

exam results, attendance, and homework assignments via the Internet.[8] Notably, and uniquely, Estonia created the "X-road," a decentralised data exchange environment that connects the government's various e-services databases.[9]

Such high levels of digital dependence make Estonia potentially vulnerable to cyber threats. This vulnerability was demonstrated in 2007. Following the removal of a Soviet war memorial from Tallinn's city centre, a number of Estonian e-services and websites were overloaded by a distributed denial of service (DDOS) attack, believed to be of Russian origin.[10] The attack degraded the availability and functioning of services crucial to Estonia's information society, including government websites and online banking systems.[11] The attack, however, inflicted no long-term property damage, loss of life, or substantial financial loss.[12] Nevertheless, the attack illustrated the potential for cyber attacks to threaten Estonia's national and economic security. Since this incident, there has been notable change in Estonia's strategic posture: cyber security is now regarded as a higher political priority. A number of initiatives have since been launched, including the publication of an official Estonian cyber security strategy, the creation of a formalised cyber reserve force, and the establishment of the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn.[13] What follows is a review of Estonia's current cyber crisis management strategy.

A. Domestic Institutional Organisation

In Estonia, there is a clear centralised leadership structure for response to cyber crisis situations. The responsibility for overall cyber security strategy and policy coordination lies with the Ministry of Economic Affairs and Communication; this responsibility was relinquished by the Ministry of Defence in 2011.[14] Within the Ministry of Economic Affairs and Communication, the Estonian Information Systems Authority (*Riigi Infosüsteemi Amet*—RIA) serves as the central cyber security

[8] Tim Mansel, "How Estonia Became E-Stonia," *BBC News*, 16 May 2013, http://www.bbc.co.uk/news/business-22317297.

[9] Finland recently signed an agreement with Estonia to adopt the latest version of the X-Road. See Aivar Pau, "Finland and Estonia on Joint X-Road Starting November," *Postimees*, 17 July 2015, http://news.postimees.ee/3264073/finland-and-estonia-on-joint-x-road-starting-november.

[10] Mark Landler and John Markoff, "Digital Fears Emerge After Data Siege in Estonia," *The New York Times*, 29 May 2007, http://www.nytimes.com/2007/05/29/technology/29estonia.html?hp; and Aviram Jenik, "Cyberwar in Estonia and the Middle East," *Network Security*, Vol. 2009, No. 4 (April 2009), pp. 4–6.

[11] Andreas Schmidt, "The Estonian Cyberattacks," in Jason Healey, ed., *The Fierce Domain: Conflicts in Cyberspace, 1986-2012* (Washington, D.C.: Atlantic Council, 2013).

[12] Sharon L. Cardash, Frank J. Cilluffo, and Rain Ottis, "Estonia's Cyber Defence League: A Model for the United States?" *Studies in Conflict and Terrorism*, Vol. 36, No. 9 (September 2013), pp. 777–787.

[13] Camile Marie Jackson, "Estonian Cyber Policy After the 2007 Attacks: Drivers of Change and Factors for Success," *New Voices in Public Policy*, Vol. 7 (Spring 2013), pp. 1–15.

[14] Anna-Maria Osula, "National Cyber Security Organisations: Estonia" (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 24 March 2015).

competence and coordination centre, supervising the application of cyber security measures for systems that provide vital services to the Estonian state. The Ministry of Interior also acts as a coordinating body during crisis situations.

The 2009 Emergency Act requires providers of vital services to immediately notify the relevant national government department about attacks, and they must also provide information to other bodies upon request. Governmental powers can be further escalated through the 1996 State of Emergency Act if a threat emerges that threatens the constitutional order of Estonia.[15] This Act significantly centralises the crisis management response by concentrating rights, duties, and liabilities in the Prime Minister, who becomes the chief authority during a state of emergency. In serious crisis situations, the Prime Minister is able to restrict certain rights and freedoms in the interest of national security and public order. Therefore, while certain cyber crisis management responsibilities lie with individual government departments, if a situation becomes serious and significantly threatens Estonia, there is a very clear process for the escalation of powers to central bodies such as the Estonian Information Systems Authority and the Prime Minister.

The Estonian Computer Emergency Response Team (CERT-EE) provides a support function in cyber crisis situations. It is responsible for handling security incidents within Estonian networks, providing warning of potential security incidents, and analysing the spread of malware and incidents that have taken place in Estonian computer networks.[16] With the high level of e-government services, it is clear that CERT-EE has an important role in safeguarding Estonian infrastructure. Moreover, the government utilises its embassies abroad to maintain secure cloud systems—"data embassies"—that can sustain e-services in the event of a cyber attack on Estonia's domestic infrastructure. Estonia's "digital continuity" project aims to ensure that in the event of any cyber crisis situation, crucial e-government services will continue to function.[17] Thus the idea is that if Estonian-based systems are under attack or services become compromised in the event of a national emergency, data embassies abroad can assist in the recovery process.

[15] Ibid.

[16] Ibid.

[17] "How to Back Up a Country," *The Economist*, 7 March 2015; "Implementation of the Virtual Data Embassy Solution," *Estonian Ministry of Economic Affairs and Communications and Microsoft Corporation* (3 February 2015); and Taavi Kotka and Innar Liiv, "Concept of Estonian Government Cloud and Data Embassies," in Andrea Kő and Enrico Francesconi, eds., *Electronic Government and the Information Systems Perspective: Proceedings of the International Conference EGOVIS 2015* in Valencia, Spain, 1-3 September 2015.

B. Stakeholder Mobilisation

The implications of cyber crisis situations reach beyond governmental institutions. For any response to be successful, governments must interact with other stakeholders. The Estonian government has adopted a comprehensive and inclusive approach with non-governmental actors playing important roles in cyber crisis situations. In Estonia there has been a particular emphasis on mobilising civil society. The current Estonian Deputy Director for National Security and Defence Coordination, Kristjan Prikk, has claimed that while other states have sought to overcome cyber threats by allocating vast budgets to the problem, Estonia has instead strived to create a nation of citizens alert to online threats.[18] In Estonia, there is an emphasis on educating citizens about risks and promoting an understanding of cyber security.[19] According to Prikk, Estonia has adopted "not just a whole of government approach, but a whole of nation approach."[20]

This "whole of nation" approach was clearly evident during the 2007 DDOS attack, during which a number of stakeholders collaborated in order to defend against and mitigate the effects of the suspected Russian action. Three days after the initial attacks occurred, a number of Estonian experts came together, including Internet service providers, banks, police, governmental envoys, mobile telecommunication firms, and envoys from the government's Security and Information Boards.[21] This informal alliance was able to organise assistance in a number of ways, for example, by supplying relevant appliances and hardware, filtering malevolent traffic, and providing information on the threat's scope, nature, and technical detail.[22] By creating opportunities for collaboration, this informal alliance enabled different actors to work closely together in order to help overcome the unfolding crisis. Principles of loose governance and trust-based information-sharing facilitated this *ad hoc* collaborative framework.

