CENTRE FOR TECHNOLOGY & GLOBAL AFFAIRS

www.ctga.ox.ac.uk

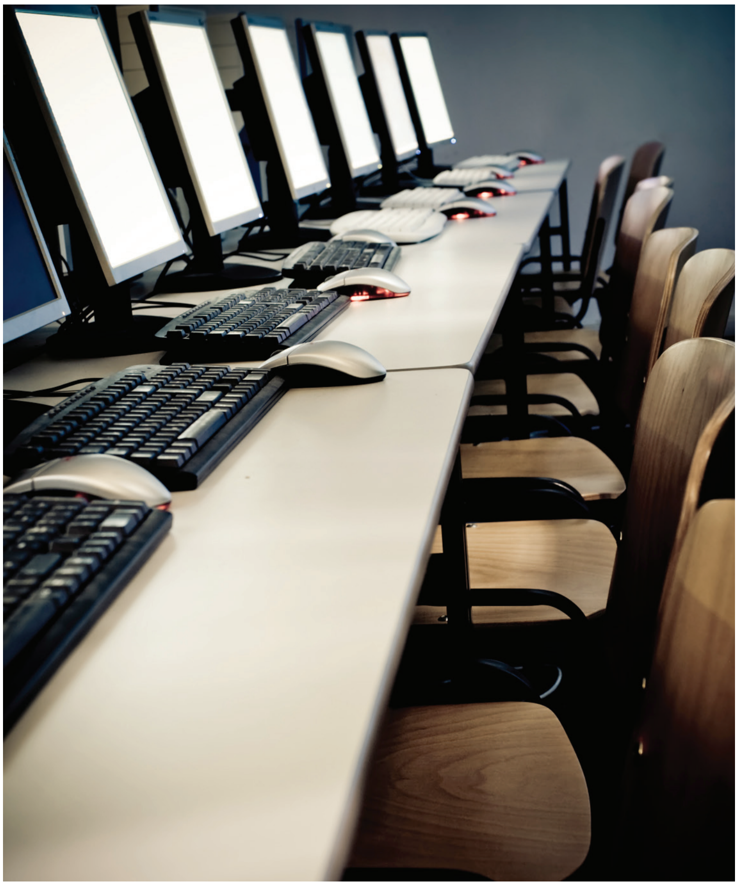
UNIVERSITY OF OXFORD

Working Paper Series – No. 10 March 2019

Beyond Awareness: The Breadth and Depth of the Cyber Skills Demand

Jamie Collier
Research Affiliate, Centre for Technology and Global Affairs
University of Oxford
jamie.collier@cybersecurity.ox.ac.uk

Andrew Martin
Professor of Systems Security
University of Oxford
andrew.martin@cs.ox.ac.uk



European Union
European Social Fund

Investing
in your future

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

ABSTRACT

As cybersecurity challenges have multiplied across society, there is increasing confusion about how those challenges should be addressed. For many years, computer security was the preserve of a small cadre within the IT profession: in most cases, limited to a few individuals in banks and those concerned with National Security. It now seems to be widely accepted that this narrow perspective is simplistic and inadequate, because it fails to address some of the biggest problems. And yet a vision of cybersecurity as "everyone's problem" seems equally untenable. Many people are simply not equipped to make meaningful decisions relating to this topic, whether in their private or professional lives. In addressing contemporary cybersecurity challenges, a "responsibility paradox" has therefore emerged: while it is now widely acknowledged that cybersecurity extends beyond the purview of IT departments, others often fail to embrace further leadership on the issue. To help in overcoming this problem, this paper explains the importance of involving an eclectic range of disciplines, organizations, and skill sets in addressing cybersecurity challenges. Acknowledging the impracticalities of everyone becoming a "cybersecurity expert," the paper discusses practical measures for overcoming skill gaps. The empirical focus of the paper is on EU cybersecurity policy, with special attention to Estonian and regional efforts that seek to facilitate collaboration between diverse disciplines and to improve security practices.

1. INTRODUCTION

Cybersecurity has become such a pressing concern for businesses and organizations – as well as individuals – that there is a widely reported shortage of "cybersecurity professionals."[1] And yet the description of the skills needed by such professionals is often narrowly drawn – skills centred around risk assessment, or around technical familiarity with a particular product or standard. In fact, the challenge for society is surely much broader than this. The cybersecurity skill shortage extends to other disciplines and areas of expertise such as law, business strategy and public policy. Moreover, there is a particular dearth of talent that can understand and communicate across different domains; for example, individuals who can speak the language of a technical cybersecurity team yet who can also articulate concerns to a board or ministerial level in an accessible manner.

Such a breadth of concern is clearly seen in the routine requirement for staff in many sectors to undergo training in "cybersecurity awareness" despite evidence that such training has at best a negligible effect on overall cybersecurity outcomes.[2] Such awareness may be a desirable baseline, but it is not itself adequate to equip professionals with the skills they need to make decisions cognisant of their security implications. It is often recognised that responsibility for cybersecurity extends far outside the "IT department" – ideally, all the way to the boardroom – yet paradoxically key decisions about the design of products, services, and operations are necessarily made by professionals with no particular cybersecurity expertise.

Such disconnections inevitably lead to bad cybersecurity choices being made. Without proper communication and input from a variety of perspectives, security policies often result in requirements and procedures that pit security against utility and usability. Users typically find ways to circumvent overly stringent and inconvenient security policies. Faced with unreasonable demands (i.e. "change your password now, and ensure these rules are followed"), users will typically follow a path that involves the minimum effort (changing password *qwerty1* into *qwerty2*) without truly engaging with the risks and reasoning behind the policy. Likewise, civil servants may bypass encrypted work computers that include awkward and disruptive security protocols by using their personal devices for professional work instead. In other instances, sensible security policies are ignored. The 2017 *WannaCry* ransomware spread affected systems in over forty British National Health Service (NHS) hospitals as a result of software which had not been updated in line with the manufacturer's recommendations.[3] While running up-to-date software features is routine security advice, in a resource-constrained environment, the impact of not following that advice may not be foreseen. For managers faced with many pressing concerns, a delay to a time-consuming, costly, and uncertain update programme may seem a rational decision. This surely arises if the technical risks of outdated software, and the underlying system dynamics of proactive adversaries, are not adequately articulated at upper executive or even government minister level.

