The Challenge of Networked Complexity to NATO's Digital Security

Laurin B. Weissinger
Lecturer
The Fletcher School
Tufts University

Abstract: In the aftermath of the 2016 Democratic National Convention (DNC) hack and with ongoing disinformation campaigns attacking democratic elections worldwide, cyber defence has never been more important for the North Atlantic Treaty Organisation (NATO) allies. However, current security strategies often fall short because they do not adequately address the problem of networked complexity. To protect cyberspace, national assets and key institutions, we must solve for the strategic, tactical and operational complexities of the technology stack, including its interconnections and interdependencies.

States and organisations must address three levels of complexity: entity, layered and networked complexity. Entity complexity is the complexity of a single component or system, for example, a central processing unit (CPU). Layered complexity arises when we layer multiple levels of complex hardware and software. The third level of complexity involves emergent networks and interactions of multi-layered technical and socio-technical systems.

This paper establishes the critical importance of understanding networked complexity in cyber security, a topic which is underrepresented in extant cyber security literature. It proposes practical solutions, including a focus on 'defence in breadth'. All systems, including consumer-grade products, must be shipped more secure by default. Mitigating networked complexity in cyber defence will also require better threat and attack modelling. Security strategies should move from hierarchical models to a graph-driven, networked understanding of cyber security that incorporates socio-technical dimensions. Lastly, states should leverage the security community and public-private partnerships.

Keywords: *Networks, complexity, national security, defence, cyber security*

1. INTRODUCTION

Today's world is digital, complex and networked; security must address that. Internet outages, cyber criminality like ransomware (Mathews, 2017; Conolly & Wall, 2019) and information operations like the DNC hack have already caused considerable damage (Nakashima, 2016; Taub, 2016). Western democracies are particularly vulnerable among digitised states due to how their societies and economies are organised. Free markets, individual liberties, free enterprise and open societies (Popper, 2013) foster complex network of ties rather than limiting actors to top-down relationships.

Socio-technical systems and 'information networks' (Castells, 1996; Castells, 2000; Castells, 2001) in their interconnected entirety constitute the basis and fabric of our society, making society and economy in Western democracies highly interdependent:

> A network society is a society where the key social structures and activities are organised around electronically processed information networks ... It's about social networks which process and manage information and are using micro-electronic based technologies ... The global economy is based on the ability of the core activities—meaning money, capital markets, production systems, management systems, information—to work as a unit in real-time on a planetary scale. [This] increases the complexity, the size and, ultimately, the volatility of global financial markets (Castells, 2001).

This paper explores networked complexity and the global cyber security risks that emerge when computer systems (comprising layers of complex components themselves) are connected across organisations and used to run crucial and complex social, bureaucratic and economic processes. The vulnerabilities described in this paper will only intensify with increasing, widespread use of oftentimes insecure (Singh et al., 2016) IoT devices, more industrial control systems and growing reliance on IT systems overall. Since 2007, more 'things' than people have been using the internet (Evans, 2011). Unless states develop a 'security in breadth' approach, these cyber security risks threaten the very existence of open societies and the democratic freedoms championed by NATO allies.

The paper explains how networked complexity threatens cyber security and how states and organisations can mitigate the dangers and solve for the challenges posed by networked complexity. The first section provides foundational framing for understanding interdependence and complexity. The second elucidates why interdependence and complexity are critical for contemporary cyber security. The final section proposes practical policy solutions.

2. HISTORY AND TYPES OF COMPLEXITY

This section describes how systemic interdependence and resulting complexity have developed alongside the evolution of technology and society over the last 150 years and categorises different tiers of this phenomenon. Emile Durkheim (1893), a scholar of modernity, conceptualised the increasingly specialising, interdependent structure of then-contemporary society in the late 19th century as 'organic'. Through specialisation, distinctive technology and mastery, experts become individually so productive that even groups of untrained individuals cannot match them. Society and its members specialise and optimise under organic conditions, relying on each other like organs in a body. This process creates ties and dependencies all across society.

Thus, each specialist becomes dependent on other social 'organs' to perform their own function. For example, contemporary agriculture in developed countries is a high-yield, high-tech enterprise, using drones, sensing technologies, and data mining (Meola, 2016; NIFA, 2020). Food production has become more effective and efficient, but farmers are now reliant on various specialist providers of niche technologies (Cyber Risk, 2020) that they require but cannot themselves produce.

Computers consist of interacting, complex and specialised hardware and software components and are built around similar ideas as Durkheim's organic society. This paper posits three levels of complexity (Table I) that apply to technical, social and socio-technical systems: entity complexity, layered complexity and networked complexity.

Table I: Types of Complexity

	Entity Complexity	Layered Complexity	Networked Complexity
Dimensions	Component/ Node	One-dimensional ties/dependencies	Multidimensional networks of ties/ dependencies
Ties / Dependencies	N/A (excludes manufacturing)	ties = $n^{components} - 1$	ties = $n^{components} * (n^{components} - 1)/2$
Dependency Types	N/A	Uni-directional	Multi-directional, interactive
Example	Random Access Memory Module	OS running inside virtual machine	Computer network used by organisation

Entity complexity speaks to the complexity or intricacy of a single component. For example, modern, general purpose operating systems are based on millions of lines of code written by multiple teams of engineers, under varying situational and procedural entanglements (Clarke et al, 2016). They are designed to function with different sets of hardware and software and in various circumstances. Truly grasping them as a whole, as Fathi's (2018)

account of the development of Windows Vista shows us, is nearly impossible. Correspondingly, many specialised professions, complete with their particular lexicons, cannot be easily grasped by outsiders due to their intricacy.