Yet despite the effectiveness of the Estonian technical community's response, the attack also marked the end of that community's autonomy from state interference and regulation.[23] In the aftermath of the attack, the Estonian government woke up to the danger of cyber crisis situations and increasingly

---

[18] Jackson, "Estonian Cyber Policy After the 2007 Attacks".

[19] Marthie Grobler, Joey Jansen van Vuuren, and Jannie Zaaiman, "Changing the Face of Cyber Warfare with International Cyber Defense Collaboration," in Matthew Warren, *Case Studies in Information Warfare and Security: For Researchers, Teachers, and Students* (Reading: Academic Conferences and Publishing International Limited, 2013), pp. 38–54.

[20] Jackson, "Estonian Cyber Policy After the 2007 Attacks."

[21] Schmidt, "The Estonian Cyberattacks."

[22] Ibid.

[23] Ibid.

attempted to formalise the "whole of nation" strategy by creating institutions and regulations to oversee and guide what was previously an informal and largely self-driven approach. This formalising process accelerated after 2007, as demonstrated by one of the most significant legacies of the attacks—the establishment of the Defence League Cyber Unit (popularly referred to as the Cyber Defence League, or CDL) within the Estonian Defence League, the reserve military force.[24] By creating the CDL the Estonian government has been able to harness the desire of civil society to contribute to defensive efforts in the midst of a crisis situation.[25] The CDL consists of volunteers who possess some form of expertise in cyber security and, indeed, many of its volunteers were part of the informal 2007 alliance. In crisis situations, members of the CDL can be assigned to CERT-EE to help protect critical national infrastructure. The CDL has also acted pre-emptively in other instances: in 2011, the CDL was on standby during the country's parliamentary elections: with many Estonians voting online, the voting system was an obvious target for cyber disruption. In 2012, the CDL organised a cyber crisis simulation exercise for Cabinet Ministers, fostering interest and preparedness in cyber crisis situations among the highest levels of government.[26]

Formation of the CDL confers a number of advantages to Estonia's crisis management capacity. First, it allows the government to effectively borrow civilian cyber security expertise as and when it is required. CDL members can work in the private sector yet still contribute meaningfully to national crisis situations. The 2007 informal alliance relied on a preexisting network of civil actors with high levels of trust between certain individuals; however, there were inevitable gaps in this network because it lacked a parent organisational structure. By contrast, the CDL does not rely on individual and personal relationships; it has a structure that renders it more coherent and sustainable in the long term.[27] Second, the CDL gives the government access to a cost-effective, highly skilled, and specialised reserve force. CDL members are volunteers who only get paid when they are formally called up. This is a much more efficient allocation of Estonian resources than the employment of cyber security professionals on a permanent basis. Third, as part of the military reserve, CDL members can perform a variety of functions including planned missions, training, exercises, planning, etc. This means that the CDL can play a meaningful role in any type of cyber crisis response. Unlike traditional Estonian reserve units, which protect military assets, the CDL protects non-military assets,

[24] Cardash et al., "Estonia's Cyber Defence League."
[25] Jackson, "Estonian Cyber Policy After the 2007 Attacks."
[26] Cardash et al., "Estonia's Cyber Defence League."
[27] Piret Pernik and Emmet Tuohy, "Cyber Space in Estonia: Greater Security, Greater Challenges" (Tallinn: International Centre for Defence Studies, August 2013).

including civilian critical national infrastructure. The CDL is therefore viewed favourably among the general public and the cyber security community in Estonia, generating a sense of goodwill in the popular perception that can motivate citizens to join its ranks.[28] In addition to the CDL, the Estonian government has developed a close relationship with private sector firms that own and manage critical national infrastructure. Given the high degree of economic liberalism in the state, maintaining such relationships remains highly important. These close industry links often emerge naturally owing to Estonia's small population and geographic size. And the links are in some respects formalised. Providers of vital services provide valuable input to government departments. For example, the Committee on the Protection of Critical Infrastructure was set up in 2011 and also includes private sector IT managers and risk management specialists.[30]

Establishment of the CDL was the most significant step the Estonian government has taken to formalise interaction with multiple stakeholders in dealing with crisis situations. It provides an established institution and forum for such interaction to take place. In addition, the presence of critical national infrastructure firms in government initiatives such as the Committee on the Protection of Critical Infrastructure shows that the government regards the private sector as an important voice. The initiatives discussed above, however, rely on volunteers or firms agreeing to voluntary guidelines. In addition to these largely voluntary initiatives, the government also enforces strict regulation of owners of critical national infrastructure subsystems. This has enabled the Estonian government to enforce governmental guidelines in cyber crisis situations.[31]

C. International Engagement

Turning to Estonia's interaction with the international community, it is clear that there is a strong emphasis on international engagement in the country's cyber crisis management strategy. In addition to its inclusive approach to domestic stakeholders, Estonia is also active in international fora. It acts as a strong advocate for greater international cooperation within the cyber security domain—and it has even encouraged citizens in other nations to become "e-residents" in Estonia, allowing them to establish Estonian digital identities as part of its vision of a "country without borders."[32] While much

[28] Cardash et al., "Estonia's Cyber Defence League."
[30] Ibid. For instance, the Emergency Act requires owners of critical national infrastructure firms to draw up on-going risk assessments and plans in the event of a cyber attack.
[31] Osula, "National Cyber Security Organisations: Estonia."
[32] Taavi Kotka, "10 Million 'e-Estonians' by 2025!" *Taavikotka*, https://taavikotka.wordpress.com/, accessed 4 December 2015.

of Estonia's international engagement relates to broader initiatives of this sort and long-term cyber security capacity-building, there is also a strong specific emphasis on cyber crisis management. This can be observed in the country's of various international security mechanisms, including bilateral, regional and multilateral institutions.

On a bilateral level, Estonia enjoys a close relationship with the United States. A letter signed on December 3, 2013 by U.S. Secretary of State John Kerry and Estonian Minister of Foreign Affairs Urmas Paet pledged to create stronger ties between the two states.[33] This included not only an effort to enhance ties between each state's central cyber security coordination bodies but also expressed an aspiration to build relationships between specific government departments (such as between the U.S. Department of Energy and the Estonian Ministry of Interior). There is also a clear agreement to cooperate at a cyber crisis management level: closer links were pledged between U.S. institutions, such as the National Cyber Security and Communications Center and the U.S. Computer Emergency Readiness Team (US-CERT), and Estonian institutions, such as the Estonian Information Systems Authority and CERT-EE. Both states also agreed to exchange information on instances of best practice in the protection of critical national infrastructure. This cooperation has extended to a working level encompassing the CDL, which has partnered with the 175th Network Warfare Squadron of the Maryland Air National Guard.[34] Estonia also places emphasis on regional (and bilateral) cooperation with other Nordic-Baltic countries. This cooperation includes a variety of functions such as sharing technical information, offers of emergency assistance, pooling of resources, and specific inter-agency cooperation.[35] The closeness of such regional cooperation is not surprising: because the Nordic-Baltic states are small nations, they are—as a practical matter—often compelled to work closely together on security affairs.