Sometimes, a complex technical analysis is necessarily reduced to a simple answer, in order that a senior executive may take an apparently informed decision. The authors of

[1] James Nunns, "Cyber Security Skills Shortage to Hit 1.8 Million by 2022," *Computer Business Review*, June 6, 2017, http://www.cbronline.com/news/cybersecurity/protection/cyber-security-skills-shortage-hit-1-8-million-2022/; Nicholas Megaw, "Cyber Security Sector Struggles to Fill Skills Gap," *Financial Times*, November 18, 2015, https://www.ft.com/content/4cabd0fe-8940-11e5-90de-f44762bf9896; Alice Hancock, "Skills Shortage Exposes UK Companies to Cyber Crime," *Financial Times*, March 14, 2017, https://www.ft.com/content/47fe9410-08d8-11e7-97d1-5e720a26771b.

[2] Maria Bada, Angela Sasse, and Jason Nurse, "Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour?", 2015, pp. 118–31.

[3] João Medeiros, "WannaCry Laid Bare the NHS" Outdated IT Network – and It's Still Causing Problems," *Wired*, May 24, 2017, http://www.wired.co.uk/article/nhs-cyberattack-it-ransomware.

this paper are aware of one company which in the early days of "bring your own device"[4] was faced with a decision about which employees' devices were sufficiently secure to be allowed to connect to the corporate infrastructure. Executives asked for a technical analysis, and received the distilled answer "Android: No; iPhone: Yes." The CTO was amused (but confused) to meet his opposite number in a similar firm a few weeks later, and learn that the second firm had asked the same question within its own organization, and received back the answer "Android: Yes; iPhone: No." It is hard to avoid the conclusion that an apparently scientific process was in fact nothing of the sort. How is the Board to make meaningful decisions about managing risk to the business in this context?

Issues of cybersecurity are confounding because they touch many parts of the enterprise including product development, email communications, and the storage of intellectual property, yet often have no easy default answer. Buying the newest solution may expose one to unforeseen risks; retaining an old solution may also be far from risk free, especially when it falls into the "legacy" category and ceases to be supported by its designer or manufacturer.

Perhaps there is a deeper tension at work. It is often said that the security analyst or systems designer must have a sceptical or devious mind – the kind of mindset that enables one to think like the attacker or adversary – as well as the skills necessary to envisage the attacks which might be perpetrated. By contrast, the entrepreneur thrives in taking risks, and tends to be optimistic about outcomes. Constant exposure to the worst of human nature may render one cynical; a customer-centric, service-oriented mentality might tend to make one think the best of people.

It has also long been said that this tension is best resolved through multi-disciplinary teams. Yet, such efforts are often poorly executed. Executives may initially get involved in the formulation of a broad strategic plan, yet the execution is often left to technical security teams to implement with boards reluctant to revisit the issue or to refresh themselves on security protocols thereafter.

This tension is also seen on a national and international stage when politicians discuss cybersecurity. Here, an increasingly technically literate press are quick to expose flaws in government pronouncements. For example, as the then UK Home Secretary, Amber Rudd was criticized for her muddled article on encryption where she both acknowledged the benefits of encryption while also implying that it was not necessary for "real people."[5] Likewise, when the German and French ministers of the interior sent a joint letter to the European Commission calling for measures to stem terrorist incidents, their demands for technology companies to develop encryption systems that are secure yet easily crackable by law enforcement were criticised by the technical press given the impossibility of developing such a system.[6] Here, other issues are at play: the politician may not be an expert on the technical details of the policy he or she espouses, but will have a large group of advisors, all of whom have their own agendas. The details of the argument being espoused may be obscured by a need – or perceived need – for secrecy (from law enforcement and intelligence agencies). Alternatively, cybersecurity issues are increasingly becoming politicized. Government statements that promise a tough line on encryption regularly proceed terrorist attacks as a way for government officials to signal (albeit perhaps in a superficial and ineffective manner) that they are responding to the attack at hand. Likewise, to justify increased spending on cybersecurity, politicians have a habit of invoking the dangers of cyber terrorism despite an empirical reality that suggests that the threat is severely overblown.[7] However, whatever the incentive, the result is often a failure to communicate – and hence we might say a failure of democracy.

In this paper, we address why no one academic or professional perspective can address these issues alone and discuss how an interdisciplinary solution provides some prospect for overcoming the problems outlined above. The focus then turns to examine current efforts in Estonia and the European Union, where the need for an interdisciplinary approach to cybersecurity is imperative in the long-term. Finally, we consider some of the difficulties of creating an interdisciplinary approach before outlining our conclusion.

2. THE NEED FOR AN INTERDISCIPLINARY APPROACH

Because the technologies and practices of cyberspace are commonplace to so many aspects of society, each group of professionals sees the challenges of cybersecurity through its own disciplinary lens. Yet, it may be generally observed that without an integration of these perspectives, meeting the security challenge tends to be forever out of reach. This is in large part because security is in essence not about analysing and gaining control over some physical process,

[4] A "Bring your Own Device" (BYOD) refers to an approach that allows employees to use their own personal devices (such as phones, tablets and laptops) for their work.

[5] Amber Rudd, "We Don't Want to Ban Encryption, but Our Inability to See What Terrorists Are Plotting Undermines Our Security," *The Telegraph*, July 31, 2017, http://www.telegraph.co.uk/news/2017/07/31/dont-want-ban-encryption-inability-see-terrorists-plotting-online/.

[6] Iain Thomson, "Germany, France Lobby Hard for Terror-Busting Encryption Backdoors – Europe Seems to Agree," *The Register*, February 28, 2017, https://www.theregister.co.uk/2017/02/28/german_french_ministers_breaking_encryption/.

