BASC WORKING PAPER SERIES

A COMPREHENSIVE CYBER SECURITY APPROACH: BOLSTERING CYBERSECURITY CAPACITY THROUGH INDUSTRIAL POLICY

Melissa K. Griffith

Working Paper 2018-07

BERKELEY APEC STUDY CENTER
552 Barrows Hall
University of California
Berkeley, California 94720-1950
September 2018

This paper is part of a project "Comparative Industrial Policy in the Cyber Security Industry: Policies, Drivers, and International Implications," organized by Vinod K. Aggarwal and Andrew Reddie of the Berkeley APEC Study Center and funded by the Center for Long-Term Cybersecurity at the University of California, Berkeley. This research has been supported by Elinkeinoelämän Tutkimuslaitos (ETLA - The Research Institute of the Finnish Economy) and the Center for Long-Term Cybersecurity (CLTC) at the University of California, Berkeley. Thanks go to ETLA for hosting me in Helsinki, Finland as a Visiting Research Fellow in 2017/2018 and for providing feedback on this project. Thank you to Vinod Aggarwal, Andrew Reddie, and the Berkeley APEC Study Center (BASC) at the University of California, Berkeley for organizing this paper series and providing feedback throughout the process. Finally, special thanks go to the many individuals who met with me to be interviewed on Finland's cybersecurity policies and practices. Their insights were invaluable.

A Comprehensive Security Approach:
Bolstering Cybersecurity Capacity through Industrial Policy
Melissa K. Griffith
BASC Working Paper 2018-07

Abstract:

Finland, at the easternmost border of the European Union (EU), has set itself apart as a global leader in cybersecurity technology. However, there is a distinction between the presence of technical expertise and the effective deployment of that technology throughout industry, government, and the broader civilian population. This broader deployment is essential because for advanced industrial economies, the ability to protect and defend their use of cyberspace is just as vital to a flourishing economy as it is to mounting an effective national defence. How has Finland leveraged existing cybersecurity expertise in a manner that protects both civilian and government use of cyberspace? The government has approached this task by utilizing an existing logic for market intervention: Finland's geopolitical position and its corresponding defence doctrine's emphasis on defence of society by maintaining society-wide resilience in the event of a crisis. In comprehensive security (*kokonaisturvallisuus*), which includes cybersecurity, the responsibility for and the safeguarding of the vital functions of society are jointly held by private and public actors, industry and government, defence forces and citizens. Given this focus on industry and civil society's role within the provision of security, Finland's approach is well suited to the realities of addressing cybersecurity.

Keywords:

cybersecurity, Finland, comprehensive security, national defence strategy, industrial policy, marketcraft

Melissa K. Griffith[1]
University of California, Berkeley
Department of Political Science
210 Barrows Hall
Berkeley, CA 94720
Melissa.k.griffith@berkeley.edu

[1]Melissa K. Griffith is a Ph.D Candidate at the University of California, Berkeley. She specializes in international relation, foreign policy, security studies, and cybersecurity. Melissa has presented her work for the World Affairs Council and the Research Institute on the Finnish Economy (ETLA) where she is currently a research fellow. Melissa holds a B.A. in International Relations from Agnes Scott College and a M.A. in Political Science from the University of California, Berkeley.

1. Introduction

The 21st Century is underpinned by cyber technology. Today, everything from commerce to critical infrastructure to the military 'operate on what has become a globalized network of networks' (Singer and Friedman 2014, 2). For advanced industrial economies, the ability to protect and defend their use of cyberspace is just as vital to a flourishing economy as it is to mounting an effective national defence.

Finland, at the easternmost border of the European Union (EU), has set itself apart as a global leader in cybersecurity technology. It boasts a strong and diverse set of cybersecurity players and consistently places near the top of global and EU rankings on various aspects of cybersecurity competency and capacity. Given Finland's relative technical strength in this space, the question for Finland has now became, 'how can we leverage this existing capacity and competency into society writ-large in a manner that protects both civilian and government use of cyberspace'?

The government has approached this task by leveraging an existing logic for intervention: Finland's geopolitical position and its corresponding defence doctrine's emphasis on defence of society by maintaining society-wide resilience in the event of a crisis. Finland's concept of comprehensive security (*kokonaisturvallisuus*) is animated by a systems-based approach, which emphasizes the importance of interdependencies between individuals, firms, industries, universities, research organizations, and government ministries in achieving security. In comprehensive security, as in the sub-category of cybersecurity, the responsibility for and the safeguarding of the vital functions of society are jointly held by private and public actors, industry and government, defence forces and citizens.

Early cybersecurity interventions have mirrored this systems-based approach focusing on cooperation between various ministries, between public and private actors, and between private and private actors. The end result is a web of overlapping clusters tasked with specific responsibilities and characterized by deep and frequent information sharing, training and exercises, and coordination of operations during and after times of crisis. Therefore, for Finland, cybersecurity, like its parent category of comprehensive security, is based on a concept centred on maintaining critical resilience in and defence of society. Given this focus on civil society's role for the provision of security and the recognition that threats do not need to be military in nature to cause significant harm to and impose high costs on broader society, Finland's comprehensive security approach is well suited to the realities of addressing cybersecurity.

This paper proceeds in four parts. First, I provide an overview of the existing cybersecurity ecosystem within Finland with an eye toward existing competency and capabilities. Second, I introduce the motivation for government cybersecurity intervention: the need, given the existing threat space, to bridge technical cybersecurity expertise and Finland's conceptualization of cybersecurity as 'ensuring the security and functioning of society'. Third, I analyse the character of comprehensive security and how it has shaped cybersecurity policy interventions in Finland. This section includes an analysis of the role of the EU's policy interventions within this framework of comprehensive security as well as reference to Carman and Harris' typology of state industrial policy (1984). Finally, I conclude with a discussion of persisting areas of concern and the particular strengths of the Finnish system in meeting those challenges.

2. The Character of Finnish Cybersecurity Expertise and Competency

Market interventions are rooted in the assumption that some activity or provision of goods is both desirable and absent from the existing market ecosystem.[2] Therefore, before we can discuss the motivations behind Finland's intervention in markets to bolster cybersecurity competency and capability, it is important to first examine the depth and breadth of Finland's current cybersecurity ecosystem. Notably, this ecosystem is simultaneously an outcome of previous government interventions in various forms and the foundation upon which current cybersecurity policies and interventions rest.

What is the character of Finland's current cybersecurity ecosystem? The short answer is that Finland is a global leader in cybersecurity technology. More specifically, Finland has a relatively vibrant security ecosystem in terms of the range of firms and the expertise they bring to bear. Finnish expertise has been recognized globally and remains deeply embedded within its broader expertise in ICT and the broader technology industry.

Despite being a relatively small country, Finland boasts a strong and diverse set of cybersecurity players including dedicated cybersecurity companies such as F-Secure (formerly Data Fellows), SSH Communications, and Stonesoft (acquired by Intel in 2011); cybersecurity consulting companies such as Nixu and Trusteq (acquired by KPMG in 2015); and dominant industry players with a strong cybersecurity research and competency components such as Nokia and Bittium.[3] Finnish cybersecurity providers have been recognized for their strength in a wide range of tools including antivirus, anti-malware, firewalls, cryptography, and security testing. Dominant industry players such as Bittium and Nokia have likewise provided secure telecommunications networks and devices, wireless networks, health service platforms, automobile manufacturing, IoT and wearables, etc. to both the Finnish government and the broader civilian population.

