FIIA
BRIEFING PAPER
GEOECONOMICS SERIES

JUNE 2022 / 341

AUTONOMY THROUGH DIGITAL RESILIENCE

THE IMPORTANCE OF UPHOLDING THE NATIONAL TECH STACK

Markus Holmgren

FINNISH
INSTITUTE
OF INTERNATIONAL
AFFAIRS

AUTONOMY THROUGH DIGITAL RESILIENCE

THE IMPORTANCE OF UPHOLDING THE NATIONAL TECH STACK

- The national tech stack refers to the totality of a nation's technological capability, including its infrastructure, supply chains, governance, and knowledge base. In a digitally interconnected world, strong and resilient tech stacks are the key to maintaining the capability for autonomous decision-making.

- Expertise is key for digital resilience. Once knowledge of how to build, repair, rebuild, reconnect, or reform technological infrastructure is lost, it cannot be quickly replaced.

- Even-handed binding regulation is paramount for strengthening digital resilience. Yet not all regulation is beneficial, which is why expertise and public-private cooperation are important. Legislation should bind actors irrespective of the technologies utilised.

- It is impossible for any nation to invent updates and build digital capabilities by itself in a way that competes with the rest of the world. Therefore, attempting excess self-sufficiency is counterproductive. Instead, nations need to secure access to critical international data and service flows, for which reason mutual reliability and goodwill should be strategically developed.

- Tech stacks are closely interlinked with one another, which means that enforcing common rules increases performance and digital resilience.

MARKUS HOLMGREN

Research Fellow

Global security

Finnish Institute of International Affairs

ISBN 978-951-769-729-3
ISSN 1795-8059
Language editing: Lynn Nikkanen
Graphics: Otso Teperi
Cover photo: Pixabay/Bruno

This FIIA Briefing Paper has been prepared as part of FIIA's co-operation with the National Emergency Supply Agency (NESA).

FIIA
FINNISH
INSTITUTE
OF INTERNATIONAL
AFFAIRS

Arkadiankatu 23 b
POB 425 / 00101 Helsinki
Telephone +358 (0)9 432 7000
Fax +358 (0)9 432 7799

www.fiia.fi

The Finnish Institute of International Affairs is an independent research institute that produces high-level research to support political decision-making as well as scientific and public debate both nationally and internationally.
All manuscripts are reviewed by at least two other experts in the field to ensure the high quality of the publications. In addition, publications undergo professional language checking and editing. The responsibility for the views expressed ultimately rests with the authors.

AUTONOMY THROUGH DIGITAL RESILIENCE

THE IMPORTANCE OF UPHOLDING THE NATIONAL TECH STACK

INTRODUCTION

There are few areas of economy and security that are not critically dependent on Information and Communication Technology (ICT) solutions, the most important of which is the internet.

Practically all supply chains are international. Banking and financing services are operated with automated transnational data flows, and governments have to be able to make and communicate informed decisions without delay. In fact, any system, building or, increasingly often, an individual device that is *not* connected to the internet appears critically outdated. At the same time, everything that uses digital services also produces data, which is why data has become a strategic resource.

In a brief period of decades, the internet has become a globally shared system on which states and companies rely, but which they control only in a limited sense. Understanding how a nation's capability for autonomous decision-making is tied to the internet and related technologies is a complicated multidisciplinary endeavour that requires accounting for geoeconomic, geopolitical, as well as economic interests. To help with conceptualising the collection of technologies used in running a nation, as well as digital resilience, this Briefing Paper introduces the term *national tech stack*.

The paper proceeds by firstly elaborating on the notion of the national tech stack in relation to improving digital resilience. It then pays attention to four of its aspects: digital infrastructure, technological supply chains, internet governance, and the expertise that ties them together. Based on the analysis, the paper concludes with a brief reflection on the possibilities and challenges related to national digital resilience.

NATIONAL TECH STACK AND DIGITAL RESILIENCE

The term tech stack, sometimes referred to as the data ecosystem, does not have a universally accepted definition. However, in general, it can be defined as the set of technologies and capabilities required to build and run a website, application, project, or system. The *national* tech stack thus refers to the totality of a nation's technological capability, including infrastructure, supply chains, governance, and knowledge base, which it leverages to maintain the capability for autonomous decision-making.

Curiously, every national tech stack is inherently international because critical infrastructure, supply chains, governance procedures, and expert labour markets are all international.