[7] The grugq, "Cyber Terrorists Can't Cyber," *Medium*, January 1, 2016, https://medium.com/@thegrugq/cyber-terrorists-can-t-cyber-144406a2d78b.

but about frustrating the aims of one or more adversaries. If those adversaries' thinking is more agile or integrated than that of the defenders, they will tend to have the upper hand. There is a strong alignment between some academic and professional disciplines of relevance – but also much divergence. Since we are considering primarily questions of education, research, and practice, all of these realms are relevant to our study.

Professional Silos

We may identify a number of professional and scientific disciplines which naturally and – unhappily perhaps – form "thought silos" containing welcome wisdom but failing to connect to necessary insights in other fields.

Clearly, in almost all areas of human endeavour, there are points of contact between different disciplines and specialisms; this is the stuff of civilization and society. A well-understood example of this context is seen in developing an understanding of climate change and its impacts. This is an issue requiring contributions from climate physicists, oceanographers, economic geographers, alternative energy providers, policy and regulation experts, and more – even perhaps historians of science. All of these skill sets are fundamental in confronting the problem, albeit from entirely different approaches and perspectives. Yet, while the need for such an eclectic approach to climate change is now accepted as conventional wisdom, the cybersecurity challenge, by contrast, is too often regarded as solely a technical challenge. Yet, the need for improved connections between silos are profound. The narrow view of cybersecurity is at least in part due to the relative immaturity of the discipline, and its present state of flux; indeed, it could be argued that cybersecurity is not a discipline but an emerging meta-discipline. It may be that at some future time, there will be a common understanding of the elements of disciplines X and Y which must be understood in discipline Z in order to build an understanding of cybersecurity. Such a distillation of views is certainly not available now; it must be a matter of debate whether it will become evident in the foreseeable future.

The outmoded distinctions that have been historically established between various academic and professional disciplines fail to reflect contemporary reality. Indeed, if disciplinary boundaries were drawn again today, topics such as cybersecurity demonstrate that issues as disparate as software engineering, cryptography, and system design can overlap with non-technical questions of privacy, philosophy, and deterrence. Yet, the majority of current thought silos were formed before the issue of cybersecurity emerged. The relationships between various thought silos are based, therefore, not on the needs of today but on historical precedent. There is established crossover between international relations and law since both disciplines have long examined war. Similarly, the intelligence community has an established link with cryptography academics given their mutual interest in encryption. Yet, for the most part, the crossovers that are needed to examine cybersecurity effectively do not exist: international relations academics have not needed to collaborate with system engineers in the past; policy experts have not been required to consult software engineers and cryptographers. Often, even the subdivisions within two separate disciplines are wildly misaligned. An example is the issue of privacy. For the technical community, both privacy protection and digital rights protection are examined together with the material differences in processes insignificant. Within the legal discipline, however, the distinction is markedly more significant, with one related to criminal law and the other related to the private law of contracts.

The lack of disciplinary overlap, and therefore the lack of communication between disciplines, has meant that many thought silos have proceeded in isolation without the necessary consultation and communication. The policy community (in both an academic and professional capacity) have been guilty of producing theories and agreements that are not grounded in technical realities. International efforts such as the UN Group of Governmental Experts (a UN-mandated working group in the field of cybersecurity) and the production of the Tallinn Manual (a non-binding, scholarly effort to apply international law to the issue of cybersecurity) have been criticized by those in technical and operational communities for failing to adequately understand technical details related to the topic at hand.[8] By contrast, in proposing political responses to some of the most significant incidents in recent years, those from more technical backgrounds have often proposed solutions that while sensible in practice, are wholly inconceivable due to the reality of politics, bureaucratic interests, and negotiations.

Table 1: Thought Silos

Business
Computer science
Crime
Cryptographers and other mathematicians

[8] Arun Mohan Sukumar, "The UN GGE Failed. Is International Law in Cyberspace Doomed as Well?," *Lawfare*, July 4, 2017, https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well; Dave Aitel, "UNGGE and Tallinn 2.0 Revisited," *CyberSecPolitics*, August 23, 2017, https://cybersecpolitics.blogspot.co.uk/2017/08/ungge-and-tallinn-20-revisited.html; Dave Aitel, "Reflections on the GGE 'Failure'," *CyberSecPolitics*, July 7, 2017, https://cybersecpolitics.blogspot.co.uk/2017/07/reflections-on-gge-failure.html.

Education and training
Insurance
Intelligence
Internet, media and communication studies
Law
Politics and international relations
Public policy
Psychology
Risk management
Security operations teams
Security Solutions vendors
Systems engineers and designers; software develops

Example Domain: Privacy

An illustrative example of this problem exists in in the protection of individual privacy. Drivers for this concern come in part from business goals (some vendors make privacy a positive distinctive for their product), in part from ethics, in part from politics (a desire to avoid emulation of repressive regimes of past and present). These goals are made precise in law and regulation, for example, the European General Data Protection Regulation.[9] That this regulation is a considerable evolution of the two-decades-old EU Data Protection Directive (95/46/EC) is an indication that privacy represents something of a moving target, driven in part by the evolution of technology, and in part by a developing understanding of how privacy may be violated or abused.

The appropriate technical implementation of such regulations is of course a contended area with no simple solutions. The "Privacy by Design" movement[10] begins to make the bridge, albeit driven by a more abstract notion of privacy than necessarily that embodied in legislation. As an initiative from Information and Privacy commissioners in various jurisdictions, it remains quite high-level (some would say detached from reality). Its interpretation within a particular software or systems design is a matter of a separate professional judgement – and it is worth noting that here (as in many areas of security) good design may be undermined by unthinking implementation. For example, in collecting, processing, and presenting data from the *Streetview* programme, Google claims to have followed good practice. But according to some accounts, someone tasked with actually building the system collected far more data from nearby WiFi access points and their users than was necessary, thereby potentially undermining a carefully considered privacy policy.[11]

Example Domain: HCISec

The area of human-computer interaction has long been a stand-out area of computer science: making computer systems which people can use easily and productively requires quite a different skill-set from the task of designing and implementing software. Critically, this draws on insights from psychology and sociology. More recently, it has become clear that such concerns are crucial in the development of security-related functionality. A seminal paper[12] reported the difficulty that "ordinary" users had in making use of mainstream email encryption software.