This is not to overlook the significance of American dominance in cybersecurity and the information technology industry more broadly. The North American market, primarily driven by the United States (US), comprises over half of global spending on cybersecurity (Cybersecurity Ventures 2016) and more broadly, the Big Five tech giants (Alphabet, Amazon, Apple, Facebook, and Microsoft) are all American companies.[4] These are two realities not overlooked by the Finns or the EU.

However, while Finland has its share of multinational subsidiaries, the domestic security ecosystem remains relatively large, particularly in relation to its population and market size. In

---

[2] See Aggarwal and Reddie's "Comparative Industrial Policy and Cybersecurity: A Framework for Analysis" in this special issue for a discussion of the literature on market failures and motivations for interventions within the discipline of Political Science.

[3] Nokia maintained a research group for cybersecurity until 2010 and was a dominate player in the Finnish cybersecurity market in terms of the scope of research produced, cybersecurity patents held, and in the provision of secure telecommunications networks and devices. For more information on Nokia's position within the broader cybersecurity ecosystem in Finland, refer to Pelkonen, Savola, and Salonen (2017).

[4] For a more detailed analysis of the American ecosystem and corresponding industrial policies see Aggarwal and Reddie's "Iterative Industrial Policy: How the United States Pursues Cybersecurity" in this special issue.

the security space, Finland has a reasonable balance domestically given the presence of industrial companies, domestic champions that compete at scale in Europe and beyond, a variety of Small and Medium Size Enterprises (SMEs), and start-ups. In some infrastructure spaces, local players resoundingly dominate. Take telecommunications as an example. Nokia and Sonera (the Finnish arm of the Swedish Telia Company) lead the Finnish market and seek to maintain this edge as leaders in 5G research and development (Soesanto 2017; Nokia 2016).

Finnish technical cybersecurity expertise has also been recognized and leveraged beyond the domestic market. Finnish expertise has been raised in conversations focusing on potential Finnish added value to EU projects such as Industry 4.0 and broader efforts to secure the Single Market. Similarly, companies like Novasano, an American healthcare company, have opened operations in Finland due in large part to world class expertise in product development including 'data privacy management, cyber security threat prevention, reliable infrastructure and identity management' (Invest in Finland, 2017).

Finland has also maintained high rankings on a variety of external cybersecurity assessments. For example, last year Finland ranked in the top tier of countries - termed "leaders" - due to their commitment to cybersecurity (International Telecommunication Union 2017). Also in 2017, Finland was acknowledged as the most cyber secure country in the EU (with a focus on vulnerability to cybercrime), beating Estonia for the top spot (Website Builder Expert 2017). Several years earlier in 2012, Finland outranked states such as France, Germany, the United Kingdom (UK), and the United States (US) to find itself in the top tier for computer security alongside Israel and Sweden (Blitz 2012) and in 2013 Finland ranked in the top 5 in terms of balancing economic growth and national security needs through cyber readiness (Hathaway 2013).

Paradoxically, world class technological expertise coupled with high rates of connectivity have led to a unique flavour of cybersecurity procurement within private companies in Finland. Like many of its fellow Scandinavian countries, Finland has been both a frontrunner in high levels of Internet connectivity for its general population but also in government and public services. Given the abundance of security providers as well as the challenges of maintaining in-house teams for such broad swathes of government and industry, many Finnish companies have chosen to outsource their cybersecurity needs (Haaramo 2018). Uniquely, however, Finnish companies often have the technical aspects already in place when seeking out cybersecurity services. This means that firms, like CGI's Nordic Cyber Security Centre, frequently split the provision of technical and operational security in Finland and provide the latter more than the former (Haaramo 2015).

Looking more broadly, cybersecurity expertise is embedded within one of three sectors of the Finnish economy: information and communications technology (ICT), a sector which is partially the result of market-oriented government policies. As a relatively small country with limited resources, Finnish market-oriented policies have long had a component of active industrial intervention.[5] It found success in 'riding the wave' (Ali-Yrkkö et al. 2017) of globalization through employing specific marketcraft (i.e. broad market interventions defined by Vogel as

[5] The most recent internal devaluation is just one example. In this instance, the government struck a deal with labour to spur economic growth. For additional information refer to Forsell and Rosendahl (2016).

'how and why governments make markets work' (2018, 1) through a 'range of market-oriented policy action' (2018, 138)). By the late 20th and early 21st century, this marketcraft had resulted in an export-led, knowledge-based economy comprised of three broad sectors (the ICT industry, the technology industry (minus ICT), and the forestry industry) ((Ali-Yrkkö et al. 2017). The structures that made this transformation possible – emphasis on innovation and knowledge as a competitive asset, high levels of general education, strong informal and formal networks between a wide range of actors, and resistance to protectionism - have been leveraged to develop and sustain a thriving ecosystem of cybersecurity innovation and expertise in Finland. Therefore, the existing cybersecurity ecosystem is simultaneously an outcome of previous government interventions in various forms and a foundation upon which current cybersecurity policies and interventions rest.

In conclusion, via numerous metrics, Finland is among the leaders of the cybersecurity pack. It maintains a strong ICT sector and boasts a diverse ecosystem of cybersecurity players and capabilities. However, simply because Finland remains at the forefront of cybersecurity technology does not mean that it does not face significant challenges to maintaining and further developing cyber resiliency and security. The remainder of this paper proceeds in three parts. The next two sections address motivations for and government intervention in this space while the final section offers concluding thoughts and identifies remaining areas of concern and potential future development.

3. Motivations for State Intervention

Given Finland's relative strength in cybersecurity technology, why should the state intervene in the market? There is a distinction between the presence of technical expertise and the effective deployment of that technology throughout industry, government, and the broader civilian population. Additionally, having existing expertise is not sufficient for maintaining a technological edge as both the domain (the existing attack surface) and the number and sophistication of digital security threats grows. Finally, it is one thing to maintain a diverse ecosystem of technological expertise and quite another to scale that expertise up into a broader effort toward comprehensive societal security, which necessitates resilient critical infrastructure and services within a country.

Cyberspace, as a domain, is an ever-evolving threat space. With every new line of code or every new Internet of Things (IoT) device, the potential attack surface increases. The IoT global market alone is expected to reach 8.9 trillion USD in 2020 as compared to 2.99 trillion USD in 2014 (Columbus 2017). In addition to the exponential growth of the potential attack surface, there is no reason to believe we have reached a plateau in the proliferation of digital security threats targeting that attack surface. In fact, the opposite is glaringly evident. In its 2018 Internet Security Threat Report, Symantec reported that in 2017 it witnessed a 92% increase in downloader variants of malware, a 54% increase in variants of mobile malware, a 46% increase in ransomware variants, a 600% increase in IoT attacks, and a 29% increase in reported industrial control system (ICS) related vulnerabilities in comparison to the 2016 observed rates (Symantec 2018). Given this evolution, Finland has a vested interest in not only maintaining its

technical edge but also in securing a comparative advantage in emerging areas of technological cybersecurity expertise.

Moreover, cybersecurity is not an end goal in and of itself. Rather, security enables other types of activity while insecurity undermines those activities. Cybersecurity - whether it is being discussed at the level of the individual, the firm, the state, or regional or international organizations - is in its most basic sense about protecting and defending your own use of cyberspace. This was explicitly recognized on the first page of Finland's 2013 Cyber Security Strategy: 'Cyber security means the desired end state in which the cyber domain is reliable and in which its functioning is ensured' (Finland´s Cyber Security Strategy 2013, 13). Economic, social, and government activity rely on and leverage cyberspace for their day to day functioning. Insecurity (whether the goal of an attack is espionage, disruption, or financial gain) can destabilize day to day operations, undermine trust, and result in significant financial and national defence costs.