Layered complexity is the outcome of vertical dependencies, like running specialised applications on operating systems which can run virtually using a hypervisor that hands instruction down to the CPU. Similarly, in value chains, many business models and products rely on already complex products or services that they build on top of and cannot function without, for example, digital communications or developed road and rail networks.

This paper predominantly focuses on the third level: networked complexity. A multitude of interdependencies is a reality for both social and computer systems. Computer systems and value chains are not monolithic or simply layered, but rather an assortment of networked components (Mahutga, 2012). Analytically, such socio-technical systems present themselves as intricate and not always intelligible, webs of interdependencies, which is why networked complexity and the resulting security risks warrant particular attention. While some nodes and ties may be more important than others and some hierarchies exist, most of the relationships are necessary, or at least beneficial, to the overall functioning of a system. For example, software requires the hardware layers and most hardware is ineffectual alone—only complete systems function.

In this context, a 'system' is an entity or network that has a social function and includes all components necessary for operation. Some computer components, like graphics adapters, are essentially computers in their own right, but they cannot operate on their own. Similarly, a group of individuals with one social function, e.g. the production of goods, is a social system. For a manufacturing company, the IT department would be a subsystem or component; it is necessary but not sufficient for production.

Complex, networked systems are difficult to understand and predict while demonstrating emergent properties (Goldstein, 2011): different agents and subsystems interact and together create systemic evolution. This is why replicating complex (production) networks remains problematic for high technology like contemporary military systems (Gilli & Gilli, 2019). Accumulated, uncoordinated decisions on a micro level can effect macroscopic change (Schelling, 2006). The more functions, variables and relationships a system needs to manage, the more likely it becomes that unexpected events will occur and errors, inconsistencies and inefficiencies will be missed.

Even within components, networked complexity can exist: the philosophy of Unix, the system that inspired contemporary operating systems, is to create small programs that are extremely effective and efficient at doing one specific task and to make those specialist programs interact (Kernighan & Pike, 1984). Using and networking building blocks remains best practice in contemporary software development. System architects usually buy

standard hardware from expert manufacturers and use a proven operating system, relying on someone else's network and protocol implementations. Then they build upon an established database like MariaDB and packages like OpenSSL for encryption. Finally, software is written in higher-level programming languages designed by others. Only in outlying cases where existing building blocks are insufficient would one use lower-level code like Assembler or build specialised hardware. This adds additional complexity and vulnerabilities: many satellites rely on old, space-optimised, weight-and-power-limited computers that thus lack basic security features (Eddy, 2019).

To properly function, all systems and organisations require resources they often cannot provide, produce, or even fully understand (Hirsch, Fiss & Hoel-Green, 2009). In such complex systems, non-complex and complex errors and vulnerabilities emerge. The latter may be unpredictable or inconsistent in their macro-level effects (Schelling, 2006). This paper focuses on addressing the security issues that arise when we take many inherently intricate, niche-expertise-based products and connect them all into large and heavily interdependent networks that consistently cross the socio-technical divide.

3. How Networked Complexity Shapes the Security Environment

Organic interdependence and specialisation allow for considerable improvements in productivity, speed and quality in computing (Dally et al., 2020) and in society (Krugman, 1980; 1981). The same networked complexities and dependencies produce unintended and unwanted security vulnerabilities. This section explains how complexity shapes the security environment, how dependencies both increase and decrease security risks and how complex and non-complex errors and vulnerabilities arise.

As Table I shows, a complete security analysis of a networked system quickly becomes impossible. Each added node or subsystem can significantly increase dependencies and interactions that would have to be modelled, analysed and proven to be secure.

Nevertheless, 'outsourcing' security often results in a clear net benefit if not overdone (Schneier, 2002). Expert providers can leverage specialisation to provide better and otherwise unavailable security products and services. Thanks to specialisation and economies of scale, smaller organisations and non-experts can improve their security by relying on specialised outlets with more experience, expertise and skill. For example, most organisations would see security increase when moving their email to a hosted solution by Google or Microsoft, or by relying on specialist authentication providers like Duo. The security of key components, like operating systems, has also improved considerably in recent years.

This does not mean it is impossible for small organisations to run secure systems. Rather, relying on outside expertise is likely to yield better results because specialists can provide a niche product or service to multiple customers at an individually lower cost. This optimisation of security cost/benefit ratios occurs at all levels: NATO's militaries and multinational firms do not provide all IT services internally or build all their equipment themselves; like other organisations, they acquire resources from specialists (defense.gov, 2020).