The problem is seen clearly in the issue of password management. The requirements placed upon users in choice of passwords and frequency of changes are driven (at least in part) by sound technical analysis, but often take no account of the functioning of human memories, or of the social functions surrounding, say, password sharing in an office environment. Moreover, the burdens placed upon users are driven in part by an economic analysis: it is cheaper to ask users to manage difficult passwords than to implement systems which avoid the need for such passwords. Inter-disciplinary studies have thrown these issues into sharp relief, leading ultimately to radical changes to official password guidance.[13]

Example Security Challenge: Attribution

Hackers have access to several technical tools that help them to cover their tracks,[14] thereby making it difficult for states to definitively name a perpetrator – something that has become increasingly necessary as hacking has taken on a geopolitical dimension.[15] To overcome the inherent

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

[10] Cavoukian, Ann.: Privacy by Design (2009); Fischer-Hübner, Simone. IT-security and privacy: design and use of privacy-enhancing security mechanisms. Springer-Verlag, 2001.

[11] Jemima Kiss, "Google Admits Collecting Wi-Fi Data Through Street View Cars," *The Guardian*, May 15, 2010, https://www.theguardian.com/technology/2010/may/15/google-admits-storing-private-data.

[12] Alma Whitten and J D Tygar, "Why Johnny Can't Encrypt: a Usability Evaluation of PGP 5.0," 1999, p. 14–14.

[13] "Password Guidance: Simplifying Your Approach," *NCSC*, January 7, 2016, https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach; "Digital Identity Guidelines," *NIST*, accessed September 25, 2017, https://pages.nist.gov/800-63-3/sp800-63b.html.

[14] For example hackers have used techniques such as jump hosts, VPNs, Tor and open relays to obscure their origin for decades. See Bruce Schneier, "Attributing the DNC Hacks to Russia," *Schneier on Security*, January 9, 2017, https://www.schneier.com/blog/archives/2017/01/attributing_the_1.html.

[15] Lily Hay Newman, "Hacker Lexicon: What Is the Attribution Problem?,"

challenges of attribution, a "constellation of evidence"[16] is required: drawing on a variety of sources and investigative techniques can help to make a more compelling case about an aggressor's identity. Crucially, if a combination of strategic, operational and technical data makes attribution more convincing,[17] it follows that a variety of skill sets are required to overcome the problem.

Demonstrating that the Russian Government acquired, and subsequently leaked, Democratic National Committee (DNC) documents during the 2016 US presidential election provides a case in point. Technical forensic evidence was naturally a vital component of attribution attempts. For example, the command-and-control server (essentially a digital fingerprint) used on the DNC server was linked to a previous attack on the German parliament that German security agencies has publicly attributed to Russian military intelligence.[18]

Linguistics analysis also helped to understand the context of the hack. Gucifer 2.0, the online pseudonym that declared responsibility for the hack, claimed to be Romanian. Yet, this was disproven after Gucifer 2.0 was asked to explain the hack in Romanian; a linguistic analysis quickly showed that Gucifer 2.0's sentence constructions was unusual for Romanian natives, with a strange use of diacritics and accented letters.[19] In addition, there was significant variety in the pseudonym's written English, possibly suggesting that a team of operators were behind the online persona.[20]

Political and strategic analysis also help to provide context. It has been argued[21] that the DNC hack sits comfortably within the wider framework of Russia's evolving military doctrine which comprises a broader view of what can qualify as a military target or military tactic.[22] This shows that consideration of political factors can be highly informative in providing a contextual backdrop.[23]

3. AN INTERDISCIPLINARY APPROACH TO EU CHALLENGES

Europe faces several emerging cybersecurity challenges that no single thought silo can confront in isolation. Instead, a cohesive response provides the greatest prospect for overcoming these nascent security issues. This section explores challenges of European cybersecurity, with a special emphasis on the approach of Estonia – a leading nation in this field – to their resolution.

Digital Single Market

The stated priorities of the Estonian Presidency of the Council of the European Union, wherein cybersecurity forms a key item of the agenda, provide a case in point. For the further development of the European digital single market to be a success, public confidence in the security of the infrastructure is vital. In this context, cybersecurity should not be perceived as an inconvenience or as an additional cost, but more importantly as an enabler of future growth in the digital realm. For foreign businesses and investors who are increasingly aware of the importance of cybersecurity, a secure and resilient digital single market gives Europe an increased competitive advantage over other regions.

A cohesive approach to cybersecurity is particularly important in the development of the European digital single market – a complex and multifaceted project. So far, EU initiatives have taken a mature approach with the 2013 Cybersecurity Strategy of the European Union acknowledging that "the private sector owns and operates significant parts of cyberspace, and so any initiative aiming to be successful in this area has to recognise its leading role."[24] This has led to a significant investment in public-private partnerships.[25] Furthermore, in May 2018, a new set of EU rules on data protection and privacy in electronic communications and a first common cybersecurity law was introduced. Encouragingly, both schemes acknowledge the wide group of stakeholders involved in cybersecurity.[26]

Going forward, the Digital Single Market's continued success will depend on a mature regulatory approach, which entails a difficult balancing act. On the one hand, a range of organizations have continuously failed to implement even

Wired, December 23, 2016, https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/.

[16] Ibid.

[17] Rid and Buchanan, "Attributing Cyber Attacks."

[18] Thomas Rid, "All Signs Point to Russia Being Behind the DNC Hack," Motherboard, July 25, 2016, http://motherboard.vice.com/en_uk/read/all-signs-point-to-russia-being-behind-the-dnc-hack.

[19] Lorenzo Franceschi-Bicchierai, "Why Does DNC Hacker 'Guccifer 2.0' Talk Like This?," *Motherboard*, June 23, 2016, https://motherboard.vice.com/en_us/article/d7ydwy/why-does-dnc-hacker-guccifer-20-talk-like-this.

[20] "All Signs Point to Russia Being Behind the DNC Hack."