The far-reaching impact of cyberattacks and insecurity is not merely theoretical. Awareness of this widespread vulnerability has only increased in the past few years. In 2016 alone, we publicly witnessed incidents in numerous critical sectors globally: communication (Deutsche Telecom and Yahoo), democratic institutions (the Democratic National Committee and the Philippines' Commission on Elections), energy (the power grid in Ukraine), financial services (the Central Bank of Bangladesh and Tesco Bank), healthcare (the Australian Red Cross and National Health Service Hospitals in the UK), IT services (domain name provider Dyn), and security (the FBI and Homeland Security in the US) (EPSC Strategic Notes 2017, 2).

With this reality in mind, Finland has set out to 'ensure the security [or functioning] of society' (Finland´s Cyber Security Strategy 2013, 1). For Finland, security of society includes a series of verticals or activities such as 'management of Government affairs, international activity, Finland's defence capability, internal security, functioning of the economy and infrastructure, population's income security and capacity to function, and psychological resilience to crisis' (Finland´s Cyber Security Strategy 2013, 2). In order to maintain critical services and infrastructure resilience, the government hopes to limit single points of failure, contagion, and crises of confidence by building in resilience to systems and seeking to harmonize goals and activity between ministries and an array of relevant private actors. This requires that Finland not only recognize the interdependences between individuals, firms, industries, universities, research organizations, and government ministries but that they explicitly leverage strong private-public networks and levels of trust for cooperation and coordination.

In sum, cybersecurity at the national level has three broad dimensions: technical, operational, and strategic. In the technical space, Finland, as previously discussed, has existing expertise on a wide range of tools and a vested interest in maintaining that edge. At the strategic level, Finland has laid out a vision of cybersecurity centred around ensuring the continued functioning of society in the event of crisis. The specific task remaining then has been the operationalization of this strategy: spreading and applying technological expertise to broad swathes of industry, civil society, and government; information sharing and coordination in response to threats and in determining responsibilities between public and private actors; pooling of resources to stay ahead of the evolving threat landscape, maintaining critical infrastructure and services, etc. In an effort

to build and flesh out this operational space, Finland has relied on a previous and well-established form of government intervention: its comprehensive security approach enshrined in its Security Strategy for Society. This form of security intervention and policy relies on a uniquely Finnish, systems-based approach.

4. Finnish Cybersecurity Intervention: A Comprehensive Security Approach

As a relatively small country bordering a much larger power, Finland's security doctrine has developed out of the following concern: how can a smaller country, which in times of crisis and/or war would in effect be an island, ensure the performance of its economy, society, and defence forces in the face of external, aggressive action? Finland's answer is that to 'safeguard its independence and territorial integrity' (Security Strategy for Society 2017, 18), public and private actors alike can be and often are security actors (turvallisuustoimija), critical in maintaining and providing for the vital functions of society (yhteiskunnan elintärkeä toiminto) in times of crisis. National security, therefore, is directly tied to the interdependencies between different actors as well as the management and harmonization of these various actor's goals and interests.

Embedded within this broader strategic context, the strength of Finnish cybersecurity interventions is grounded in a systems-based approach both to conceptualizing comprehensive security and in operationalizing that vision by targeting government intervention at multiple levels ranging from the national to the municipal. Provision of cybersecurity is inherently challenging because it lies at a series of intersections: the intersection between public and private interests and capabilities, the intersection between economic and security activity, the intersection between internal and external security, the intersection between civil and military responsibility, and often the intersection between war and peace. These characteristics have placed significant strain on states that have sharply delineated responsibility for security to its public sector, and most often its military and intelligence services in conjunction with political elites. Finland, in contrast, has traditionally understood its security to be located within these intersections.

In order to illustrate Finland's comprehensive security approach to industrial cybersecurity policy, this section of the paper proceeds in four parts. First, I preface this analysis with a few caveats. For any research focusing on Finnish policy residing at the intersection of national security and economic activity, there are several important caveats worth discussing. Second, I briefly outline Finland's Security Strategy for Society and the way cybersecurity has been incorporated into this framework. Third, using the typology introduced by Carman and Harris, I highlight how Finland's comprehensive security approach has led to a series of deeply embedded and enmeshed *market modifying*, *market substituting*, and *market facilitating* interventions, which taken together encapsulate the strength of their systems-based industrial cybersecurity policy. This section highlights domestic efforts as well as a selection of efforts enacted at the EU level that have direct impact on the Finnish market.

4.1. Caveats

Before proceeding with an analysis of economic and national defence-based interventions, there are two restraints worth noting for any work focusing on government policy residing at the intersection of security and economic concerns. First, not all cybersecurity policy is made public. Second, not all market interventions are clearly earmarked as cybersecurity specific interventions.

First, there is simultaneously a public and private face to cybersecurity policy. Not all cybersecurity efforts and policies are located in the public domain. Some efforts, such as the Finnish Defense Forces facilitating the cybersecurity market by purchasing specific capabilities and developing others in house, will by necessity fall outside the public domain and be absent from this analysis of Finnish industrial policy. It is worth noting, however, that there may be less activity in the private domain than we might otherwise assume. Marking something confidential can hide both a plan or activity from public sight as well as a lack of plan or activity from public sight. One Finnish interviewee referred to this as classifying an empty box.

The division between privately available and publicly available information is only magnified in the Finnish case. Finnish security policy is centred on the defence of society, ensuring that this defense does not provoke a larger neighboring state (i.e. Russia) which poses both a kinetic threat and economic challenge. This has historically led to a largely quiet and publicly limited set of discussions and security efforts. Finnish officials have pointed publicly to the importance of maintaining good relations with Russia, while also maintaining that this approach is not appeasement since Finland does maintain capabilities for its defence (Standish 2016). This specific emphasis on tailoring public security policy, rhetoric, and posturing in order to not aggravate a particular regional power was also strikingly reflected in interviews. Finns frequently referenced 'potential threats from the East' as shorthand for a consistently unnamed Russia. For Finland, efforts in any security space walk a fine line between publicly and privately addressed issues and concerns.

Second, not all interventions will be separated into cybersecurity buckets. Given Finland's focus on building cybersecurity into all aspects of Finnish life, current Industrial policy targeting the ICT and technology industries more broadly should by design have a cybersecurity element. However, cybersecurity may not be specifically earmarked or publicly delineated within these efforts. Take Finnish *market facilitating* R&D funding through Tekes (now Business Finland) for AI and 5G as one example (Tekes 2017). Neither of these projects are explicitly about building out cybersecurity capability or competency but both technologies have a direct impact on and contain components applicable to cybersecurity.[6] While Finland may very well be effectively folding cybersecurity into each of these industrial policy efforts, the exact financial commitments and/or practical emphasis placed on cybersecurity within each remains largely unseen. In effect, any analysis of industrial cybersecurity policy is likely to miss areas of intervention that should now be, given the emphasis on security by design, occurring as part of any product or service reliant on, connected to, or interacting with cyberspace.

[6] For example, the AI working group contains a contingent of cybersecurity experts from industry, often those found in other cybersecurity initiatives such as CyberTrust.