While this specialist-led approach can reduce vulnerabilities per product or service, it increases networked complexity and dependencies. When connecting to and relying on immense numbers of providers, systems and hardware/software stacks, the universe of cases, including the potential states, situations, dependencies, interactions, attack vectors, vulnerabilities and risks grows immensely. It is common practice in research and analysis to limit the inquiry to a manageable number of cases and variables (Nielsen, 2016). However, in our networked world, it becomes difficult organisationally and technically to retain security perimeters, to track what is needed to run processes, or to identify which of the many relationships or data flows are legitimate (Vijayan, 2013). For example, organisations often struggle to block malware and phishing sites hosted on large, legitimate cloud services, as these services see sufficient use to be allow-listed (Nelson, 2016).

The 'seams', that is the interactions between systems rather than individual systems themselves, are a key security concern when connecting organisations (Schneier, 2003). Organisations often cannot interface easily because they have divergent needs and processes; in effect, they speak different languages. Furthermore, seeing the interface between two organisations as a dyadic relationship is oversimplified. Different, potentially insecure, social and technical systems might have to be tied together to acquire the required resources. For national cyber security, these issues are exacerbated: networked complexity increases exponentially with the width of our analysis parameters, creating emergent properties and hard-to-trace dependencies and interactions.

Complex systems can produce both complex and non-complex errors. The latter are consistent, while the former is indeterminate or emergent. It is extremely difficult to test complex entities exhaustively, particularly under networked conditions where interactions affect how vulnerabilities present themselves. Complex vulnerabilities in hardware and software may only arise in outlying cases and be triggered only by specific circumstances and can thus remain undiscovered for years. The Heartbleed vulnerability in OpenSSL only manifested itself in some versions of the package and was disclosed two years after the implementation of the vulnerable 'heartbeat' feature (Durumeric et al., 2014). More drastically, the Spectre and Meltdown vulnerabilities found in 2018 affected thousands of microprocessors that 'implement out-of-order execution' (Meltdownattack.com, 2020). Spectre and Meltdown remained undetected for many years and had different effects

depending on the affected system—a prime example of how complexity can create security risks.

Complex systems can also create non-complex errors: in the case of the Intel FDIV bug, the affected processors produced errors when dividing numbers (Price, 1995). The bug was discovered within a year and Intel replaced the affected units. The Intel F00F bug from 1997 was also predictable and consistent; certain instructions would cause the CPU to 'hang up'. Software workarounds were created and deployed, resolving the issue (Collins, 1998). The FDIV and F00F errors were non-complex errors in a complex system: they were rather obvious and, most importantly, consistent. Spectre and Meltdown, by contrast, constitute complex errors. Hidden in the complexities of branch prediction and out-of-order execution, these vulnerabilities are less obvious and produce inconsistent outcomes depending on processor type and applications. Currently, it is only possible to harden systems against the exploitation of Spectre; the vulnerability is not fixed (Meltdownattack.com, 2020).

While these bugs and vulnerabilities are predominantly technical in nature, the political economy of security was part of the reason why the Heartbleed vulnerability was overlooked: the OpenSSL project was painfully underfunded and understaffed. Multi-million-dollar companies and essentially the entire internet user base relied on a few volunteers, as John Walsh (2014) outlined:

> OpenSSL … is largely staffed by one full-time developer and a number of part-time volunteer developers. The total labor pool for OpenSSL maybe adds up to two full-time developers. Think about it, OpenSSL only has two people to write, maintain, test and review 500,000 lines of business-critical code. Half of these developers have other things to do.

Complex errors are not only present in cyber security but also appear in other complex systems and across socio-technical divides. The Boeing 737 MAX jets' fatal flaw was also a result of socio-technical networked complexity. The interaction of control systems, sensors, the fuselage design, management pressure, economic incentives, lack of functional regulatory oversight and the culture change created by the Boeing McDonald Douglas merger, all had their inter-related impact on a plane that cost over 300 people their lives (Sgobba, 2019; Herkert et al., 2020).

The examples above demonstrate different complexity-related issues: some errors like the FDIV and F00F are borne out of complex systems but could be identified and addressed easily. Complex systems, however, can also produce complex errors that are situation-specific and hard to predict or fix, as demonstrated by Heartbleed and Spectre/Meltdown. The Heartbleed and the Boeing 737 MAX examples also show how socio-technical interactions can cause literally and metaphorically fatal failures across domains.

Standardisation and strict operating protocols such as in air traffic and railways safety and control have long been tools to reduce complexity, counteract emergence and reduce failure rates (Vaughan, 2005; Hutter, 2001). In cyber security, however, this approach of codifying behaviour, unifying equipment and separating duties is less effective and therefore not the focus of this paper. First, computer and social systems diverge to an extent that makes complete standardisation impossible. Second, safety has very different objectives than security. Third, safety deals with trained, benevolent professionals rather than creative, malicious adversaries.

Security must also be analysed differently, specifically covering socio-technical networks, as evidenced by the DNC hack. Political parties and their leadership are at risk because they are closely tied to the core institutions of democracy, fundamental governance and societal aspects of most NATO members. Compromising a political party's leadership can disrupt the heart of a country's political system. Adversaries do not have to change election results. Sowing distrust and suspicion can be enough to blemish the central democratic institution in popular perceptions. Thus, less direct and more clandestine and socially-focused operations are an important vector to study (Hansen & Lim, 2019). Generally speaking, the old perimeter logic hardly applies anymore: compromises through others, be they employees' private devices or business partners' systems, are likely, particularly when dedicated adversaries—state or otherwise—are involved.