[21] Ibid.

[22] Dmitry Adamsky, "Cross-Domain Coercion: the Current Russian Art of Strategy," *Proliferation Papers* 54 (November 2015).

[23] Jason Healey, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks," February 3, 2012.

[24] "Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyberspace," February 7, 2013.

[25] In July 2016, the European Commission launched a new public-private partnership on cybersecurity expected to trigger €1.8 billion of investment by 2020. See "Commission Signs Agreement with Industry on Cybersecurity and Steps Up Efforts to Tackle Cyber-Threats," June 5, 2016, http://europa.eu/rapid/press-release_IP-16-2321_en.htm.

[26] "The Directive on Security of Network and Information Systems (NIS Directive)," *European Commission*, July 5, 2016, https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

routine cybersecurity protocols. This has led to suggestions that there is a market failure in cybersecurity.[27] Yet, the solution to such a problem is complex. Even states such as the UK that have a high level of cybersecurity maturity have previously acknowledged that regulation is a blunt instrument for improving cybersecurity.[28]

Government officials have an extensive range of policy responses to choose from, including further regulation, the development of certification schemes, shifting legal liabilities, etc.[29] Here, there are open challenges in determining sensible options to pursue given that many government and intergovernmental interventions risk being ineffective or even counter-productive. With a broad menu of policy options to choose from, there is an inherent complexity in deciding how to proceed. Fortunately, for many of these issues, the EU has a successful track record of delivery. Outside of a cybersecurity context, European officials have previously intervened to ensure that the privacy and rights of European citizens are upheld – principles related to cybersecurity and that will be vital to a correctly functioning Digital Single Market.[30] EU policy can also draw on the valuable insights gathered from its member states, many of which have already considered how they should intervene (or not) to improve cybersecurity. In confronting such a nascent security challenge, sharing instances of best practice will be vital. Crucially, as an intergovernmental organization that sets regulation, directives, and other legislative acts, EU officials have the expertise and experience to develop the mature regulatory approach that the continued development of the Digital Single Market will require.

Although the EU has the potential to improve cybersecurity in the digital single market, there is still an acute danger that further political intervention will be ineffective, or even counterproductive, if the technical, practical and operational realities of cybersecurity are ignored by government officials who do not understand the issues in depth. Cybersecurity issues are also becoming increasingly politicized: on contentious issues such as government vulnerability disclosures, numerous actors have direct interests related to the issue, leading to active lobbying efforts that risk skewing debates and leading to bad policy outcomes. To minimize risks of governmental ignorance and further politicization, European and national government officials should consult widely, working with a variety of private sector organizations, as well as those with technical and operational insight. Going forward, governments should seek to develop and collaborate with talent that can articulate the regulatory and policy implications of more technical details.

Empowering All Citizens

Estonian priorities for the Presidency of the Council of the European Union rightly emphasized the importance of empowering all citizens online.[31] This notion is particularly important when it comes to cybersecurity. Unlike conventional security challenges where citizens have turned to the state as the provider of defence, anyone can be targeted online directly; aggressors can therefore bypass state-driven defensive efforts. Citizens must understand how they can stay safe online and avoid involuntarily sharing their personal data with third parties. Educating and informing the public about cybersecurity is therefore paramount to empowering users online and ensuring they can defend themselves adequately.

The importance of empowering a wider demographic of citizens to secure themselves online is uncontentious. Yet, turning this vision into a practical reality is far from straightforward. Given the variety of demographics vulnerable to cyberattacks, confronting this challenge requires a multifaceted response: teaching children and teenagers about staying safe online requires an altogether different strategy to educating professionals about common attack methods or informing the elderly about email scams. It is clear that any solution will require a wide range of skills and expertise. Teaching school children about how to stay safe online is necessary as students increasingly interact with technology at a young age. Here, education experts are vital in designing viable curricula, running pilot schemes that investigate the sort of messages and educational techniques that are most effective, etc.

Understanding the psychology of our cybersecurity habits

[27] Emanuel Kopp, Lincoln Kaffenberger, and Christopher Wilson, “Cyber Risk, Market Failures, and Financial Stability, WP/17/185, August 2017,” *IMF Working Paper* 17, no. 185 (August 7, 2017); Tom Reeve, “_Industry’s Cyber-Security “Market Failure” Must Be Addressed,” *SC Magazine*, May 23, 2016, http://www.scmagazineuk.com/industrys-cyber-security-market-failure-must-be-addressed/article/498249/; Sam Jones, “GCHQ Chief to Say Free Market Failing on Cyber Security,” *Financial Times*, November 9, 2015, https://www.ft.com/content/4ec3e438-8708-11e5-90de-f44762bf9896.

[28] Jamie Collier, “Strategies of Cyber Crisis Management: Lessons From the Approaches of Estonia and the United Kingdom,” in *Ethics and Policies for Cyber Operations*, ed. Mariarosaria Taddeo and Ludovica Glorioso, (Cham, 2016).

[29] Nathan Alexander Sales, “Regulating Cyber-Security,” *Northwestern University Law Review* 107, no. 4 (2013): 1503–68; Eli Dourado, “Working Paper: Is There a Cyber Security Market Failure?,” *Mercatus Center Working Paper* 12, no. 5 (January 23, 2012).

[30] Examples include the ePrivacy Directive, the General Data Protection Regulation, and the “Right to be Forgotten” ruling. See “Digital Privacy,” *European Commission*, July 30, 2014, https://ec.europa.eu/digital-single-market/en/policies/online-privacy; “Factsheet on the ‘Right to Be Forgotten’ Ruling ,” *European Commission*, accessed September 21, 2017, http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf.