Given these two caveats, this paper does not portend to offer a comprehensive analysis of all government cybersecurity interventions. Rather it seeks to provide an overview of dominant, publicly observable interventions. These interventions provide an important foundation for future analysis and provide insight into the types of activities that are likely also occurring in tandem behind closed doors. However, they are just that: dominant and publicly observable.

4.2. Integrating Cybersecurity into Finland's Security Strategy for Society

As previously mentioned, Finland has a systems-based view of security policy, as evidenced by its Societal Security Strategies.[7] There are two important insights encapsulated in this concept of comprehensive security. First, as a small country living next to a regional and historically active power, defence of society is a task that requires the mobilization of vast resources. This means that the responsibility for security cannot only be housed within the defence forces alone but also with civilian society being prepared for war even during peace time in order to ensure national survival in times of crisis. Second, threats to national security do not need to be military in nature to be incredibly costly or crippling. Therefore, the crux of comprehensive security is that, regardless of the cause of crisis, private and public actors must ensure and safeguard the continued delivery of certain functions in times of peace so they are resilient in times of conflict.

Comprehensive security planning in Finland is more than just political rhetoric. It includes the identification of specific infrastructure and services vital to resilience in a time of crisis while also detailing operational responsibilities to ensure that resilience ranging from the municipal to the national level for both private and public actors. Finland's most recent Security Strategy for Society identified three broad areas of activity: (1) regular threat and risk assessments that take into account the interdependencies and vulnerabilities within the entire system and not just within a specific sector or organization, (2) crafting and implementing operational guidelines and assigning responsibilities across all sectors and levels of government to be implemented during a crises, and (3) crafting and implementing operational guidelines and assigning responsibilities to be implemented during the aftermath of or recovery period following a crisis (Security Strategy for Society 2017).

One central component of Finland's comprehensive security approach is a focus on maintaining the security of supply (huoltovarmuus), both in terms of essential infrastructure but also in terms of the goods and services they provide. The central organization responsible for coordinating security of supply, the National Emergency Supply Agency (NESA), is a public-private partnership. Charly Salonius-Pasternak, a Senior Research Fellow at the Finnish Institute of International Affairs and former International Affairs Advisor to the Finnish Defence Forces, explains the central role of the NESA in planning crises:

> The National Emergency Supply Agency (NESA) coordinates twenty-one 'planning pools' (examples include the media, healthcare, transport, communications, and so forth) to ensure that different sectors continually update plans, including for the way in which private sector competitors can deliver services through each other's logistics or service networks. In addition to this, NESA oversees through partnerships and contracts reserves

[7] The first societal security strategy was published in 2003, entitled "Strategy for Securing the Functions Vital to Society". This first strategy was followed up three years later in 2006 still using the same name. The name was changed for the third iteration in 2010 to "Security Strategy for Society". "Security Strategy for Society" was also utilized for the latest and fourth iteration released in 2017.

> of energy, foodstuffs, pharmaceuticals and other raw materials. It also plans and pays for redundancy and support arrangements for IT systems, financial services and communications. (2017)

In addition to building models and assigning responsibilities for these "planning pools", the NESA carries out exercises with its array of public and private partners to better assure preparedness in times of crisis.

Finland's Cyber Security Strategy and two subsequent implementation programs have explicitly acknowledged that 'the Cyber Security Strategy does not change the tasks defined in the Security Strategy for Society' (Finland´s Cyber Security Strategy 2013, 20). They have been thought of as a subset of this broader goal. Cybersecurity as an emerging concern, does not fundamentally alter the broad strategy for providing security for its population through a focus on comprehensive security. If anything, it cements the importance of public-private partnerships and a broad range of actors as security actors.

Instead of disrupting the focus on comprehensive security, cybersecurity is integrated with the existing strategic framework. Cyber-attacks are understood as introducing a new set of avenues for crises. Cybersecurity then becomes both a foundational factor underpinning societal security and resilience as well as a specific concern within essential services such as data-communication systems, networks, and services. Consequently, Finnish policy efforts have focused on how to operationalize cybersecurity resilience within these already existing strategic frameworks. The 2013 strategy, for example, pointed to the addition of a new coordinating mechanism to the existing delineation of tasks and assigned responsibilities between the private and public sector. The newly created National Cyber Security Centre Finland (NCSC-FI), located under the Finnish Communications Regulatory Authority (FICORA), was tasked with maintaining cybersecurity situational awareness, assisting relevant authorities, and providing information and guidance Finland´s Cyber Security Strategy 2013, 20). CERT-FI, and its mission to provide solutions for and gather information on information and security threats, was then incorporated within this national information security authority. The Finnish Defence Forces, separately, were tasked to "create a comprehensive cyber defence capability for their statutory tasks" (Finland´s Cyber Security Strategy 2013, 8).

Cybersecurity also made its way into the NESA's robust mandate in a variety of manners (Kauppinen 2015). First, the NESA describes cyber insecurity as a potential cause of disruption in the security of supply and resilience of critical infrastructure and services. Second, the NESA identifies specific cyber intensive industry and services such as data-communication systems, networks, and services as critical infrastructure. Third, the NESA plans and pays for redundancy and support arrangements within the ICT sector, such as IT and communications systems. Fourth, the NESA added the Finnish national computer security incident response team, CERT-FI, as one of the authorities under its framework responsible for maintaining the security of critical infrastructure and services. Fifth, it conducts exercises to simulate potential crises and system-wide responses with clear cybersecurity components, such as those currently run in

cooperation with the Technology Industries of Finland.[8] These exercises are important because the mandate for the defence forces and the government is to protect their own networks, thus leaving the core responsibility for protecting civilian networks to industry itself (NESA 2018).

In conclusion, Finland's approach to comprehensive security including security of supply has led to cooperation between public and private actors that is both deep and daily in character and requires little day to day enforcement. Cybersecurity, as an underlying condition for continued delivery and functioning of other core services and industry as well as an important component of the provision of security of supply, has been readily incorporated into this pre-existing structure. Given the two previously discussed important insights stemming from a concept of comprehensive security, this Finnish approach to national defence is particularly well suited to incorporate cybersecurity given the necessity of civilian industry in obtaining security and the scope and depth of harm cyberattacks can cost on a society without a corresponding deployment of military means.

4.3. Applying Carman and Harris' Typology of Interventions to Comprehensive Security

There are two main ways of assessing the relative strength of Finnish cybersecurity interventions. The first, which was discussed in more detail in the previous section, focused on the adaptability of the comprehensive security model to the realities and requirements of cybersecurity. The second, which will be discussed in more detail in this section, is the manner in which the comprehensive security model integrates a range of market interventions allowing for a systems-based approach to cybersecurity.

Notably, Carmon and Harris' typology seeks to conceptually delineate between the different types of interventions a state can make in their domestic market. While this makes sense if you think about intervention as falling into discrete buckets, it does run up against the Finnish model for intervention in practice, which represents a deliberate effort to view intervention as systemic and systems-oriented rather than broken down into specific types of activities that a state might want to undertake in any given policy space.

With that said, however, taking Carman and Harris' typology as a starting point, there are three particular interventions that they identify which the Finnish model applies the most readily and extensively in its operationalization of comprehensive security. Taken together the interwoven *market modifying*, *market substituting*, and *market facilitating* interventions demonstrate the strength of their systems-based industrial cybersecurity policy. Finnish cybersecurity policy has deployed these three types of market interventions in conjunction with each other at various administrative levels and in a broad array of sectors. As a result, therefore, you can observe each of these categories of market interventions interwoven into the ways that Finland has understood the types of threats it faces and the types of interventions it is willing to pursue in response to those threats.