4. POLICY, TREATMENTS AND SOLUTIONS

For NATO countries and other open societies, networked complexity means that weaknesses within and attacks via the cyber realm are hard to analyse and predict. National and international interdependencies are so numerous and intricate that tracing and treating all security-relevant dependencies, attack paths and resulting risks is unrealistic. Adversaries, criminal and state-sponsored, have manifold options to compromise, disturb or otherwise undermine technical and social processes and key institutions. This section proposes solutions to reduce the attack surface and mitigate security issues borne out of interdependence and complexity.

While no one can eliminate the risk inherent in linking with other organisations or in running complex organisations and systems, mitigation is workable and can be effective. Security management measures can avoid or reduce the risk of an adverse event or incident taking place, or alleviate its detrimental impacts. The goal for organisations and governments should not be to create perfect security systems but instead to make compromising systems harder for adversaries to infiltrate and attack at every stage.

A. Security Management

The challenge of interlinked systems and complex dependencies calls for

more attention than currently warranted. Information security risk management processes have long addressed and dealt with dependencies and different attack paths. With growing complexity, however, existing methodologies, registers and models are more difficult to deploy and thus more expensive and failure-prone.

Now more than ever, organisations require numerous sets of niche knowledge and skills working in tandem to address security, which specifically entails technical and non-technical experts. These teams also need considerable time and resources to design, grasp, secure and maintain computer systems in their procedural and organisational contexts (Clarke et al, 2016). More time and effort must be dedicated to holistically analysing potential attack vectors and the security and trustworthiness of partners and suppliers.

In particular, analyses must incorporate socio-technical interactions, not just social or technical levels on their own. While labour-intensive, tracking and categorising ties and dependencies alongside what they entail can inform security policy, strategy and tactics and identify key nodes or ties requiring additional controls. While post-facto security is often less effective than building 'secure by design', the approach still reduces risk and is sometimes unavoidable, particularly when legacy systems are involved.

This holistic approach will be a multi-pronged challenge for many security professionals, who are often technical specialists (Weissinger, 2018). Few have cross-domain expertise, though this is changing. Additionally, non-technical personnel are often considered inferior or irrelevant by those within technical circles (ibid.). Lastly, individual time and bandwidth are limited: security specialists cannot be experts in everything and thus must cooperate and usually are not trained to do so (ibid.).

IT security management literature and standards like the ISO 27000 (2018) family and NIST 800-53 (2020) also underscore the importance of good security and risk management. Unfortunately, aptly implementing these high-level standards requires expertise, time, resources and, most of all, the will to improve security. With audits and certifications, experts often lament the tendency to demote security to 'box-ticking' exercises and the at times circumspect independence of auditors (Weissinger, 2018). Nevertheless, the Payment Card Industry Data Security Standard (PCI DSS) is a good example of useful standard enforcement. Whilst it did not lead to enhanced security everywhere, its mandatory nature did force payment processing companies to take security precautions (Wilson et al., 2018).

Crucially, security management can only reduce, not eliminate, risk (Purser, 2004) and, unfortunately, digitally securing a state is obviously far more elaborate, particularly when societies and economies are diverse, open, interlinked and interdependent (Castells, 1996; Castells, 2000).

B. Using Expertise Securely

Specialist organisations can bring non-specialists up to speed and also pro-

duce security that is of better quality and available more quickly. The greater the number of organisations that rely on them, the more likely it is that key security providers will become sought-after targets. However, shifting responsibility towards specialist providers and manufacturers is rational; very few actors have the ability to adequately address sophisticated threat actors.

To leverage expertise through layering and networks, three conditions must be at least partially met. First, individual components (technical and organisational) need to and need to be forced to, follow security best practices, particularly for components that are essential due to their stack position or layer, such as CPUs and operating systems. Second, ties or interconnections between layers and across networks must be established and maintained securely. Finally, any organisation relying on external providers and manufacturers must strictly monitor those relationships. Thus, we require more efficient and effective methodologies and approaches to assess the trustworthiness of service providers (Weissinger, 2017; Weissinger, 2018).

C. Secure by Design

To manage security risks stemming from increasing complexity and dependency on outside parties, system architects and managers should build towards greater resilience. For critical systems that must not be compromised, the best solutions are often not technical but architectural. For example, France's media blackout prior to its elections helped foil a Russian interference campaign in 2017 (Vilmer, 2018). 'Old-fashioned' low-tech or no-tech safeguards can also be resurrected, like paper trails being used to help secure elections.

To increase resilience across society, components—that is, products and services—must become more secure by default, based on an approach this paper terms 'defence in breadth', in addition to defence in depth. Defence in breadth means that security is designed into products and services, including consumer-oriented ones.

Agencies and key businesses matter profoundly to national security and they in turn are staffed by individuals relying on consumer products. While targeted security improvements are necessary, they are insufficient to fully manage networked security risks. Focusing security efforts only on key government institutions or critical infrastructure—however defined—leaves adversaries with a multitude of easily attackable devices, people and organisations through which they can compromise key targets indirectly. Furthermore, as evidenced by the DNC example, criticality has often been defined in an overly limited manner.