On the multilateral stage, Estonia is a highly active and leading proponent of intergovernmental cooperation in cyber security through fora such as North Atlantic Treaty Organisation (NATO), the European Union (EU), the United Nations, the Council of Europe, the Organisation for Security and Co-operation in Europe, the International Telecommunication Union, and other bodies.[36] In particular,

---

33 John F. Kerry, "Remarks at a Cyber Partnership Agreement Signing with Estonian Foreign Minister Urmas Paet" (Washington, D.C.: U.S. Department of State, 3 December 2013), http://www.state.gov/secretary/remarks/2013/12/218240.htm.

34 Cardash et al., "Estonia's Cyber Defence League." This partnership includes Estonian reservists taking part in secondments at the Maryland Air National Guard in the United States.

35 Liina Areng, "Lilliputian States in Digital Affairs and Cyber Security," *The Tallinn Papers*, Vol. 4, No. 4 (12 December 2014), pp. 1–15.

36 Osula, "National Cyber Security Organisations: Estonia."

Estonia has been a strong proponent of NATO's role in cyber security. The country has hosted cyber-related exercises such as the NATO Cyber Coalition and has also offered the Estonian Defence Force's cyber range for NATO alliance training.[37] Perhaps most notably, Estonia also hosts the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, whose simulation exercises give the centre some crisis management relevance despite its primary mission being research and analysis.[38]

4. UNITED KINGDOM

Cyber security is an acute security concern for the United Kingdom. In 2014, 90 percent of all UK households had a broadband connection, ranking fourth highest in the EU.[39] Many services vital to the UK economy are reliant on digital technologies—law, financial services, aerospace design, etc. In these sectors, a reliable ability to store information and communicate digitally is vital. As the government continues to implement a "Digital by Default" strategy by which government services are increasingly run online, the United Kingdom's digital dependence will only grow larger, meaning that cyber crisis management will become both more complex but also more important.

The first UK Cyber Security Strategy was published in 2009 and then updated in 2010. This led to the inauguration of cyber crisis management bodies such as the Office of Cyber Security, located in the Cabinet Office, and the Cyber Security Operations Centre, housed by the UK Government Communication Headquarters (GCHQ).[40] Yet it was not until the 2011 Cyber Security Strategy that the issue was supported with significant resources over a longer period with spending plans outlined until 2015. The Conservative-Liberal Democrat coalition signalled their commitment to the issue by allocating £650 million in 2011 with a further £210 million investment in 2013, while at the same time, cutting government spending in other areas significantly.[41] Although the strategy includes a number of broader objectives (such as education and training and long-term capacity-building), cyber crisis management is a main priority. Indeed, one of the four core objectives of the 2011 strategy is for the United Kingdom to be more cyber resilient. The protection of critical national infrastructure is at

[37] Pernik and Tuohy, "Cyber Space in Estonia."

[38] The centre, for instance, organises an annual "Locked Shields'" event, a technical, real-time network defence exercise that tests responses to hypothetical crisis situations.

[39] Anna-Maria Osula, "National Cyber Security Organisation: United Kingdom" (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2015).

[40] "Cyber Security in the UK" (London: Parliamentary Office of Science and Technology, 22 September 2011), http://researchbriefings.parliament.uk/ResearchBriefing/Summary/POST-PN-389.

[41] Francis Maude, "UK Cyber Security Strategy: Statement on Progress 2 Years on," (London: Cabinet Office, 12 December 2013), https://www.gov.uk/government/speeches/uk-cyber-security-strategy-statement-on-progress-2-years-on.

the heart of the document. In addition, the 2010 National Security Strategy ranked cyber attacks as a Tier One threat—above threats posed by nuclear attacks and organised crime.

A. Domestic Institutional Organisation

In many respects, the government's internal response to cyber crisis management echoes its stance on traditional crisis management situations. The UK Cabinet Office Briefing Room (COBRA), chaired by the Prime Minister, acts as the central crisis management response system for crisis situations, including those that are cyber-related. Similar to the United Kingdom's conventional response to crisis situations, however, the power and responsibility for a cyber crisis situation rests with the relevant government departments. Although the 2009 National Cyber Security Strategy created national entities to deal with cyber security, this trend has been reversed. The 2011 Cyber Security Strategy led to caution in escalating responsibility to centralised bodies.[42] Instead, such responsibilities "are provisional and can be adjusted if experience suggests that a different mix of inputs will produce better results."[43] This has resulted in a highly decentralised approach where a number of different government departments function in a multi-layered and dynamic system of coordination.

The emphasis in the United Kingdom's response is therefore on decentralisation. This means that much of the responsibility in cyber crisis situations lies with the specific government departments affected. Departments are allocated responsibility for sectors relevant to them. For example, the Department of Health would lead a response against any attacks on hospitals, while the Department of Transport would lead against attacks affecting rail or aviation networks. This decentralised strategy is intended to facilitate a formalised, yet flexible approach: the government can bring in different departments as and when the situation requires. As responsibility for each sector have been allocated to a government department, however, the decision-making process on which departments should handle a particular cyber crisis situation is intended to remain predictable and clear.

Within this decentralised approach, central government bodies have only limited authority; they act merely in a coordinating capacity seeking to deliver a coherent government response. The Cabinet Office provides the lead for this coordination role. Historically, responsibility for cyber security was

[42] *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space* (London: Cabinet Office, June 2009), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf.
[43] Osula, "National Cyber Security Organisation: United Kingdom."

vested in the Home Office, but in 2009 this role moved to the Cabinet Office in order to enable a response that focused on cyber security in a broader sense, that is, with a focus in areas traditionally outside the purview of the Home Office such as education and training.[44] Within the Cabinet Office specifically, the Office of Cyber Security was formed in 2009, later becoming the Office of Cyber Security and Information Assurance in 2011. And although CERT-UK has technical staff and expertise it can offer to government departments, use of this capability is reserved for severe emergencies on the theory that departments will normally be able to address problems themselves. In this regard, while CERT-UK does provide a technical perspective in cyber crisis situations, it only does so at a high level and the technical assistance it offers is deliberately limited. The main focus of the Centre for Protection of National Infrastructure (CPNI) is to prevent cyber crisis situations occurring by recommending security controls and offering advice on how to avoid crisis situations occurring. While necessary, the preventative emphasis of the CPNI means that the organisation has a limited role when a crisis situation is occurring.[45] Within this role, however, the CPNI has achieved a strong network of security-cleared contacts that can be utilised in the event of a crisis situation.

A regards the defence sector, the United Kingdom's cyber security strategy clearly emphasises a demilitarised approach. A large degree of the security responsibility is handed down to civilian departments. The military's primary responsibility is to protect its *own* networks; its remit does not extend to other government departments. Neither the 2011 National Strategy for Defence nor the Ministry of Defence (MoD) Defence Plan 2010–2014 mentions cyber attacks as a threat. In addition, the MoD has no jurisdiction to develop policy to protect critical national infrastructure and maintains only a limited advisory role to the CPNI and intelligence agencies such as GCHQ.[46]

The United Kingdom's decentralised strategy has the advantage of facilitating a flexible response to a crisis situation, but it comes with a number of shortfalls. From an institutional perspective, cyber crisis management has become highly crowded; inevitably, there is overlap and inefficiency between different departments. For example, both Her Majesty's Revenue and Customs (HMRC) and the Department for Work and Pensions run their own security operation centres, despite such a facility also being provided by CERT-UK. This results in unnecessary redundancy and an increasingly costly

[44] Ibid.