[8] For example, the current (spring 2018) Chief of Preparedness, Pasi Eronen, at Technology Industries of Finland focuses on the overall cybersecurity posture and preparedness within Finnish industry and works closely with the National Emergency Supply Agency (NESA) to organize national level cybersecurity exercises.

Market Modifying

A significant portion of Finland's approach to security motivated intervention falls into the category of market modifying policies: attempts to change the behaviour of government and industry through statutory requirements, government resolutions, platforms for voluntary cooperation and coordination, and the creation of forums intended to build shared understandings of threats and increase trust between private and public actors. Similarly, EU cybersecurity standard setting and regulatory frameworks deployed with an eye toward harmonizing and strengthening member state capabilities likewise seek to generate outcomes that the market would otherwise not generate.

Despite the reoccurring joke that Finland is a small country and that everyone working in cybersecurity knows each other personally, Finland has put significant effort into building strong networks and trust in order to allow for shared understandings of threats and coordinated action in addressing them. As previously discussed, building coordination and cooperation is a core component of the Societal Security Plans. In their strategic inception, these plans could best be described as market modifying endeavours seeking to alter the behaviour of both private and public actors through an array of statuary requirements, government resolutions, and voluntary participation in established frameworks. It is also a core component of Finland's National Cybersecurity Strategy, which explicitly calls for the creation of an 'efficient collaborative model between the authorities and other actors for the purpose of advancing national cyber security and cyber defence' as its first strategic guideline (Finland´s Cyber Security Strategy 2013, 7).

However, this trend toward market modifying interventions is mirrored through other specific deployments of this comprehensive security model, such as Finland's National Defence Courses. These courses are explicitly designed to 'improve cooperation between different sectors of society and facilitate networking of people working in the various fields of comprehensive security' by bringing together various leaders in industry with political and military elites (NDU 2018). These courses are held at a variety of levels ranging from national to regional. The national-level National Defence Courses are approximately a month in duration, providing ample opportunity for participants to gain a more nuanced understanding of Finland's foreign and security policy and begin to develop shared narratives around the national interest. Although the cybersecurity industry historically was not a common target of these courses, they are being folded into this structure, including the recent addition of a shorter, pilot defence course focusing on cybersecurity. Ultimately, akin to other market modifying efforts, these courses provide an important foundation of trust and lead to strong informal networks between leaders across various sectors of society and government, which leads to greater opportunity and more robust coordination down the line.

A market modifying strategy can also be observed in public private partnerships such as the Finnish Information Security Cluster (FISC), which through its defence working group brings together cybersecurity industry and the defence community. Unlike the traditional defence industry, which has had built up shared vision and trust with government and defence forces over many years of iterated interactions, the cybersecurity industry remained largely outside these networks. In fact, defence industry originally had its own defence motivated cybersecurity

working group, which Pekka Blomberg (a former Chairman of Cyber Defence working group from 2013 to 2017) helped to establish within the Association of Finnish Defence and Aerospace Industries (AFDA) as early as 2010. However, with the creation of FISC in 2012 containing the Finnish Information Security companies which were largely absent from AFDA, the decision was made to merge the FISC defence working group and the AFDA working group. The decision to merge sought to avoid competing structures and to further break down barriers between cybersecurity companies, government, and the defence industry. The merged group was located under the FISC umbrella. Notably, the defence working group was and remains one of the most popular working groups in the cluster in terms of attendance.

FISC, whose membership is comprised of 'companies and organizations that provide nationally important information and cyber security products and services', provides an important avenue for relevant industry and government to further break down barriers and build up coordination in the pursuit of comprehensive security (FISC 2018). Beyond the narrower category of defence, the group focuses on a range of topics formalized into specific working groups, including the three original working groups: the industrial internet, growth, and the aforementioned defence. FISC sought, in part, to form a bedrock of trust and shared understanding in order to facilitate informal and/or voluntary cooperation between industry and government. Notably, FISC membership is comprised of Finnish firms such as Bittium and F-Secure but also many foreign multinationals such as Microsoft and Cisco.

Significantly, efforts to modify existing market dynamics within Finland have not just been limited to the Finnish state. It is not possible to examine government intervention in and the evolution of the cybersecurity market and eco-system within Finland without recognizing the role the EU has played and will continue to play in this domain. Finland has pursued a path of strong economic integration and views the EU has an important market and security community. In fact, the EU is directly referenced in the most recent Security Strategy for Society with an eye toward the importance of this regional institution for both the security and economic vibrancy of Finland (Security Strategy for Society 2017, 17).

Like its member countries, the EU has also deployed a series of industrial policies that have shaped cybersecurity capacity and competency within Finland. Many of these efforts have occurred within and are concerned with broader EU activity and coordination. Others have focused specifically within member states themselves, largely through regulations and standard setting. It is the latter category of EU intervention that is directly modifying industry behaviour in the Finnish market and so it will be this latter category that will be discussed in more detail in this paper.[9] There are two initiatives of particular importance at the moment for Finland: The EU's new General Data Protection Regulation (GDPR) and Directive on Security of Network and Information Systems (NIS Directive). Both the GDPR and the NIS Directive are expected to come into effect this year, 2018. The Finnish Ministry of Justice formed a working group to address the implementation of the GDPR last year while the Finnish Ministry of Transport and Communication submitted a proposal to parliament earlier this year on how to implement the NIS Directive. By seeking to strengthen and harmonize member states approaches to data privacy (GDPR) and cybersecurity resilience and preparedness (NIS Directive), these two EU

[9] For a discussion of broader EU policy here see Paul Timmers' "Industrial Policy in a Regional Context: EU Approaches to Bolstering the Cybersecurity Market" in this special issue.

initiatives are actively altering both Finnish government and industry behaviour around privacy and security.[10]

In conclusion, this category of intervention – prioritizing frameworks and requirements for cooperation and coordination - has comprised the bulk of Finnish and EU efforts in this space. It forms the bedrock of the Societal Security Strategies and the National Cybersecurity Strategy and has been mirrored in the National Defence Courses and the creation of FISC. EU interventions into the Finnish market through the GDPR and NIS Directive can also best be understood as largely market modifying endeavours.

Market Substituting

To a lesser extent, Finnish industrial cybersecurity can be characterized as market substituting: where interventions seek to supplement existing market activity in order to achieve key provisions of goods or services, which actors in any given market would otherwise not produce. You can most significantly observe this type of intervention in the Finnish case around the creation of and assistance with supply pools of activity and services in critical sectors. In addition, Finland has substituted existing market activity through the provision of cybersecurity specific education and training to create a broader pool of professionals for both the private and public sectors in this space.

One primary example of market substituting efforts in the comprehensive security framework, occurs through the NESA. Namely, as the previously discussed, the creation of and government assistance with security of supply in critical sectors. This intervention targets goods and services that would not be provided, either in scope or in kind, by the market more broadly. However, due to national security concerns, the state has created a security market, or a supply market, in which these goods and services are generated during times of peace specifically so that they can be utilized in times of crisis.

Education initiatives represent another example of market substituting behaviour. Through the creation of a publicly funded, largely comprehensive education system, Finland already has strong market substitution in the realm of education. This previous intervention forms the bedrock of educational outcomes within the country and played an important role in Finnish efforts to transition to a knowledge-based and hi-tech economy (Ali-Yrkkö et al. 2005).