[31] “Cybersecurity and the Estonian Presidency,” *EU2017*, August 3, 2017, https://www.eu2017.ee/news/insights/cybersecurity-and-estonian-presidency.

is also vital, yet this is often neglected. Governments have previously launched cybersecurity awareness campaigns in an attempt to educate the public about how they can stay safe online. Yet, often these initiatives fail short in their aim of changing behaviour with the scale of the psychological challenge underestimated: people must not only be able to understand and apply the advice on offer, they must also be willing and motivated to make personal changes (a challenge that requires shifting attitudes and intentions).[32] To enact change, understanding the drivers that shape people's habits, (including conscious, unconscious, personal, environmental and social factors) is vital.[33] Moreover, public messaging campaigns must also be implemented without overwhelming citizens – an individual faced with numerous ambiguous warnings and complicated advice, may experience "security fatigue" and consider abandoning all protection efforts entirely.[34]

Further, to empower citizens online, cybersecurity advice, and the development of solutions, should reflect empirical realities. Ultimately, it is impractical to assume that policymakers and business executives have the time and interest to develop cybersecurity skills and expertise. Despite countless warnings, people will still continue to click on untrusted links and open emails from unknown sources. Accounting for these practical realities, the question, therefore, becomes how systems and protocols should be designed accordingly. Again, an eclectic range of skillsets are required to develop useful proposals, both to understand this problem and develop solutions. Understanding how organizations operate regarding cybersecurity practices requires people that understand business management. Developing viable systems and protocols involves both technical staff and those with an awareness of risk management.

Defending Against Disinformation Campaigns

Recent disinformation and election interference campaigns have further highlighted the political impact of cyber incidents. The most well publicized of these cases was the attempt by the Russian government to unsettle the political process in the US in the run up to the 2016 Presidential election.[35] In a European context, there are suspicions of similarly unwelcome interventions, most clearly observed in the French 2017 presidential election.[36]

Stopping, or at least mitigating, the negative impact of such campaigns requires a cohesive state response. Many of the sensitive files that were obtained by the Russian government in the US election were obtained through rudimentary intrusion techniques that are certainly preventable. The lack of cybersecurity awareness at the higher levels of government is certainly disappointing and underlies the need for political organizations and policymakers to step up. Yet, it also means that a small investment in training could have a disproportionally positive impact on improving cyber defences. This foremost requires better coordination between politicians and specialist cybersecurity teams.

Security planners should also assume that foreign adversaries will continue to obtain and leak sensitive data, despite an increased awareness among political groups about the risks of such data leaking.[37] If leaks and other disinformation tactics continue, any adequate solution must involve a variety of disciplines by necessity given the address broader and more strategic issues at hand. For international relations academics, there are open questions regarding how states can nullify the deniability of election interference that aggressors thrive on. Here, researchers should consult with policymakers to ensure that their proposals contain practical solutions. Media specialists will also play a role in proposing how political groups develop effective PR strategies to mitigate the negative impact of politically-motivated leaks. At the European level, there are questions on how to address organizations such as WikiLeaks that were complicit in the dissemination of foreign government-provided leaks. Further, with much of the disruption coming from the leaks being publicized in mainstream publications, governments must decide how they should persuade, or even mandate, the way in which news outlets report on foreign government-directed leaks – a contentious issue for news outlets given the tension between a free press and becoming unwitting agents in a foreign government disruption campaign.[38]

Of course, not all cybersecurity issues can or should be taken on at an intergovernmental level. Nations have different cultural and political views that lead to diverging opinions on issues such as privacy that necessitate alternative security models. Yet, with national borders increasingly irrelevant online, at least in terms of the proposition of digital threats, the response to cybersecurity should contain a strong international component. Multilateral bodies and international cooperation will therefore play an important

[32] Bada, Sasse, and Nurse, "Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour?."

[33] Ibid.

[34] Ibid.

[35] "Russian Hacking and Influence in the U.S. Election," *The New York Times*, accessed September 21, 2017, https://www.nytimes.com/news-event/russian-election-hacking?mcubz=3.

[36] Andy Greenberg, "The NSA Confirms It: Russia Hacked French Elecction 'Infrastrucutre'," *Wired*, May 9, 2017, https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/.

[37] Jamie Collier and Monica Kaminska, "Bashing Facebook Is Not the Answer to Curbing Russian Influence Operations," *Council on Foreign Relations*, September 18, 2017, https://www.cfr.org/blog/bashing-facebook-not-answer-curbing-russian-influence-operations.

[38] Ibid.

role in overcoming many of the cybersecurity challenges outlined above. Given the EU's track record of implementing change based on widespread political consensus, it provides the ideal platform for many contemporary cybersecurity challenges including those outlined above. Crucially, with numerous international organizations seeking to expand their purview to incorporate cybersecurity, EU policymakers should consider where developing initiatives within the EU brings clear added value – as opposed to unhelpful mission duplication.

4. POLICY RECOMMENDATIONS

Confronting contemporary cybersecurity challenges requires nations and organizations to adopt a more interdisciplinary approach to the issue, as well as a need further develop interdisciplinary skills. While these may be regarded as distinct challenges, they are, in fact, symbiotic: cultivating an interdisciplinary approach within an organization will naturally enhance crossover and mutual understanding across different skillsets while holistic educational schemes will help in shifting cultures to accommodate a more eclectic range of viewpoints. The ensuing discussion outlines three policy recommendations that can help to achieve these aims.

Develop Educational Schemes

For all of the above discussion on the lack of talent in non-technical disciplines, there remains a chronic shortage in various technical disciplines across many economies.[39] Governments have begun to wake up to this reality and new educational schemes have been introduced, including integrating coding in school curricula.[40] Formal educational initiatives are complemented by the proliferation of online classes available,[41] many designed specifically for children and free of charge. Yet, despite signs of progress, governments could certainly do more to foster technical talent. Going forward, it will be important to further develop educational programmes in both computer science and other related generalist STEM subjects, as well introduce more focused cybersecurity programmes. This will include specialist cybersecurity programmes, but should also include the further integration into the curricula of related fields (such as including cybersecurity modules in computer science university courses). As such efforts are implemented, education ministers must ensure that that the skills being taught in the classroom or lecture theatre match up with those in demand by industry.