[45] Wayne Harrop and Ashley Matteson, "Cyber Resilience: A Review of Critical National Infrastructure and Cyber Security Protection Measures Applied in the UK and USA," *Journal of Business Continuity Emergency Planning*, Vol. 7, No. 1 (7 March 2014), pp. 149–162.

[46] Osula, "National Cyber Security Organisation: United Kingdom."

institutional response. There also concerns that with responsibilities divided among central government departments including the Home Office, the Foreign and Commonwealth Office, and the Cabinet Office, that the institutional response is overly complex.[47] In addition, such a devolved approach can foster dysfunctional relationships between departments. Government departments are not necessarily incentivised to cooperate with one another. Each department sees itself as "sovereign" and therefore prioritises its own survival and growth on a stand-alone basis. Different departments are potentially faced with conflicting objectives. It is reported that cultural gaps exist between organisations that seek to prevent cyber-attacks (e.g., law enforcement) and those that exist to respond to cyber attacks and minimise the damage (e.g., CERT-UK).[48] There is a real danger that the lack of cohesion creates a climate of mistrust, whose consequences for policy effectiveness during a crisis are potentially severe.

B. Stakeholder Mobilisation

From a cyber crisis management perspective, the UK government's interaction with other stakeholders is narrow and focused predominantly on privately owned critical national infrastructure. Liberal economic policies and a belief in market mechanisms have resulted in a large proportion of the United Kingdom's critical national infrastructure remaining in the private sector. Indeed, with 80 percent of the United Kingdom's critical national infrastructure owned and managed by the private sector, it dominates the critical national infrastructure landscape. These principles of economic liberalism and faith in market mechanisms are reflected in a cyber crisis management capacity. With the exception of some caveats (discussed below), the UK government treats the owners of private critical national infrastructure as responsible for managing cyber attacks against their own computer systems. There is a degree of trust upon which firms recognise that it is in their own interest to implement effective cyber security and cyber crisis management procedures. The government has created its own certificate in Cyber Essentials and Cyber Essentials Plus that firms can advertise if they adhere to a set of government cyber security standards. Although now mandatory for government contractors, the principle idea behind the certification scheme was to help private sector firms turn cyber security into a competitive advantage by exhibiting their competence in this area.

---

[47] Ibid.

[48] Tracey Caldwell, "Call the Digital Fire Brigade," *Network Security*, Vol. 2014, No. 3 (14 March 2014), pp. 5–8.

Government organisations play only a supporting role for an already sophisticated private sector, recognising that the private sector possesses many of the technical skills required and the government can make a contribution at a higher level in a coordination capacity. The government aims to use CERT-UK as a body to bring together private and public sector expertise in order to create a coordinated and cohesive response to cyber crisis situations.[49] In this regard, CERT-UK takes a high-level, strategic view of cyber crisis situations, with less emphasis on providing a sophisticated technical capability. For example, CERT-UK established the Cyber Security Information Sharing Partnership (CISP) in order to create a portal where both governmental organisations and private sector firms can share threat intelligence. Indeed, in crisis situations, CERT-UK are able to direct owners of critical national infrastructure to trusted security vendors rather than provide technical assistance itself.

From a cyber crisis management perspective, the UK government takes a special interest in privately owned critical national infrastructure assets. Both CESG (the cyber security branch of GCHQ) and the Centre for the Protection of National Infrastructure (CPNI) perform risk assessments and audit security arrangements for critical national infrastructure, producing risk and vulnerability reports. The CPNI has also made twenty specific control recommendations for owners of critical national infrastructure to implement.[50] Privately owned critical national infrastructure is, however, predominantly managed independently. There is a clear absence of any central point of control or of laws that require operators of critical national infrastructure to conform to minimum security standard.[51] The UK government acknowledges that regulation would be a blunt instrument in the field of cyber security. The government is aware that critical national infrastructure exists in a variety of sectors that should be managed and regulated differently. This is because of the specific challenges faced in certain industries, given the highly specialised nature of the technology used. For example, within the energy sector, infrastructure such as the power grid needs to be compatible with both antiquated physical structures such as power stations, installed over fifty years ago before cyber security was a priority, and highly modern systems and technologies. This is highly complex from a regulatory perspective: the rate of technological change is likely to outpace regulatory timelines. In

[49] "Cyber Emergency Response Team Launched by UK," *BBC News*, 31 March 2014, http://www.bbc.co.uk/news/technology-26818747.

[50] Harrop and Matteson, "Cyber Resilience."

[51] Warwick Ashford, "Is UK Critical National Infrastructure Properly Protected?" *Computer Weekly* (3 March 2011), http://www.computerweekly.com/news/1280097313/Is-UK-critical-national-infrastructure-properly-protected.

addition, the skills required to regulate in this area are highly specific, requiring a combination of legal skills and a deep technical understanding of complex, unique, and highly sophisticated systems.

The government's hands-off role and emphasis on self-regulation is not merely a matter of its own policy choices. There is a desire within government to implement stricter regulation and laws over particularly vital services such as the power grid and water supply. There is especially a concern within government about potential cyber crisis situations that would negatively affect the public to a significantly greater extent than an individual firm. For example, within the National Grid, a large-scale power outage would have a much greater effect on the nation (with loss of life and civil unrest possible) compared to the impact on National Grid itself (a small number of staff might be affected). This creates potential for misaligned priorities between the owners of privately operated critical national infrastructure and the public as a whole.

Despite the government recognising the need for further private sector regulation, the process remains difficult to implement. The private sector is protected from government interference through strong property rights that significantly constrain the government's role, making the enforcement of mandatory guidelines in a cyber crisis situation far from straightforward. Furthermore, difficulty in interpreting preexisting regulation has provided a challenge for government organisations. Traditional crisis management regulation, such as that which was focused on business continuity, was written before cyber security was considered an important issue. Yet there is nothing in such regulation that precludes its application in the domain of cyber security. Government departments are therefore currently in a process of understanding how preexisting regulation might apply in a cyber security context. For example, the financial services sector is an example where progress has been made. There is a strong link between industry and the Bank of England, which has established strong regulatory power, having already overseen simulated cyber attack exercises with banks.

Outside of the conventional defence structures, the United Kingdom operates a cyber reserve force in the form of the Joint Cyber Unit (JCU). Although the JCU comprises civilian reservists,[52] civil society as a whole is reluctant to participate in securing the United Kingdom. JCU reservists receive payment for their involvement; there would be significantly less interest if reservists were asked to volunteer for free services. In addition, the remit of the JCU is narrow, covering only military networks. In

[52] Tony Morbin, "Cyber Reserves Call on Private Sector," *SC Magazine* (4 October 2013), http://www.scmagazineuk.com/cyber-reserves-call-on-private-sector/article/314776/.

short, civilian and volunteer groups do not play a significant role in securing the digital systems of UK critical national infrastructure.