This existing level of education has also been substituted through additional cybersecurity specific interventions. One such intervention occurred by leveraging the existing general conscription system, where a large percentage of the Finnish Defence Forces are comprised of reservists rather than career military personal. One advantage to this system is that the military itself is able to leverage expertise from a wide range of sectors in its defence given that these individuals work across all of Finnish society. Another advantage is that the defence forces themselves can substitute existing levels of education b altering how it trains these conscripts. In fact, starting in 2015, the Finnish Defence forces began to offer cybersecurity training to all its conscripts (Hermunen (2015). These conscripts are able to deploy this baseline knowledge in the

[10] While they are not equivalent goals, in practice it can be difficult to draw a line between security and privacy. One is not the other but building systems for privacy implies a degree of security.

context of their service requirement but also when they return back to their civilian sectors. In addition to this broad training, specialized training was offered to a smaller number of conscripts that then returned to cybersecurity jobs within industry. This intervention partially addressed two broader concerns simultaneously: bolstering and maintaining cybersecurity competency within the defence forces themselves and improving cybersecurity competency within the broader civilian workforce.

In conclusion, to a lesser extent, Finland has pursued market substituting interventions alongside its highly ambitious market modifying initiatives. Both efforts are somewhat novel: the creation and maintenance of security of supply markets focusing on critical goods and services and leveraging a conscript system to augment the existing education system.

Market Facilitating

To an even more limited extent Finland has deployed market facilitating interventions by investing in and providing specific goods and services to better facilitate industry and government efforts to secure their own systems. This has been pursued in three categories of activity: the increasing role of the government as a customer for cybersecurity technology, the provision of a monitoring and warning system that provides key threat information to be used by those seeking to secure their own systems, and investments in research and development.

The government has facilitated cybersecurity development and activity by increasing its role as a customer of the cybersecurity sector, both in terms of purchasing commercial products and in contracting with firms in the production of government specific products. There is a long history of 'government as customer' inventions in Finland including the notable role Nokia played in providing secure communication devices for the Finnish Armed Forces and in building out national communications infrastructure for the country as a whole (Doz and Wilson 2018). One impediment to government purchasing specific cybersecurity technology has been the existing intelligence laws, which prohibited the interception of confidential communications without the suspicion of a crime. This in turn limits mass data collection and analysis, which is widely recognized as a pivotal step in threat assessment and detection. The parliament is currently debating intelligence reform, two laws and one Constitutional reform, centring around mass data collection and analysis of confidential electronic communications (Reuters Staff 2018). If these restrictions were to be removed, the government could invest in and purchase specific sets of cybersecurity capabilities that it had previously been prevented from investing in. This in turn creates the potential for a broader domestic market for these products, allowing companies to sell within Finland in addition to abroad.

The Finnish National Cyber Security Centre (NCSC-FI) has also been tasked with monitoring the security situation and releasing alerts and vulnerability reports for general use. This is achieved through a detection and alert system that leverage government and private companies' situational awareness. In 2014 alone, NCSC-FI issued 'more than 600 red alerts which flagged malware targeting the nation's most critical companies' (Limnéll and Tabansky 2015). These notifications fall into three broad buckets: disturbances and information security threats, Telecom notifications of an information security incident, and notifications of information security breaches (FICORA 2018). It also produces guidelines on a range of issues.

Finally, Finland has also sought to facilitate the development and maintenance of cybersecurity capabilities through research and development funding. Although operating on a limited year and financial mandate on the public end of the private-public partnership (2015-2017), the CyberTrust Program conducted research in three main areas - secure services, securing platforms and networks, and advanced threats and security assurance – and facilitated the creation of a Security and Software Engineering Research Site in Oulu (DIMECC 2018). Research and development has also been translated into a specific service for both the public and private sector. VTT Technical Research Centre of Finland, operating under the mandate of the Ministry of Employment and the Economy, is a leading research and technology institution in Europe serving both the private and public sector. In cybersecurity, VTT specifically focuses on the design, development, and testing of cybersecurity capabilities and operations for its customers (VTT Services 2018). It also operates the Cyber War Room, which "includes a mini-Internet simulation environment that is completely isolated from all other telecommunications and where the devices or software being tested can be subjected to highly realistic cyber-attacks in a controlled way" allowing for stronger cybersecurity testing and analysis (VTT Security Testing and Analysis 2018).

Notably, research and development efforts have also occurred in cooperation with traditional market and security partners and have not been limited to Finnish industry or research initiatives. The Sendate project under the broader umbrella of Celtic-Plus, has a three-year mandate and a 25,374,000 € budget (Celtic-Plus 2018). Sendate is a research and development cluster project focusing on securing the cloud and large data centres in Europe. As a public-private partnership, the overall coordinating committee is led by a Finnish company, Nokia. On the public front, the project is funded in combination by all four states' – Finland, France, Germany, and Sweden – public research and development funding agencies. Similarly, in 2017, Finland and the US became cybersecurity research partners through a cooperation agreement reached between the Research Institute in Oulu and the US National Science Foundation's 'Industry University Cooperative Research Center' Program (DIMECC 2017). The EU, through its Horizon 2020 effort, has also set aside funds focusing on cybersecurity, which Finland has an opportunity apply (European Commission's Horizon 2020 2018).

In conclusion, while Finland's market facilitating efforts have been more limited when compared to its market modifying interventions, it has increased its own commitments as a cybersecurity customer, provided a monitoring and warning system, and invested in research and development within Finland and in partnership with other countries.

To summarize this section, within the framework provided by Carman and Harris, Finnish interventions fall into three broad categories: *market modifying*, *market substituting*, and *market facilitating.* Market modifying efforts represent the bulk of efforts, both in terms of depth and breadth, while market facilitating represent the least depth and breadth. All of these efforts, although broken apart in this section, are seen as part of a wider systems-based approach to comprehensive security.

5. Concluding Thoughts and Lessons Learned

In conclusion, Finland has set itself apart both as a global leader in cybersecurity technology and with regard to the concept and operationalization of comprehensive societal security, a framework within which Finland's cybersecurity policy and its specific market interventions are embedded. Two factors highlight the strength of this Finnish approach to industrial cybersecurity policy. First, the concept of comprehensive security has proven adaptable to the realities and requirements of cybersecurity competency and capabilities given its focus on the critical role of the civilian sector in national defence and its recognition that significant harm and costs can be imposed on states without the deployment of military means. Second, this comprehensive security model integrates a range of market interventions allowing for a systems-based approach to cybersecurity that is unique in both depth and breadth. Taken alongside high technical capabilities, this comprehensive security, systems-based model for interventions and the corresponding high levels of trust and cooperation between public and private actors that it engenders has formed the core of Finnish cybersecurity capacity and competency.

However, perhaps Jarno Limnéll, Professor of Cybersecurity at Aalto University and former Director of Cyber Security at both McAfee and Stonesoft, put it best when he explained that just because Finland appears to being doing well in comparison to other countries 'does not mean there isn't a lot more to do. We're the valedictorian in a class full of dummies' (YLE Uutiset 2017). Despite its existing cybersecurity ecosystem and its implementation of cybersecurity within a comprehensive security framework, four areas of persisting concern remain.