Defence in breadth can be supported by security research similar to Google's 'Project Zero' (2020) that focuses on often-used, essential technologies. More importantly, however, organisations and governments should make security baselines like secure defaults, basic penetration tests, security and data management audits, patching infrastructure and monitoring, manda-

tory across the board.

D. Specific Actions: Organisations
Individual organisations and agencies need to accept that networked complexity and its resulting risks, require managing. Networked complexity is hard to address with 'checkbox compliance' and with checks on building blocks alone. Therefore, socio-technical, network-based analyses must be added to conventional or routine security operations. Proper security management structures must be established. Specifically, individual organisations should trace key networks and create detailed dependency charts (Schostak, 2018; Schostak, 2014; Wheeler, 2011).

Most importantly, best practices like risk management, business continuity and disaster recovery planning should be followed and regularly audited. Particularly, organisations should think about backup solutions in the broadest sense such as planning for security failures in partner organisations.

E. Specific Actions: NATO and Governments
Grappling with the complexity of digital systems will require a division of labour within NATO, across state borders and across the public/private divide. NATO governments are increasingly cooperating and jointly investing in cyber security (Shoorbajee, 2018; CCDCOE, 2018). However, their activity is focussed on sharing capabilities (Freedberg, 2018; Emmott, 2018); active measures (Tucker, 2019); cyber norms; international law (Schmitt, 2017); and military approaches (Efthymiopoulos, 2019), but not overall vulnerability reduction. For that, the 'defence in breadth' approach, which is defensive in nature, is the best means to confront vulnerabilities stemming from complexity in cyberspace and to build cyber resilience globally.

Dealing with networked complexity will require more cooperation with manufacturers, which is underway (NATO CCDCOE, 2020), service providers, anti-abuse actors and groups and also technical standards setting bodies and academic researchers. Incorporating these diverse groups is difficult, and not only due to the number of parties. Likely, this will necessitate the development of new tools and approaches to ensure that such cooperation is balanced, technically grounded and sufficiently removed from daily politics. Experts, be they academics, independent, employed by government or private enterprise—must be remunerated and supported when engaging in standard design at bodies like the IEEE and IETF. Security research must be funded and legal frameworks developed to protect bona fide independent researchers from legal repercussions, including by private actors trying to silence inconvenient facts and findings (Lee, 2020; disclose.io, 2020). Only by leveraging this combined expertise will it be possible for states to keep up with developments in computing and cyber security.

NATO and Western governments should also increase their activities against key enablers in cyberspace. These include payment processors that work

with criminals (Levchenko et al., 2011), domain registrars that allow attackers to register domain names and 'bulletproof' hosts that specialise in keeping online malicious sites. Such critical nodes can be identified and regulated by state actors through their enforcement capabilities.

Some companies and manufacturers care about their system and data security; others fail to demonstrate due care and diligence. Due to the network effects of globalisation, an individual organisation's vulnerability can harm many others. Therefore, governments must legally enforce better security practices across the board, which does not entail simply banning foreign companies. Instead, states should require baseline security testing, features and management. States must empower experts, rather than the political apparatus, to create standards, requirements and rules. While political oversight is useful, states should primarily fill the role of the enforcer. The cyber security space is complex and solutions require considerable expertise, often garnered through many years of hands-on experience or research.

While legally forcing security baseline requirements on all devices will complicate some intelligence and law enforcement activity, the risk of catastrophic attacks on critical infrastructure and institutions is too great to not pursue this avenue. Unless states and organisations tighten security in breadth, adversaries will find spaces to stage attacks, gather intelligence, host facilitating tools and worse. However, with security in breadth, potential attackers' costs go up, reducing the number of successful attacks.

5. CONCLUSION

This paper discussed the nature of networked complexity and how it affects security both inside and outside cyberspace. As everything is connected, hardening only those systems deemed critical is insufficient for three reasons. First, current heuristics often miss key attack paths because they fail to recognise important relationships. Second, information security entails computer systems and organisations and their functions—an established but nevertheless often ignored fact. By focusing on complex interdependencies, aspects previously deemed uncritical come to the fore: consumer devices, consumer networking equipment and, crucially, social processes. Third, due to the use of contemporary trends like cloud technologies and increasing specialisation, analysing graphs of interlinked systems and resulting risks is especially pertinent.

It is impossible organisationally or nationally to fully compensate for the security risks associated with complexity. However, by tracing dependencies and relationships, analysing potential attack paths and adapting architectures and security strategies, tactics and operations to a networked environment, organisations and governments can raise the bar when it comes to security. Many of these steps will not be technical in nature but organisational, procedural or architectural. Useful tools are already available in the security and security management spaces that can address the outlined complexity

problems, at least to some extent.

Unfortunately, states likely have to enforce better security for vendors and service providers to protect national assets and critical systems. Without state pressure, it is improbable that sufficient numbers of key actors will sufficiently address security. While it may be slightly detrimental to intelligence and law enforcement activities, the best defence for organic societies like those in NATO states remains security in breadth, in addition to hardening key systems. This means establishing a high level of security throughout, from state intelligence systems through to consumer devices. This approach would obstruct future adversarial operations that try to leverage weaknesses in peripheral or non-hardened systems to attack core or critical systems or infrastructure.