C. International Engagement

The United Kingdom's international engagement in cyber crisis situations largely reflects preexisting security and intelligence partnerships. In this regard, the United Kingdom's first point of contact would be trusted allies that would be consulted on almost any security issue. The United Kingdom predominantly utilises partnerships with historical allies such as the United States. Close multilateral alliances are also used. For example, the "Five Eyes" intelligence alliance between Australia, Canada, New Zealand, the United Kingdom and the United States is seen as one of the main multilateral channels to engage with trusted allies on the issue of cyber security. The United Kingdom is most willing to cooperate with foreign powers within a preexisting alliance structure that represents a track record of trusted exchange and shared language.[53]

Apart from cooperating with its closest trusted allies, in the event of a cyber crisis, two other avenues might be followed by the United Kingdom on a more *ad hoc* basis. First, the United Kingdom would seek to engage with the state where the source of the attack is located. While this does not assume origin or intent of attack, the United Kingdom would typically request assistance from this state. However, the United Kingdom's response will largely depend on the domestic character of the state in question and its ability and willingness to cooperate. The Foreign and Commonwealth Office is likely to provide assistance in opening up a dialogue between the United Kingdom and other such states. Second, the United Kingdom would also seek to establish links and cooperation with other victims of the attack. If another country is simultaneously being attacked, the potential for collaboration will increase; if the attack has already taken place, previous victims of the perpetrator may also be consulted.

Although the United Kingdom is actively engaged in international cooperative efforts on both bilateral and multilateral levels, within both cyber crime and cyber security capacity-building initiatives, the country appears less willing to cooperate with international partners on the cyber crisis management plane. This is partly because crisis partnerships are typically less publically visible;

[53] Liina Areng, "International Cyber Crisis Management and Conflict Resolution Mechanisms," in Katharina Ziolkowski, ed., *Peacetime Regime for State Activities in Cyberspace* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2013), pp. 565–588.

however, the United Kingdom appears comparatively reluctant to engage with others on this front. For example, the United Kingdom is considerably less vocal in supporting NATO's transition into the cyber domain, questioning the applicability of collective defence to the management of cyber conflict. Compared to Estonia, the United Kingdom is reluctant to extend Article Five of the NATO Washington Treaty (the concept of self-defence and the notion that a cyber attack on one NATO state would be interpreted as an attack on all NATO members) to the cyber domain. In addition, CERT-UK did not participate in Locked Shields, a NATO CCD COE cyber simulation exercise in 2015 as well as previous years. Instead, the UK has focused the majority of if its international efforts in cyber security to non-crisis related issues such as building cyber security capacity and developing cyber norms.

Overall, the United Kingdom's approach to cyber crisis management is not highly reliant on international cooperative mechanisms. Although London does regard international engagement as important, the domestic initiatives represent a significant proportion of the United Kingdom's crisis control capability. Outside case-by-case cooperation during specific incidents, trusted allies and preexisting intelligence-sharing mechanisms such as the Five Eyes are the main locus of cooperative efforts, underlining the importance that the United Kingdom places on trust and historical ties in the management of its international security relationships.

5. DETERMINANTS OF NATIONAL CYBER CRISIS MANAGEMENT STRATEGIES

Having examined the Estonian and the UK cyber crisis management strategies individually in the preceding sections, this section compares them and reviews their similarities and differences. In particular, the analysis identifies explanatory variables that may account for major differences in the two national models. The section also draws lessons and insights for policy and strategy.

A. Comparison between Estonia and the United Kingdom

Estonia and the United Kingdom have several similarities in their organisation of government institutions in relation to responding to cyber crisis situations. For both countries, there is a clear focus on civilian-led organisations that manage and coordinate cyber crisis situations, with the responsibility held by the Estonian Ministry of Economic Affairs and Communication and the UK Cabinet Office respectively. Both states have sought to demilitarise the cyber issue, raising questions more broadly on the role national militaries can and should play in cyber security and cyber crisis situations.

Moreover, both states have, to an extent, delegated cyber crisis situations to individual government departments; thus, specific departments typically find themselves responsible when cyber attacks are directed at, or affect, sectors relevant to them. But while both states have adopted similar approaches in this regard, the strategies, outcomes, and implications are quite different.

In Estonia, there remain very clear procedures to escalate responsibility to coordination bodies such as the Ministry of the Interior, the Estonian Information Systems Authority, and even the Prime Minster's Office. By contrast, given the United Kingdom's much larger governmental structure, the decentralisation process is more complex, with a multi-layered approach that makes it more difficult to escalate responsibility to higher coordination bodies. This also reflects constraints on the UK Prime Minister's power, given the existing limits on any rapid assumption of centralised control in crisis situations. For these reasons, central bodies such as the Office for Cyber Security and Information Assurance, CERT-UK, and CPNI largely have coordination roles with less decision-making authority or hands-on technical duties. Although perhaps inevitable given the larger size of the UK government, this reality makes for a less efficient allocation of resources with instances of repeated spending and the duplication of similar products and services.

Both states have also recognised that the government alone cannot respond effectively to cyber crisis situations. Their approaches in interaction with non-governmental stakeholders have been quite different, however. Estonia has taken a very wide approach to mobilising multiple stakeholders in a "whole of nation" approach that is consistent with the security strategy historically adopted by low-population states. This strategy is often referred to as a Total Defence Model, where it is recognised that given a small population, a full-time military force is alone insufficient to provide national security.[54] In a cyber security context within Estonia, the participation of civil society is reflected through the workings of the Cyber Defence League. Although it is part of a military organisation, the Cyber Defence League is clearly civilian in nature: it comprises volunteers from civil society who contribute in their spare time and are available in the event of a crisis situation. Furthermore, the remit of the CDL extends far beyond military infrastructure to the protection of national critical infrastructure in non-military departments. Estonia has backed up voluntary institutions with

[54] Talavs Jundzis, "Defence Models and Strategies in the Baltic States," *The International Spectator: Italian Journal of International Affairs*, Vol. 31, No. 1 (January 1996), pp. 25–37; Ants Laaneots, "The Estonian Defence Forces--2000," *Baltic Defence Review*, Vol. 1 (January 1999), pp. 1–7; and Milton Paul Davis, "An Historical and Political Overview of the Reserve and Guard Forces in the Nordic Countries," *Baltic Security and Defence Review*, Vol. 10 (August 2008), pp. 171–201.

relatively strict regulation applicable to privately owned critical national infrastructure; this creates a sense that the Estonian government is the clear source of control and leadership in crisis situations.

By contrast, within the United Kingdom there is a clear emphasis on a private sector–led approach, given that businesses own and manage the majority of critical infrastructure. The UK government's hands-off role has developed within the backdrop of a state that embraces economic liberalism and market mechanisms. Although largely deliberate, the lack of government interference can also be explained due to difficulties in interpreting existing regulation. In addition, unlike Estonia, the United Kingdom has been unable to mobilise other stakeholders such as civil society more broadly, operating a significantly more limited cyber reserve force. Given the United Kingdom's comparatively larger population—and by extension larger military presence—British citizens do not feel as compelled to participate in the provision of national security when compared to Estonia as there is a recognition that national security is sufficiently provided by full-time military personnel.