First, despite the presence of societal security strategies alongside the national cybersecurity strategy and its related implementation documents[11], Finland's approach to cybersecurity remains highly sectoral, siloed, and lacking in centralized management. This was one of the concerns raised in the 2017 government report entitled, 'Finland's cyber security: the present state, vision and the actions needed to achieve the vision' completed for the Prime Minister´s Office. (Lehto et al. 2017). This has also inhibited efforts to assess gross national activity in this space given the lack of a strong centralized oversight or management of cybersecurity activities occurring within various ministries. Despite its strength in cooperation and coordination, efforts are hampered without clearer strategic management of all the various efforts occurring at all levels of government and in cooperation with various industry partners.

Second, a frequently cited concern in informal discussions and interviews with key member of industry, is that the government's focus on cooperation and information sharing has not been accompanied by significant, public financial investments in cybersecurity technology or capacity outside of government ministries and the defence forces (i.e. these interventions lack the significant financial investments present in the *market facilitating* approaches of other states which are announcing large sums of money to be earmarked toward the creation of and maintenance of cybersecurity competency and capabilities). Within the Finnish approach to cybersecurity, financial commitments are distributed between and buried within various ministries' budget making an overall assessment of such commitments challenging. There are some efforts occurring within the EU as well such as the 2018 call for proposals for a €50

[11] Most notably, the Implementation program for Finland's cyber safety strategy 2017-2020.

million pilot under Horizon 2020, which would focus on the development of a research and development network across EU member countries seeking to address cybersecurity industrial challenges (European Commission's Horizon 2020 2018). However, looking to other international examples, many Finnish companies felt that financial commitments to cybersecurity in the civilian space were relatively weak and that this represents a central challenge to the provision of cybersecurity for Finnish society writ-large.

Third, despite the exponentially growing digital attack surface and the proliferation of digital security threats, people remain the weakest link in cybersecurity. People are the weakest link in the security supply chain (both as consumers and as employers). Attackers rely on what individuals do (open emails, plug in flash drives, click on links, etc.) and what they do not do (install updates, maintain backups, etc.) in designing their attacks. People are also the weakest link in terms of the cybersecurity skills gap. Both the private and public sector demand for cybersecurity professionals outpaces the availability of such professionals (Haaramo 2018). Despite having a strong national education system, Finland continues to face a gap between demand and supply. Interestingly, the skills gap and the explosion in demand for cybersecurity professionals has resulted in an emerging set of discussions around the automation of specific security tasks through machine learning and artificial intelligence (Gil 2018).

Fourth, the question of securing the product lifecycle remains a central concern amongst efforts to secure cyber systems within Finland. Most notably, the Cybersecurity Implementation Programme for the years 2017-2020 has emphasized the importance 'cyber self-sufficiency' (Adamowski 2017) and that the EU's 2017 Cybersecurity Package has similarly emphasized security autonomy. However, as a relatively small country with a limited population and resources, it is not possible for Finland to contain the entire security lifecycle of products. This means that domestic industry will continue to specialize and that the market will be augmented by products emanating from outside of Finland. Many of the dominant players in ICT are currently American, and increasingly Chinese. The question for Finland then becomes, what aspects of the product lifestyle can be sourced from Finnish companies? From what is leftover, what needs to be secured from outside Finland and what portion of those products can already be secured from other EU states or developed cooperatively within the EU? Galileo is an example of intervention and pooling at the EU level in the pursuit of a capability individual member states were unlikely to secure alone. Nicknamed the European GPS, Galileo seeks to provide EU members with an alternative to the U.S.'s GPS as well as China's Beidou and Russia's GLONASS (European Commission Galileo 2018). Following this question of broader EU alternatives, the question for Finland then becomes how to import technology and rely on non-domestic providers of technology in the most secure manner possible. The reliance on global supply chains coupled with the specialization required of small, agile economies remain two economic realities that bring with them deep security concerns for Finland.

References

Adamowski, Jaroslaw. 2017. "Ukraine conflict puts cyber-security high on agenda in Eastern Europe". *SC Magazine UK*. 1 June 2017. Accessed on 3 April 2018. https://www.scmagazineuk.com/ukraine-conflict-puts-cyber-security-high-agenda-eastern-europe/article/1474564

Aggarwal, Vinod and Reddie, Andrew (2018) "Comparative Industrial Policy and Cybersecurity: A Framework for Analysis," BASC Working Paper Series, 2018-01.

Aggarwal, Vinod and Reddie, Andrew (2018) "Comparative Industrial Policy and Cybersecurity: The U.S. Case," BASC Working Paper Series, 2018-02.

Ali-Yrkkö, Jyrki, Marrku Lehmus, Petri Rouvinen, and Vesa Vihriälä. 2017. *Riding the Wave: Finland in the Changing Tides of Globalization.* Research Institute on the Finnish Economy (ETLA).

Blitz, James. 2012. "Israel, Finland and Sweden top for computer security". *Financial Times*. 30 January 2012. Accessed on 2 April 2018. https://www.ft.com/content/0e626614-4ab5-11e1-a11e-00144feabdc0

Carman, James M. and Robert G. Harris. 1984. "Public Regulation of Marketing Activity: Part II: Regulatory Responses to Market Failures**"** *Journal of Macromarketing* 4(1):

Celtic-Plus. "Sendate Project". Accessed on 1 April 2018. https://www.celticplus.eu/sendate-planets/

Columbus, Louis. 2017. "2017 Roundup Of Internet Of Things Forecasts". *Forbes*. 10 December. Accessed on 3 April 2018. https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#6454a6661480

Cybersecurity Ventures. 2016. "Cybersecurity Market Report*". Cybersecurity Ventures.* Accessed on 4 March 2018. https://cybersecurityventures.com/cybersecurity-market-report-test/

DIMECC Cyber Trust Program: We Return the Trust to the Digital World**.** Webpage**.** Accessed 10 April 2018. http://cybertrust.fi/

DIMECC. 2017. "Finland and U.S. Become Cyber Partners". Accessed 1 March 2018. https://www.dimecc.com/finland-usa-become-cyber-partners-new-research-cooperation-builds-upon-success-dimeccs-innovation-program-cyber-trust/

Doz, Yvos and Keeley Wilson. 2018. *Ringtone: Exploring the Rise and Fall of Nokia in Mobile Phones.* Oxford University Press.

EPSC Strategic Notes. 2017. "Building an Effective European Cyber Shield: Taking EU Cooperation to the Next Level". *European Political Strategy Centre* Issue 24. https://ec.europa.eu/epsc/sites/epsc/files/strategic_note_issue_24.pdf

European Commission. "Commission launches a call for proposals for a €50 million pilot to support the creation of a network of cybersecurity competence centres across the EU". Webpage. Accessed 25 March 2018. https://ec.europa.eu/programmes/horizon2020/en/news/commission-launches-call-proposals-%E2%82%AC50-million-pilot-support-creation-network-cybersecurity

European Commission. "Galileo". Webpage. Accessed 25 March 2018. http://ec.europa.eu/growth/sectors/space/galileo_en

Finland´s Cyber Security Strategy. 2013. https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf

Finnish Communications Regulatory Authority (FICORA). "Information security services of the NCSC-FI". Webpage. Accessed 1 April 2018. https://www.viestintavirasto.fi/en/cybersecurity/ficorasinformationsecurityservices.html

DIMECC. 2017. "The Finnish CyberTrust Programme 2015-2017 Final Report." *DIMECC Publications Series* no. 20. http://cybertrust.fi/wp-content/uploads/2017/10/DIMECC717_CyberTrust.pdf