6. REFERENCES

Castells, M. (1996) *The Information Age: Economy, Society and Culture*. Cambridge, MA, Blackwell.

Castells, M. (2000) Materials for an exploratory theory of the network society. *British Journal of Sociology*. 51 (1), 5–24.

Castells, M. (2001) Identity and Change in the Network Society. *Interview with Harry Kreisler*. Available from: http://globetrotter.berkeley.edu/people/Castells/castells-con4.html. [Accessed 4th September 2020].

Clarke, P., O'Connor, R. V. & Leavy, B. (2016) A complexity theory viewpoint on the software development process and situational context. In: Perry D.E. and Raffo, R. (eds.) *ICSSP '16: Proceedings of the International Conference on Software and Systems Process. Proceedings of the International Conference on Software and Systems Process 14-15 May 2016, Austin, Texas.* Association for Computing Machinery. pp. 86–90. Available from doi: 10.1145/2904354.2904369.

Collins, R. (1998) The Pentium F00F Bug. *Dr. Dobbs*. 1st May 1998. Available from: https://www.drdobbs.com/embedded-systems/the-pentium-f00f-bug/184410555. [Accessed 15th June 2020].

Connolly, L.Y. & Wall, D.S. (2019) The rise of crypto-ransomware in a changing cyber crime landscape: Taxonomising countermeasures. *Computers & Security.* 87 (101568). Available from: http://www.sciencedirect.com/science/article/pii/S0167404819301336.

Cyber Risk International (2020) *Cyber Threats to the Agriculture Sector.* 7th April 2020. Available from: https://cyber riskinternational.com/2020/04/07/cyber threats-to-the-agriculture-sector/. [Accessed 17th May 2020].

Dally, W. J., Turakhia, Y & Han, S. (2020) Domain-Specific Hardware Accelerators. *Communications of the ACM.* 63 (7), 48-57. Available from: https://cacm.acm.org/magazines/2020/7/245701-domain-specific-hardware-accelerators/fulltext.

defense.gov (2020) *DOD Reaffirms Original JEDI Cloud Award to Microsoft*. 4th September 2020. Available from: https://www.defense.gov/Newsroom/Releases/Release/Article/2337557/dod-reaffirms-original-jedi-cloud-award-to-microsoft/. [Accessed 1st September 2020].

disclose.io (2020) *Response to Voatz's Supreme Court Amicus Brief*. 14th September

2020. Available from: https://disclose.io/voatz-response-letter/. [Accessed 16th September 2020].

Durkheim, E. (1984) *The Division of Labour in Society*. New edition. Basingstoke, Palgrave Macmillan.

Durumeric, Z., Li, F., Kasten, J., Amann, J., Beekman, J. G., Payer, M., Weaver, N. C., Adrian, D., Paxson, V., Bailey, M. D. & Halderman, J. A. (2014) The matter of heartbleed. In: Williamson, C., Akella, A. and Taft, N. (eds.) *IMC 2014: Proceedings of the 2014 Internet Measurement Conference, 5-7 November 2014, Vancouver, Canada.* Association for Computing Machinery. pp. 475-488.

Eddy, M. (2019) Want to Hack a Satellite? It Might Be Easier Than You Think. *PC Mag*. 7th March 2019. Available from: https://uk.pcmag.com/news/119996/want-to-hack-a-satellite-it-might-be-easier-than-you-think. [Accessed 5th December 2019].

Efthymiopoulos, M. (2019) A cyber security framework for development, defense and innovation at NATO. *Journal of Innovation and Entrepreneurship*. 8 (12). Available from: doi:10.1186/s13731-019-0105-z.

Emmott, R. (2018) NATO cyber command to be fully operational in 2023. *Reuters*. 16th October 2018. Available from: https://www.reuters.com/article/us-nato-cyber-idUSKCN1MQ1Z9. [Accessed 15th September 2020].

Evans, D. (2011) The Internet of Things: How the Next Evolution of the Internet Is Changing Everything. *CISCO White Paper*. April 2011. Available form: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. [Accessed 5th March 2019].

Fathi, B. (2018) What Really Happened with Vista: An Insider's Retrospective. *Medium*. 3rd January 2018. Available from: https://medium.com/@benbob/what-really-happened-with-vista-an-insiders-retrospective-f713ee77c239. [Accessed 3rd May 2020].

Freedberg, S. (2018) NATO To 'Integrate' Offensive Cyber by Members. *Breaking Defense*. 16th November 2018. Available from: https://breakingdefense.com/2018/11/nato-will-integrate-offensive-cyber by-member-states/. [Accessed 14th September 2020].

Gillis, T. (2016) Complexity is the enemy of security. *Network World*. 8th August 2016. Available from: https://www.networkworld.com/article/3103474/complexity-is-the-enemy-of-security.html. [Accessed 5th November 2017].

Goldstein, J. (2011) Emergence in Complex Systems. In: Allen, P., Maguire, S. & McKelvey, B. (eds.) *The SAGE Handbook of Complexity and Management*. London, Sage. pp. 65-78.

Google Project Zero (2020) *About Project Zero*. Available from: https://googleprojectzero.blogspot.com/p/about-project-zero.html. [Accessed 4th July 2020].