In terms of international engagement, Estonia is a much more active participant at the bilateral, regional, and multilateral levels. Although well organised and advanced at the policy level, Estonia simply does not have the same level of financial resources and government personnel as other states, meaning international engagement is crucial. That is not to say that the United Kingdom regards international engagement as unimportant. It should also be noted that the UK has made significant contributions to international cooperation in broader aspects of cyber security, including capacity building and the formulation of cyber norms. In a cyber crisis management context, engagement with trusted UK allies and as *ad hoc* cooperation with other potential victims, is taken seriously and seen as a useful way to avoid or mitigate a crisis situation. The United Kingdom, however, is not as reliant on international mechanisms, given the level of internal financial resources and government personnel that exist within the United Kingdom. This difference is clearly reflected in each state's stance towards NATO: Estonia has been an active proponent for extending NATO's remit to include cyber security and to apply Article Five to cyber attacks; the United Kingdom appears sceptical of NATO involvement in the cyber domain, arguing that its remit should extend to only the protection of NATO's own digital infrastructure and networks.

In sum, when comparing Estonia and the United Kingdom, it is difficult—perhaps impossible—to determine which state has the superior cyber crisis management strategy, because both states have

developed tailored policies specific to their own characteristics and needs. The focus of analysis now turns to an examination of the factors that explain the divergence in the two countries' strategies.

B. Explanatory Variables

This section identifies the most significant variables that influence the two state's cyber crisis management strategies and explains how the different approaches emerged, emphasising the important role played by the nations' size, history, threat landscape, political philosophy, and digital dependence.

i. Size

Size—both in relation to population size and level of government resources—has a significant effect on cyber crisis management strategy. Estonia demonstrates the advantages that a small-population state enjoys: it has an inherently small government that allows flexibility in adapting to new challenges. It is no coincidence that a number of historically low-tech states such as Sweden, Denmark, Finland, Austria, and Ireland, have gained leading positions in new industries like nanotechnology, biotechnology, telecommunications, and cyber security.[55] With shorter communication links in a society that fosters trust and flexibility, it becomes easier to organise a cohesive cross-governmental response to cyber crisis situations.[56] In addition, the Estonian government has been able to apply its Total Defence model to cyber security, initially with an informal alliance that has now progressed into a more formalised framework within the Cyber Defence League. On cyber power terms, then, Estonia's size has a curious reversible property. As noted earlier, a process of power diffusion is taking place in the cyber domain: states are struggling to adapt to cyber security challenges in part because low barriers to entry and the affordable cost of information technologies have empowered non-traditional actors such as private sector firms and civilians.[57] Yet, by virtue of being small, Estonia has expanded its Total Defence model into the cyber security context; therefore, the country is better equipped to mobilise non-governmental actors in a manner larger states have struggled to replicate.

---

[55] Areng, "Lilliputian States in Digital Affairs and Cyber Security."
[56] Ibid.
[57] Nye, *The Future of Power*, chap. 5.

Estonia's strategy is consistent with the historical behaviour of "small powers" in the international system. According to Rothstein, "a small power is a state which recognises that it cannot obtain security primarily by the use of its own capabilities, and that it must rely fundamentally on the aid of other states, institutions, processes, or developments to do so."[58] Although the Estonian cyber crisis management strategy is run efficiently, Estonia does not have the financial resources or government personnel of larger states and therefore looks to international partners to complement its smaller capability.[59] Small states such as Estonia understand that maintaining their "soft power" and good standing with other states is vital in order to garner international support in crisis situations.[60] It is therefore important for Estonia to meet its international legal and political commitments; indeed, Estonia is the only country in Europe to meet the rules of every international organisation it belongs to—including the Eurozone's target on debt, inflation and government deficit, and NATO's minimum defence spending threshold (2 per cent of GDP).[61]

By contrast, the United Kingdom's larger population has resulted in a larger government administration with a multi-layered approach. Although necessary given the population of the United Kingdom, it is arguably too complex, fostering institutional rivalry between departments and potentially resulting in inefficient allocation and duplication of resources. The United Kingdom is in many respects only a medium-sized country and it is likely that the institutional makeup would be even more complex (and potentially inefficient) in a country such as the United States that has an even larger population and federal government structure. Although its strong focus on the private sector appears deliberate,[62] the United Kingdom would be unable to mobilise civil society during a crisis in the way that Estonia can. While there are many reasons for this, it is most significant that civilians are unlikely to feel the same need for society-led security initiatives in a state with greater resources. In addition, as a larger state with greater resources, the United Kingdom is by definition less reliant on international cooperation.

---

[58] Areng, "Lilliputian States in Digital Affairs and Cyber Security."

[59] Joe Burton, "Small States and Cyber Security: The Case of New Zealand," *Political Science*, Vol. 65, No. 2 (4 December 2013), pp. 216–238.

[60] Ibid.

[61] Ibid.

[62] Maria Bada, Sadie Creese, Michael Goldsmith, Chris Mitchell, and Elizabeth Phillips, "Computer Security Incident Response Teams (CSIRTs): An Overview" (Oxford: Global Cyber Security Capacity Centre, May 2014).

ii. History

Historical ties and institutional dependencies are highly influential in determining the allies and international partners each state prefers to work with. Many geopolitical alliances, such as NATO and regional Nordic-Baltic alliances, are still being employed despite the fact that cyber security is essentially borderless and cyber allies can theoretically exist anywhere in the world. Yet historical ties, institutional dependencies, and trust have been prioritised over cooperation with more disparate and non-traditional allies. Estonia has a strong relationship with other Nordic and Baltic states and has long been a proponent of NATO, given the geopolitical situation. These links demonstrate how important trust is in building a network of state partnerships. Likewise, the US has deemed cooperation with Estonia a priority given their long-held presence and interest in Eastern Europe after the Cold War. While cyber security may be very different from conventional security challenges, Estonia has nonetheless relied upon historical allies and relationships.

The Estonian case also demonstrates the importance of historical factors in other ways. As a newly independent nation, within Estonia there is a sense of unity and the need for society to act as one in order for the nation to survive and grow. Moreover, many of Estonia's current cyber security policies were implemented after the 2007 attack—before 2007, Estonia did not even have a formal cyber security strategy (albeit like many states at the time including the UK). Thus, although long-rooted historical factors are important determinants of domestic and international partnerships, an actual recent cyber attack is significant because it concentrates resources and political capital to the issue in a way that would otherwise appear unjustified. The latter situation prevails in the United Kingdom: the British public are relatively unconcerned with cyber security in comparison to other security issues; the topic, for instance, barely figured in the 2015 general election campaign.

iii. Threat Landscape

Both Estonia and the United Kingdom have different areas of concern regarding their most immediate threats in the cyber domain as reflected in their cyber crisis management strategies. Estonia, a newly (re)independent state, faces a clear threat from its neighbour Russia that is significantly more powerful in a military context.[63] This highlights the relevance of geopolitical factors.[64] Although cyber

[63] Andrus Park, "Russia and Estonian Security Dilemmas," *Europe-Asia Studies*, Vol. 47, No. 1 (January 1995), pp. 27–45.
[64] Pami Aalto, "Beyond Restoration: The Construction of Post-Soviet Geopolitics in Estonia," *Cooperation and Conflict*, Vol. 35, No. 1 (2000), pp. 1–24.

attacks are in effect borderless, when a state such as Estonia is concerned about a physical attack from a local neighbour, this concern inevitably spills over into the cyber domain given that aggressor states increasingly regard cyber attacks as a valid use of force—either in isolation or in tandem with a conventional attack.