Finnish Information Security Cluster (FISC). "Mission". Webpage. 25 March 2018. https://www.fisc.fi/

Forsell, Tuomas and Jussi Rosendahl. 2016. "Finland government strikes deal with unions to boost stagnant economy". *Reuters.* 3 June 2016. Accessed on 3 April 2018. https://www.reuters.com/article/us-finland-labour-metalworkers-idUSKCN0YP2F3

Gil, Laurent. 2018. "The Debate is Over: Artificial Intelligence is the Future for Cybersecurity". *SC Magazine UK*. 22 March 2018. Accessed on 3 April 2018. https://www.scmagazine.com/the-debate-is-over-artificial-intelligence-is-the-future-for-cybersecurity/article/749603/

Haaramo, Eeva. 2015. "CGI tempts Nordic customers with Finnish cyber security centre". *Computer Weekly.* 18 November 2015. Accessed on 3 April 2018. https://www.computerweekly.com/news/4500257591/CGI-tempts-Nordic-customers-with-Finnish-cyber-security-centre

Haaramo, Eeva. 2018. "Cyber attacks in 2017 drive Nordic security efforts". *Computer Weekly*. 9 January 2018. Accessed on 3 April 2018. https://www.computerweekly.com/news/450432801/Cyber-attacks-in-2017-drive-Nordic-security-efforts

Hathaway, Melissa. 2013. "Cyber Readiness Index 1.0" Report Presentation at the Belfer Center. Hathaway Global Strategies. Accessed on 1 April 2018.

https://www.belfercenter.org/sites/default/files/legacy/files/uploads/Cyber-Readiness-Index-1-0-November-2013.pdf

Hermunen, Tommi. 2015. "Finnish Defence Forces starts engaging conscripts in cyber defense". English translation of Hermunen's original article in Finnish. Accessed 25 March 2018. https://www.linkedin.com/pulse/finnish-defence-forces-starts-engaging-conscripts-cyber-hermunen/

Implementation program for Finland's cyber safety strategy 2017-2020. English Translation. Electronic Copy provided by Finnish Security Committee.

International Telecommunication Union (ITU). 2017. Global Cybersecurity Index. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

Invest in Finland. 2017. "Novasano Values Finnish Cyber Security Expertise". Accessed 3 April 2018. https://www.investinfinland.fi/-/novasano-values-finnish-cyber-security-expertise

Kauppinen, Tero. 2015. "Cybersecurity of Supply" National Emergency Supply Agency presentation at the FIIF JAM SESSION. 22 September. Accessed 4 March 2018. http://teknologiateollisuus.fi/sites/default/files/file_attachments/3_-_cyber_security_of_supply_20150922.pdf

Lehto, Martti, Jarno Limnéll, Eeva Innola, Jouni Pöyhönen, Tarja Rusi, and Mirva Salminen. 2017. "Finland's cyber security: the present state, vision and the actions needed to achieve the vision". For the Prime Minister's Office. Accessed 10 April 2018. http://tietokayttoon.fi/documents/10616/3866814/30_Suomen+kyberturvallisuuden+nykytila%2C+tavoitetila+ja+tarvittavat+toimenpiteet+tavoitetilan+saavuttamiseksi_.pdf/372d2fd4-5d11-4991-862c-c9ebfc2b3213?version=1.0

Limnéll, Jarno and Lior Tabansky. 2015. "Governments need to protect industry from cyber-espionage - and some do". *SC Magazine UK*. 20 April 2015. Accessed on 2 April 2018. https://www.scmagazineuk.com/governments-need-protect-industry-cyber-espionage/article/1478754

The National Emergency Supply Agency (NESA). "Security of supply in Finland". Webpage. Accessed 1 April 2018. https://www.nesa.fi/security-of-supply/

The National Defence University (NDU). "National Defence Courses". Webpage. Accessed 1 April 2018. http://maanpuolustuskorkeakoulu.fi/en/national-defence-courses

Nokia Press Release. 2016. "Nokia and Sonera demonstrate role of fixed and mobile networking technologies on the path to 5G". Accessed 1 April 2018. https://www.nokia.com/en_int/news/releases/2016/09/13/nokia-and-sonera-demonstrate-role-of-fixed-and-mobile-networking-technologies-on-the-path-to-5g

Pelkonen, Antti, Reijo Savola, and Jarno Salonen. 2017. *E&T.* Accessed 10 April 2018 https://cybersecurity.theiet.org/users/62121-antti-pelkonen/posts/19766-cybersecurity-competences-research-development-and-innovation-perspective

Reuters Staff. "Finnish government calls for urgent approval of intelligence bill". *Reuters*. 25 January 2018. Accessed on 3 April 2018. https://www.reuters.com/article/us-finland-security/finnish-government-calls-for-urgent-approval-of-intelligence-bill-idUSKBN1FE2DA

Salonius-Pasternak, Charly. 2017. "An effective antidote: The four components that make Finland more resilient to hybrid campaigns" *Finnish Institute of International Affairs.* https://www.fiia.fi/sv/publikation/an-effective-antidote?read

Security Strategy for Society. 2017. English Translation. https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf

Singer, P.W.and Allan Friedman .2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press; 1st edition.

Soesanto, Stefan. 2017. "Europe's digital power: from geo-economics to cybersecurity" *European Council on Foreign Relations.* http://www.ecfr.eu/publications/summary/europes_digital_power_from_geo_economics_to_cybersecurity7274

Standish, Reid. 2016. "How Finland Became Europe's Bear Whisperer" *Foreign Policy.* 7 March 2016. Accessed on 2 April 2018. https://foreignpolicy.com/2016/03/07/how-finland-became-europes-bear-whisperer-russia-putin/

Symantec. 2018. "Internet Security Threat Reports" Vol. 23. https://img03.en25.com/Web/Symantec/%7Bf8ca1fb2-b73c-46d0-ae9e-17456c45df87%7D_ISTR23-FINAL.pdf?aid=elq_

Tekes Press Release (2017). "Finland's First 5G Development Environment Opens to Business in Oulu". Website. 25 March 2018. https://www.businessfinland.fi/en/whats-new/news/news-2017/finlands-first-5g-development-environment-opens-to-businesses/

Timmers' paper on the EU in this special issue

Vogel, Steven K. 2018. *Marketcraft: How Governments Make Markets Work*. Oxford University Press, Kindle Edition.

VTT Technical Research Centre of Finland. "Services: Cybersecurity". Website. Accessed 1 April 2018. http://www.vttresearch.com/

VTT Technical Research Centre of Finland. "Security testing and analysis". Website. Accessed 1 April 2018. http://www.vttresearch.com/services/digital-society/data-driven-solutions/cyber-and-information-security/security-testing-and-analysis

Website Builder Expert .2017. “Which EU Country Is Most Vulnerable To Cybercrime?” Accessed 20 March 2018 https://www.websitebuilderexpert.com/eu-cybercrime-risk/

Ylä-Anttila, Pekka and Christopher Palmberg. 2005. “The Specifications of Finnish Industrial Policy – Challenges and Institutive at the Turn of the Century”. *Research Institute on the Finnish Economy (ETLA)*. Discussion Paper. https://www.etla.fi/wp-content/uploads/2012/09/dp973.pdf

YLE Uutiset. “Finland a "valedictorian in a class of dummies" in cyber security”. 4 February 2017. Accessed on 2 April 2018. https://yle.fi/uutiset/osasto/news/finland_a_valedictorian_in_a_class_of_dummies_in_cyber_security/9442093