Gilli, A. & Gilli, M. (2019) Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage. *International Security*. 43(2), 141-189.

Greenberg, A. (2014) Meet 'Project Zero,' Google's Secret Team of Bug-Hunting Hackers. *Wired*. 15th July 2014. Available from: https://www.wired.com/2014/07/google-project-zero/. [Accessed 29th April 2018].

Gubbi, J., Buyya, R., Marusic, S. & Palaniswami, M. (2013) Internet of Things (IoT): A vision, architectural elements and future directions. *Future Generation Computer Systems*. 29 (7), 1645–1660. Available from: https://www.sciencedirect.com/science/article/abs/pii/S0167739X13000241?via%3Dihub.

Hansen, I. & Lim, D.J. (2019) Doxing democracy: influencing elections via cyber voter interference. *Contemporary Politics*. 25 (2), 150-171.

Hirsch, P., Fiss, P. C. & Hoel-Green, A. (2009) A Durkheimian approach to globalisation. In: Adler, P. (eds.) *The Oxford Handbook of Sociology and Organisation Studies*. Oxford, Oxford University Press. pp. 223-245.

Herkert, J., Borenstein, J. & Miller, K. (2020) The Boeing 737 MAX: Lessons for Engineering Ethics. *Science and Engineering Ethics*. Available from: doi:10.1007/s11948-020-00252-y.

Hutter, B. (2001) *Regulation and Risk: Occupational Health and Safety on the Railways.* Oxford, Oxford University Press.

International Standards Organisation (2018) *ISO/IEC 27000:2018 Information technology. Security techniques. Information security management systems. Overview and vocabulary.* Available from: https://www.iso.org/standard/73906.html. [Accessed 25th November 2020].

Jeangène Vilmer, J.B. (2018) Successfully Countering Russian Electoral Interference. *CSIS Briefs*. June 2018. Available from: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180621_Vilmer_Countering_russiam_electoral_influence.pdf [Accessed 5th July 2020].

Kernighan, B.W. & Pike, R. (1984) *The Unix Programming Environment.* Upper Saddle River, Prentice Hall.

Kliem, R. (2004) Managing the Risks of Offshore in Development Projects. *EDPACS.* 32 (4), 12-20. Available from: Doi:10.1201/1079/44633.32.4.20041001/83712.2.

Krugman, P. (1980) Scale Economies, Product Differentiation and the Pattern of Trade. *The American Economic Review*, 70 (5), 950-959. Available from http://www.jstor.org/stable/1805774.

Krugman, P (1981) Intraindustry Specialisation and the Gains from Trade. *Journal of Political Economy*. 89 (5), 959–973. Available from: https://www.journals.uchicago.edu/doi/10.1086/261015.

Lee, T. (2020) Online voting vendor Voatz urges Supreme Court to limit security research. *Ars Technica*. 8th September 2020. Available from: https://arstechnica.com/tech-policy/2020/09/online-voting-vendor-voatz-urges-supreme-court-to-limit-security-research/. [Accessed 12th September 2020].

Levchenko, K., Pitsillidis, A., Chachra, N., Enright, B., Felegyhazi, M., Grier, C., Halvorson, T., Kanich, C., Kreibich, C., Liu, H., McCoy, D., Weaver, N., Paxson, V., Voelker, G. M. & Savage, S. (2011) Click Trajectories: End-to-End Analysis of the Spam Value Chain. *Proceedings of the IEEE Symposium on Security and Privacy, 22-25 May 2011, Oakland, California.* Institute of Electrical and Electronics Engineers. pp. 431-446.

Mahutga, M. C. (2012) When do value chains go global? A theory of the spatialisation of global value chains. *Global Networks*, 12 (1), 1-21.

MariaDB Foundation (2020) *About*. Available from: https://mariadb.org/about/. [Accessed 14th August 2020].

Mathews, L. (2017) NotPetya ransomware attack cost shipping giant Maersk over $200 million. *Forbes Magazine*. 16th August 2017. Available from: https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/ [Accessed 3rd February 2018].

Meltdownattack.com (2020) *About.* Available from: https://meltdownattack.com/.

[Accessed 5th May 2020].

Meola, A. (2020) Smart Farming in 2020: How IoT sensors are creating a more efficient precision agriculture industry. *Business Insider*. Available from: https://www.businessinsider.com/smart-farming-iot-agriculture. [Accessed 28th November 2020].

Nakashima, E. (2016) Russian government hackers penetrated DNC, stole opposition research on Trump. *The Washington Post*. 16th June 2016. Available from: https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html [Accessed 28th November 2020].

National Institute of Food and Agriculture (2020) *Agriculture Technology*. Available from: https://nifa.usda.gov/topic/agriculture-technology [Accessed 3rd September 2020].

National Information Technology Laboratory (2020) *NIST 800-53. Revision 5. Security and Privacy Controls for Information Systems and Organizations.* September 2020. Available from: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

NATO CCDCOE. (2018) *Japan to Join the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn*. Available from: https://www.ccdcoe.org/news/2018/japan-to-join-the-nato-cooperative-cyber defence-centre-of-excellence-in-tallinn/. [Accessed 12th September 2020].