Given the importance to the domestic economy of sectors such as financial services and aerospace design, it is important for the United Kingdom to have access to reliable online services and the ability to store intellectual property securely. Therefore, with cybercrime reportedly costing the UK economy £27 billion a year,[65] it may be that cybercrime and fraud are deemed as greater priorities in the United Kingdom than in Estonia. Although cyber crisis situations are undoubtedly still regarded as a significant threat to the United Kingdom, the importance of other cyber security issues may explain why a smaller proportion of resources are dedicated to cyber crisis management in the United Kingdom. The focus on a greater number of cyber security issues also reflects the availability of relatively more resources in the United Kingdom.

iv. Political Philosophy

Political philosophies, specifically the views held on the role of the state, are also significant determining variables. Within the United Kingdom, there is a strong sense that the private sector is the most efficient provider for a number of critical services. Therefore, even seemingly unrelated policies such as the reduced or minimal state agenda that goes back to the period of Margaret Thatcher have implications for cyber security in 2015. There is also a belief from a crisis management perspective that private sector firms are commercially incentivised to implement their own security. Although there are concerns about the potential of market failure, trust in the private sector remains a key feature of the UK strategy. Similar issues have played out in Estonia where market mechanisms have likewise been embraced by policymakers.

The United Kingdom's decentralised strategy within government, where centralised cyber security bodies operate a limited hands-off coordination function with weak authority, also largely reflects the structure of the country's political system, where much of the power for managing departments lies with the relevant cabinet minister as opposed to the Prime Minster. By contrast, in Estonia there is more emphasis on the need for a wide group of stakeholders to contribute to security. This factor

[65] Dan Raywood, "Cost of Cyber Crime in UK Estimated £27 Billion," *SC Magazine* (17 February 2011), http://www.scmagazineuk.com/cost-of-cyber-crime-in-uk-estimated-at-27-billion/article/196583/.

relates to variables discussed above, such as Estonia's size and history. Estonia also enforces compulsory military service for all male citizens, meaning that many citizens have prior experience in contributing to state security. In addition, compared to other states, the use of technology is more deeply embedded in the day-to-day life of its citizens. Because of the preeminent role that technology has played in Estonia's transition from Soviet occupation, technology and digital systems are deeply entrenched in notions of security and, indeed, in the very concept of statehood (as exemplified by new initiatives such as "e-residency") to a far greater extent than in the United Kingdom.

v. Digital Dependence

Digital dependence clearly shapes the relationship between technology and security in the two countries. As Estonia has invested in technology in order to overcome many of the transitional challenges it has faced in recent history, the country has become highly reliant on many of these digital systems. This level of dependence clearly has implications from a cyber crisis management perspective. Generally, as states increase their reliance on cyber systems, the consequences of attack against those systems are more severe, meriting a greater proportion of resources being dedicated to cyber security.

The United Kingdom also has a high level of reliance on technology. As critical infrastructure becomes increasingly connected to digital systems, there are very clear consequences in the event of an attack. At the moment, however, the level of digital dependence is lower that in Estonia, with fewer systems digitalised; therefore, the issue of cyber crisis management is further down the political agenda. In addition, the United Kingdom's main economic sectors make other cyber security issues, such as cyber crime and financial fraud, bigger priorities for the UK cyber crisis management system.

* * *

The explanatory variables discussed above are by no means exhaustive: it may be that other factors are more significant where other states are concerned. This paper is unable to suggest which variables are most significant; there is, however, potential for further study where more variables are controlled. For example, by looking at all the Baltic and Nordic states (which are more similar in a number of the explanatory variables discussed), the importance of specific independent variables may be clearer. Strategic thinking and policies on cyber crisis management and cyber security more broadly are still

rudimentary; it may therefore take considerable more time before states have fully developed their strategies and can be compared in a more meaningful manner by future scholars and analysts.

C. Lessons for Strategy and Policy

Having examined the strategies of Estonia and the United Kingdom, this paper now considers policy lessons and conclusions—both for Estonia and the United Kingdom as well as for other states more broadly.

Estonia deserves credit for its response to the cyber security challenge. Given the lack of government resources of a smaller state, it is vital for Estonia to maintain its efforts to embed cyber security into its national culture and ethos and garner the expertise of civil society in the provision of state-level cyber security. Russia's invasion of Eastern Ukraine demonstrates that the Kremlin remains a viable threat to Estonian interests and provides ample incentives for Estonians to remain active participants in their state's security. Estonia has also sought to make up for its lack of internal resources by engaging with international partners. As previously discussed, there are undoubted benefits to this cooperation. There is, however, a danger that Estonia will grow overly reliant on international assistance. As Russian invasions into Georgia in 2008 and Ukraine in 2013 have shown, Eastern European states hoping for international protection against Russian threats are likely to end up disappointed. Although Estonia is a NATO member, it should never take collective defence for granted—especially in the cyber domain, where precedents for the application of this doctrine (and other inherited security mechanisms) are still being established.[66]

The United Kingdom, meanwhile, should develop and improve its organisation of cyber crisis management *within* government. Given its large size, it is appropriate to decentralise cyber security responsibility to individual departments. A centralised strategy such as Estonia's would likely not work in the United Kingdom; it could merely fracture government institutional relationships further. Nonetheless, the disadvantages of a decentralised strategy require remedy: the government should consider policies that incentivise collaboration between departments and provide clearer guidelines over institutional remits and it should develop further oversight and coordination efforts in order to reduce unnecessary overlap and repeated spending by different departments on the same services, thereby making the implementation of cyber crisis management policy more cost-effective.

[66] Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security*, Vol. 38, No. 2 (October 2013), pp. 7–40.

Although UK policymakers may be tempted to replicate the successes of the Estonian cyber reserve model,[67] such an approach would not necessarily succeed in the United Kingdom. Crucially, with the absence of a clear and more powerful threat (as Estonia experiences with Russia) and as a larger state, the United Kingdom will struggle to motivate civil society to participate in security as willingly as their Estonian counterparts do. The UK government will have to continue to provide strong incentives for participation, including paying members for the training and exercises they participate in. The United Kingdom can take inspiration from the broad remit of the Estonian Cyber Defence League. The responsibility of the UK Joint Cyber Unit is restricted to strictly military assets but should expand to protect other government assets in the future. Although private-sector firms may be reluctant to grant a reserve force access to their systems, there are a number of government functions and systems that would benefit from the skills and expertise of a reserve force. On the international front, the United Kingdom is making encouraging steps forward in its cooperative efforts. These steps should continue and are likely to do so naturally as institutions such as CERT-UK continue to develop their resources and organisational cultures. Although international cooperation alone is by no means a definitive solution to cyber security problems, it can offer a useful supplement to other measures that involve, for example, information sharing across diverse actors and sectors in multiple national jurisdictions.