As stated earlier, addressing cybersecurity challenges requires a wide range of skillsets. Further incorporating cybersecurity into non-technical disciplines will help to broaden the topic. It also has exciting potential to reinvigorate educational programmes. For example, while there is a shortage of cybersecurity skills, the unemployment levels in disciplines such as psychology are high with many graduates struggling to find work in their chosen field. Yet, psychology has a number of applications to cybersecurity – in particular, understanding the human aspects of the process. Therefore, if psychology degrees included modules that examined issues such as the human factors of cybersecurity, there is potential to address both the cybersecurity skill gap and the high unemployment rates for psychology graduates. There is also evidence to suggest that incorporating cybersecurity into other disciplines improves engagement: an Estonian pilot in schools that teaches cybersecurity alongside drones has helped to get students interested in both topics. Likewise, an MBA programme at Tartu University has a strong emphasis on cybersecurity, thereby providing future business leaders with an important baseline understanding of the security issues at hand.

Finally, further investment is required into interdisciplinary initiatives. Such schemes have a twofold advantage: they not only equip individuals with a holistic and interdisciplinary cybersecurity skill set, they also foster a network of individuals who share a common body of knowledge while often also possessing a deeper and more specific skill set in a particular aspect of cybersecurity. Here, there are a number of successful case examples. An e-governance masters at the Tallinn University of Technology focuses on IT solutions to government challenges with interoperability between different faculties at the university central to the programme. Similarly, at the University of Oxford, a range of independent cybersecurity research centres based at various academic departments has meant that the issue is covered from various unique perspectives.[42] A cybersecurity doctoral programme[43] also actively recruits from an eclectic range of disciplines, fostering otherwise unlikely crossover

[39] Rian van Heur, "Fears of Software Skills Shortage in Germany and the Netherlands," *Computer Weekly*, January 5, 2016, http://www.computerweekly.com/news/4500269840/Fears-of-software-skills-shortage-in-Germany-and-the-Netherlands; Miles Dilworth, "UK Digital Skills Deficit Poses Major Risk to Company Productivity, BCC Warns," *The Independent*, April 6, 2017, http://www.independent.co.uk/news/business/news/uk-digital-skills-deficit-company-productivity-bcc-workforce-training-staff-workers-employees-a7670371.html.

[40] Parmy Olson, "Why Estonia Has Started Teaching Its First-Graders to Code," *Forbes*, September 6, 2012, https://www.forbes.com/sites/parmyolson/2012/09/06/why-estonia-has-started-teaching-its-first-graders-to-code/#2bfd34db1aa3; Phil Johnson, "France to Offer Programming in Elementary School," *IT World*, July 16, 2014, https://www.itworld.com/article/2696639/application-management/france-to-offer-programming-in-elementary-school.html; ET 2020 Working Group on Digital Skills and Competences, "Coding and Computational Thinking on the Curriculum," *European Commission*, September 2016.

[41] Examples include CodeAcademy, Free Code Camp and Codewars.

[42] "Cyber Security Oxford,"https://www.cybersecurity.ox.ac.uk.

[43] "Centre for Doctoral Training in Cyber Security," *Cyber Security Oxford*, https://www.cybersecurity.ox.ac.uk/education/cdt.

and collaborations.

Develop Career Pathway Schemes

Educational programmes designed to nurture a breadth of cybersecurity skills will go to waste if they are unaccompanied by appropriate career pathways schemes. Organizations that primarily target top universities in their recruiting strategies must realise that cybersecurity talent resides in unconventional places. With vast learning resources on topics such as hacking and programming available online, the resumes of many of the top cybersecurity professionals are often thin on formal education. Here, there is a challenge for governments and businesses alike in in providing the pathways for highly talented, yet unconventionally educated talent to find jobs.

There have been countless stories of teenager hackers getting arrested, often for infiltrating high-profile organizations. This is not necessarily surprising. Young people do not have the maturity or full awareness to realize the implications of their actions. Others may just be bored and keen to experiment. Here, governments and the private sector must do better by providing positive pathways for talented young people to express and further develop their skills. If the proverbial teenage hacker is made aware of how they can get involved with the cybersecurity industry, and use their talent in a way that has a positive impact on society, they are less likely to delve into illegal activity.

One scheme that seeks to connect such talent to career pathways is the UK-based Cyber Security Challenge. The organization runs a series of national competitions, learning programmes, and networking initiatives with industry designed to identify, inspire and enable more people to become cybersecurity professionals. Going forward, such initiatives should be further developed, and possibly promoted on a European-wide scale.

Yet, developing career pathways is arguably a more acute challenge for non-technical backgrounds. For those interested in the intersection of cybersecurity with subjects such as policy, linguistics, psychology, etc., it is not always clear how they can become involved in the industry. Many large tech and cybersecurity organizations will feature almost exclusively technical skills in their job opening requirement, despite many of these same firms acknowledging that they need to also look at broader topics, such as the human factors of cybersecurity or questions related to risk management and business strategy.

Schemes to cross thought silos should also be part of the solution. Governments and European wide political initiatives could, for example, develop schemes to embed those with technical or operational insight into teams that examine broader political, strategic, and regulatory questions. Likewise, businesses should identify individuals from security teams who can communicate complex security issues in an accessible manner to other business units and executives. Develop career conversion pathway schemes to place individuals with a technical or operational background into government and policymaking roles (where such individuals have demonstrated the potential and aptitude to change roles). Developing interdisciplinary institutions is also vital. Estonia, as one country that has had success in developing a holistic approach to cybersecurity owes much of this progress to the creation of institutions such as an e-governance academy that creates and transfers knowledge and best practices on e-governance, e-democracy, open information societies, and national cybersecurity.[44]

Strengthen Continuing Professional Development Schemes

Many professions place requirements on members – through registration requirements or membership of professional bodies – to undertake Continuing Professional Development (CPD). In some cases, this is the location of “cybersecurity awareness” training mentioned above. Such courses are, as previously discussed, of questionable value in training people on what to click, what to share, how to manage passwords, and so on. They clearly fall far short of providing professionals with the thinking skills necessary to ensure that new business processes are robust in the presence of security challenges. The introduction of new technology to a particular work context (an office and an operating theatre are quite different; the risks to, say, an implantable medical device different again) may fall to the subject professional – even if the implementation tasks are delegated to technical experts. Here, then, is a suitable role for professional development courses, and baseline sets of knowledge and expertise to be acquired at various stages of career progression in a very wide range of professions.