NATO CCDCOE (2020) *Siemens and NATO CCDCOE advance cooperation on cyber security for critical infrastructure*. Available from: https://ccdcoe.org/news/2020/siemens-and-nato-ccdcoe-advance-cooperation-on-cyber security-for-critical-infrastructure/. [Accessed 20th September 2020].

Nelson, P. (2016) Major cloud is infested with malware, researchers say. *Network World*. 10th November 2016. Available from: https://www.networkworld.com/article/3137260/major-cloud-is-infested-with-malware-researchers-say.html. [Accessed 28th March 2018].

Nielsen, R.A. (2016) Case Selection via Matching. *Sociological Methods & Research*. 45 (3), 569-597. Available from: https://www.mit.edu/~rnielsen/Case%20Selection%20via%20Matching.pdf.

Price, D. (1995) Pentium FDIV flaw-lessons learned. *IEEE Micro*.15 (2), 86-88. Available from: https://ieeexplore.ieee.org/abstract/document/372360.

Popper, K. (2013) *The Open Society and Its Enemies*. Princeton, Princeton University Press.

Purser, S. (2004) Improving the ROI of the security management process. *Computers & Security*. 23 (7), 542-546. Available from: http://www.sciencedirect.com/science/article/pii/S0167404804002329.

Schelling, T. (2006) *Micro Motives and Macro Behavior*. 1st edition. New York, Norton.

Schmitt, N. (ed) (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge, Cambridge University Press.

Schneier, B. (2002) The Case for Outsourcing Security. *Computer.org.* April 2002. Available from: https://www.computer.org/csdl/magazine/co/2002/04/r4s20/13rRUxNmPJg. [Accessed 24th July 2018].

Schneier, B. (2003) *Beyond Fear: Thinking Sensibly about Security in an Uncertain World.* Göttingen, Copernicus Books.

Schostack, A. (2014) *Threat Modeling: Designing for Security*. New York, Wiley.

Schostack, A. (2018) *Threat Modeling: What, Why and How?* MISTI Institute. 3rd July 2018. Available from: https://misti.com/infosec-insider/threat-modeling-what-why-and-how. [Accessed 20th January 2020].

Shimpi, A.L. (2012) The iPhone 5's A6 SoC: Not A15 or A9, a Custom Apple Core Instead. *AnandTech*. 15th September 2012. Available from: https://www.anandtech.com/show/6292/iphone-5-a6-not-a15-custom-core. [Accessed 14th September 2020].

Shoorbajee, Z. (2018) Australia and Portugal join NATO cyber cooperative. *Cyber scoop*. 23th April 2018. Available from: https://www.cyber scoop.com/australia-portugal-nato-ccdcoe/. [Accessed 16th September 2020].

Singh, J., Pasquier, T., Bacon, J., Ko, H. & Eyers, D. (2015) Twenty Cloud Security Considerations for Supporting the Internet of Things. *IEEE Internet of Things Journal*. 3 (3), 269 - 284. Available from: doi:10.1109%2FJIOT.2015.2460333.

Taub, A. (2016) D.N.C. Hack Raises a Frightening Question: What's Next? *The New York Times*. 29th July 2016. Available from: http://static.cs.brown.edu/people/jsavage/VotingProject/2016_07_29_NYT_What'sNextAfterDNCHack.pdf. [Accessed 17 September 2020].

Tucker, P. (2019) NATO Getting More Aggressive on Offensive Cyber. *Defense One*. 24th May 2016. Available from: https://www.defenseone.com/technology/2019/05/nato-getting-more-aggressive-offensive-cyber /157270/. [Accessed 8th October 2019].

Vaughan, D. (1996) *The Challenger Launch Decision: Risky Technology, Culture and Deviance at NASA*. Chicago, University of Chicago Press.

Vaughan, D. (2005) Organisational rituals of risk and error. In: Hutter, B. and Power, M. (eds.) *Organisational Encounters with Risk*. Cambridge, Cambridge University Press. pp. 33-66.

Vijayan, J. (2013) Attackers turning to legit cloud services firms to plant malware. *Computer World*. 2nd August 2013. Available from: https://www.computerworld.com/article/2484596/attackers-turning-to-legit-cloud-services-firms-to-plant-malware.html. [Accessed 5th February 2020].

Walsh, J. (2014) *Free Can Make You Bleed*. Available from: http://security.grc-daily.com/dsp_getFeaturesDetails.cfm?CID=3482. [Accessed 20th September 2017].

Weissinger, L. B. (2017) Modelling Trust and Trust-Building Among IT-Security Professionals. *Lecture Notes in Computer Science*. 10292, 557–566. Available from: doi:10. 1007/978-3-319-58460-7_39.

Weissinger, L. B. (2018) *Assessment, Trust, and Cooperation in IT-Security*. PhD thesis. University of Oxford.

Wheeler, E. (2011) *Security Risk Management*. Amsterdam, Elsevier Science.

Wilson, D., Roman, E. & Beierly, I. (2018) PCI DSS and card brands: Standards, compliance and enforcement. *Cyber Security: A Peer-Reviewed Journal*. 2 (1), 73-82. Available from: https://www.ingentaconnect.com/content/hsp/jcs/2018/00000002/00000001/art00009.