The lessons drawn from this comparative study may apply, in a limited fashion, more broadly in other national contexts. The most important lesson to take away from the Estonia-United Kingdom comparison concerns the importance of a *relative* approach to the formulation of cyber crisis management policy—that is, one that builds on nation-state characteristics. States whose policy directions in the cyber domain represent an abandonment of national identity will face difficulties in implementing policy, whether because it will encounter problems of domestic legitimacy or problems of institutional disorientation. Policymakers should not regard this reality as a restriction on their ability to write policy; they should instead realise the opportunity that exists to exploit the natural advantages that each nation possesses. For example, a small state is naturally poised to exploit fast communication links and low levels of bureaucracy; a state with a sophisticated private sector or academic institutions is well placed to utilise knowledge and expertise outside of government; a state with strong international partnerships should ensure cooperation is extended into the cyber domain;

[67] David Blair, "Estonia Recruits Volunteer Army of 'Cyber Warriors'," *The Telegraph*, 26 April 2015, http://www.telegraph.co.uk/news/worldnews/europe/estonia/11564163/Estonia-recruits-volunteer-army-of-cyber-warriors.html.

and so forth. There is in cyber security problems a source of optimism for policymakers: while the related policy challenges are largely novel, preexisting policies and partnerships are often more germane than they may first appear. For example, both the UK and Estonia have successfully extended historical international security partnerships into the cyber domain and aspects of traditional security strategy are reflected in the cyber security strategy. Nonetheless, policymakers should look toward other states for inspiration: a limited but still important number of policies and strategic decisions may be transferrable from one state to another. Furthermore, learning from states with more mature cyber security strategies and policies can be a valuable tool for decision-makers operating in less developed policy contexts—there are possible advantages to being late in the game. But in the end it is imperative that specific political, historical, and cultural factors are considered to ensure the implementation of policy remains viable.

6. CONCLUSION

States are faced with a number of options in framing strategic responses to cyber crisis situations. As the above discussion has shown, there is no "one-size-fits-all" policy: no single strategy has proved to be inherently more effective than its alternatives. A good strategy, rather, is that which is tailored to the specific circumstances of the state in question—both to optimise the best possible response from the state as a whole and to create a strategy that accurately reflects the challenges and threats that the state actually faces. Inevitably, tensions exist among the possible strategic choices that states can make. For example, within the institutional organisation of the government, it is important for the whole of government to assume involvement and responsibility in order to deliver a broad and comprehensive defence. It is also important, however, to have a cohesive strategy as well as a clear control and leadership structure. Thus there is a tension between a bottom-up approach that builds inclusion and a top-down focus on concentration of policy direction and control. Furthermore, a number of dilemmas surface when states have to address the extent to which they should rely on a wide range of stakeholders. Crucially, Estonia has shown how integrating voluntary domestic networks and international partners into the crisis control strategy can bolster the strength of the response; however, voluntary agreements are not binding, making it difficult to predict and guarantee the actual availability of assistance during crisis situations.[68] Conversely, government regulation can secure a specific level of support by compelling a given stakeholder response, but may be off-putting to the affected parties if they perceive it a blunt instrument.

[68] Rain Ottis, "Lessons Identified in the Development of Volunteer Cyber Defence Units in Estonia and Latvia," (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 18 December 2012).

With these strategic dilemmas in mind, no one state has an approach that represents the superior way to manage cyber crisis situations. Neither Estonia nor the United Kingdom has a naturally superior strategy. In fact, in many respects, the strategy of each state has distinct advantages and disadvantages, linked to each country's particular characteristics. For example, as a small state, Estonia benefits from a clear and efficient governmental process for managing crisis situations; at the same time, because of its fewer resources, Estonia is more reliant on international assistance. By contrast, as a larger state, the United Kingdom is more self-reliant—but this comes at the price of a more complex and disparate governmental approach to crisis management.

Increased reliance on cyberspace has led to a hugely challenging security environment. Cyber attacks have the potential to destabilise critical national infrastructure; a viable response mechanisms to the possibility of such attacks is a crucial part of a nation's crisis management strategy. Although states are faced with novel technical challenges, in many respects cyber security reflects traditional security challenges. For example, geopolitical issues remain relevant in determining the nature of cyber threats that a state faces—as illustrated by Estonia's concerns over future Russian attacks. International cooperation in cyber crisis situations shows that historical ties and institutional dependencies are influential in alliance formation. This relationship, however, may be inappropriate in situations where historical allies have not adapted to cyber security challenges in the same way or at the same rate as advanced cyber nations such as Estonia. Historical ties and institutional dependencies are important in 2015, primarily because of the rudimentary state of cyber security strategy; in consequence, this paper predicts that future alliances will increasingly form on the basis of ideological similarities as opposed to historical factors or geographical proximity (though ideological similarities will often arise where states are in proximity to each other or share historical links). Given the largely borderless nature of the cyber domain, there is also a real prospect that states will form non-traditional and geographically disparate alliances.[69]

The role of the state in cyber security also differs from other security domains. Given the diffuse nature of the issues, it may be extremely difficult for the military to adapt to and confront cyber threats. By contrast, the private sector is increasingly relevant because of the lack of relevant skills

[69] For example, in 2013, Brazil and Germany co-presented a UN Resolution on privacy in cyberspace, despite a lack of historical ties or geographical proximity. Colum Lynch, Shane Harris, and John Hudson, "Exclusive: Germany, Brazil Turn to U.N. to Restrain American Spies," *Foreign Policy*, 24 October 2013, http://foreignpolicy.com/2013/10/24/exclusive-germany-brazil-turn-to-u-n-to-restrain-american-spies/.

and resources possessed by governments and because in some states it and manages the majority of critical digital systems. In countries such as Estonia and the United Kingdom, where there is a very large private-sector involvement in the provision of cyber security, the government faces significant constraints in its ability to manage crisis situations; it is therefore unclear what role the government will be able to play in the long term. Less government control in the cyber domain does not necessarily equate to a weaker cyber crisis management responder for the country concerned, however. Indeed, the ability to mobilise wider stakeholders is an important aspect of the strategies of both Estonia and the United Kingdom. In both countries, non-state actors such as certain private firms and civilian groups are accorded a privileged role in the conduct of state security, highlighting the increasingly blurry distinction between state and non-state agency in the cyber domain.

This paper has identified a number of political, historical, and cultural factors that significantly shape and constraint states' cyber crisis management strategies. While many states share similar technical challenges, their responses to cyber crises may be quite different at the strategic level, given the importance of non-technical factors. For this reason, significant strategic differences exist between Estonia and the United Kingdom—two technologically advanced states. Therefore, there are likely to be even greater differences between developed and developing states. As a result, there are significant limitations to the generic advice and recommendations that can appropriately be applied to all states based on these two case studies. Instead, the analysis of cyber crisis response strategies requires an emphasis on nation- and context-specific factors. While particular features of Estonia's or the United Kingdom's strategies merit general emulation, there is no single ideal approach that is universally applicable.