Such career path plans will clearly, over time, begin to influence the design of educational programmes, far outside the conventional purview of cybersecurity education, with its particular technical biases. Indeed, it will be most constructive perhaps to begin with the definition of cybersecurity elements of CPD schemes for early-career professionals. Some will be shared across many professions (as with awareness training); some should be more discipline-specific.

Develop an Interdisciplinary Institutional Culture

While it is imperative for business leaders and government officials to become further involved in cybersecurity, there

[44] e-Governance Academy, http://www.ega.ee.

are also inherent risks in this process. For governments, there is a danger that political intervention will be counterproductive if the technical, practical and operational realities of cybersecurity are ignored. Likewise, if business leaders only approve a broad cybersecurity strategy but then neglect the issue for months or years, then they are not engaging meaningfully.

Overcoming these risks requires a genuinely interdisciplinary institutional culture. One way to develop this is through the creation of teams that comprise an eclectic range of skillsets and experiences. This would be particularly effective for political organizations – when it comes to policymaking for example, interdisciplinary teams could help enormously in examining regulation, legislation and policy. Such teams should be involved in both the formulation and the review of government processes. On issues that include interaction (or regulation of) the private sector, further developing public-private initiatives would also ensure adequate understanding between different organizations.

5 CONCLUSION: THE DIFFICULTIES AND PROMISE OF AN INTERDISCIPLINARY APPROACH

While an interdisciplinary approach has been advocated throughout this paper, there are clear difficulties in its implementation. These difficulties should not discourage organizations from adopting such an approach; but it is important to understand these inherent challenges. Three stand out.

First, the various divisions of an organization often have different cultures. The “hoodie vs. suits” caricature might be unfair, but it is certainly true that there are significant differences on a variety of factors including the expected uniform, working hours, the emphasis between hard and soft-skills, etc. Even differences in language can even cause significant confusion. For example, while active defence is conventionally understood as the use of offensive action to deny a potential aggressor a contested area or position within a political context, the technical cybersecurity community understand the term to mean an active involvement in identifying and countering threat to a network and its systems.[45] Crucially, with such divergence in culture, it cannot be assumed that fostering a more cohesive approach will be smooth.

Second, the incentive mechanisms within an organization do not necessarily support collaboration between various units within that organization. For example, many employees in a business are judged via performance metrics such as billable hours – yet, if half an employee’s time was spent developing understanding across an organization and building relationships with an IT department, this is not something that will necessarily get them much credit (in terms of the performance metrics that they are judged by) despite the obvious benefits in such collaborative initiatives. The same is true for academia. Academics are largely rewarded for publications in prestigious journals and conferences in their specific discipline – publishing genuinely interdisciplinary work may not therefore necessary help with career advancement.

Third, the entrance of new actors and cultures becoming involved in cybersecurity can become a source of tension. Those that have been working on cybersecurity for a long time understandably take offence to politicians intervening in the issue without truly engaging with the substance at hand. Rather than working together and engaging in constructive dialogue, interaction between different cultures and groups often become hostile. While this is understandable given the realities of basic human nature, it is not necessarily conducive to future progress on cybersecurity.

In the end, the current fragmented approach to cybersecurity is unsustainable; a change of mentality is required. Many instances of bad cybersecurity practice today are completely understandable as a by-product of a fractured approach to the challenges at hand. Of course, the existence of narrowly focused pockets of expertise will remain vital. It should also be recognized that an interdisciplinary approach that crosses silos will not “solve” current cybersecurity challenges. It is also true that developing approaches that cross thought and professional silos comes with both difficulties and risks.

But there are important and promising opportunities for regional and international organizations, such as the EU, to foster further collaboration between silos. By incorporating those with technical and operational skill sets further into the cybersecurity policy making process and by developing schemes to help individuals cross thought silos, the EU can set an example. By developing and promoting the importance of a variety of educational approaches to cybersecurity, the EU can help safeguard not only the cybersecurity of EU institutions, but also help to improve the overall security of the bloc.

Overall, the benefits of an interdisciplinary, cross-silo approach to cybersecurity are clear. It is imperative for governments and political organizations to recognize that current skill shortages in topics such as cybersecurity go far beyond a deficit of technical skills. While many aspects of an organization now recognize that cybersecurity should extend beyond the IT department, it is time for those in other areas to step up. This issue area is in urgent need of leadership.

[45] “Threat Intelligence in an Active Cyber Defense (Part 1),” February 17, 2015, https://www.recordedfuture.com/active-cyber-defense-part-1/.

CENTRE FOR TECHNOLOGY & GLOBAL AFFAIRS

UNIVERSITY OF OXFORD

www.ctga.ox.ac.uk

ABOUT THE CENTRE FOR TECHNOLOGY AND GLOBAL AFFAIRS

The Centre for Technology and Global Affairs at Oxford University is a global research and policy-building initiative focusing on the impact of technology on international relations, government, and society. The Centre's experts use their research findings to develop policy and regulatory recommendations addressing the transformative power of technological change.

The Centre serves as a bridge between researchers and the worlds of technology and policymaking to impact policy in the resolution of pressing problems across six technological dimensions: Artificial Intelligence, Robotics, Cyber Issues, Blockchain, Outer Space, and Nuclear Issues.

The Centre’s mission is (a) to provide leadership in creating new knowledge on practical problems affecting the security and welfare of governments, citizens, and private enterprises; (b) to influence major policy decisions and opinions in these arenas; and (c) to guide the work of leading technology developers and policymakers.

The Centre is based in the Department of Politics and International Relations at Oxford University. It is supported by core funding from Kluz Ventures.

Kluz Ventures

Centre for Technology and Global Affairs
Department of Politics and International Relations
University of Oxford
Manor Road
Oxford OX1 3UQ
United Kingdom

UNIVERSITY OF OXFORD | DPIR DEPARTMENT OF POLITICS & INTERNATIONAL RELATIONS