In the digital age, a nation's capacity for autonomous decision-making hinges to a large extent on its tech stack. If the tech stack fails, the nation's digital autonomy (understood in terms of access instead of autarchy) will diminish, and as a consequence so will its capacity for autonomous decision-making. This is why the resilience of the national tech stack has become so important.

Before moving on to digital resilience, three related terms – data, digital, and resilience – need to be defined. In this paper, data refers to the quantities, characters, and/or symbols on which computer operations are performed, which may be stored and transmitted in the form of electrical signals, and recorded on magnetic, optical, or mechanical media. Digital is something that is composed of data in the form of (binary) digits. For the purposes of this paper, resilience means having the physical, legislative, and intellectual capability to adapt rapidly and effectively in the face of adversity or disruption.[1] A resilient system takes disruptions as opportunities to improve, having carefully invested in preparing to do so.

Digital resilience encompasses those solutions that increase the adaptability of the digital system in question when faced with disruptions. In the context of nations, digital resilience can be defined as the actions that nations take to secure their vital digital functions, critical ICT infrastructure, and critical data.

These actions often go through private companies. They also require a networked approach to

[1] See Fjäder, Christian. 2014. 'The nation-state, national security and resilience in the age of globalisation', *Resilience*, 2:2, 114–129. See also Walker, Brian. 2020. 'Resilience: what it is and is not', *Ecology and Society* 25(2):11.

international security hierarchies,[2] which can be defined as a continuum on which one actor has political power over other actors, public or otherwise.[3]

The challenge with (digital) resilience lies in weighing between preparing for likely low-impact and unlikely high-impact disruptions. Threats to resilience come from many fronts, and hence preparing for each one individually is practically impossible.

The key points for building digital resilience are: 1) excess self-sufficiency at the expense of international cooperation will not strengthen resilience; 2) still, there is a critical core of services and infrastructure that ought to remain under sovereign control; and 3) expertise is critical, and it must be maintained by investing in education as well as research and development (R&D), and by keeping critical systems updated.

In general, resilience-building is a holistic process that considers stockpiles and accessibilities, capabilities, and vulnerabilities. Software, components, and critical digital services often have a short shelf life, which makes stockpiling them impractical. What this means is that digital resilience can only be built in two ways – by securing international connections or by building a comprehensive, full-fledged domestic capability, which is impossible for a small country like Finland.

The national tech stack and digital resilience are naturally interconnected in that they support and supplement each other. For example, by investing in expertise, flexible access to critical resources, and market-oriented even-handed regulation, both the national tech stack as well as its resilience are strengthened.

1. DIGITAL INFRASTRUCTURE

Digital infrastructure refers to technologies that gather, transmit, refine, or utilise digital data. It includes the software and operation principles integral to the infrastructure, as well as the hardware solutions that the software is a part of. The most important digital infrastructure is the underlying structure of the internet, including its operational principles like the internet protocol suite (TCP/IP).

In practice, much of the deployment of digital infrastructure is market-oriented and fragmented.[4] The result is a diverse network of digital infrastructure that has some innate vulnerabilities, while being naturally insulated against total collapse at the same time.

Newer technologies occasionally make old systems obsolete, but the deployment of those new technologies is often slow and geographically limited. As a result, old and new technologies co-exist. This creates some vulnerabilities, but is also a potential source of strength as diversification is the key to increasing resilience in digital infrastructure. For this reason, it is worth considering whether old infrastructure could be maintained and regularly updated also after newer systems have been deployed so that they could serve as emergency options.

At the level of individual systems, the focus of attention changes. From a resilience perspective, the aim is to detect and mitigate vulnerabilities in systems before they get exploited. There are two ways to approach the topic.

First, there are vulnerabilities to cyber-reliant systems. They can come from virtually any direction and impact any part of the system, and may be inherited by all cyber-reliant systems. Figure 1 highlights some of the most prominent sources of vulnerability.

Preparing for these vulnerability sources necessarily expands the scope of preparedness far beyond digital means. A whole-of-nation approach has to be considered.

The second way to approach the topic is to zoom in on the specific cyber vulnerabilities (Figure 2). These include:

1) Unintended taint. Unintended taints are coincidental faults in hardware or software design, or in their interaction, that hamper the operations or cyber security of the product. Good examples of these are hardcoded passwords[5] and outdated features.

2) Malicious taint. Malicious taints are purposefully vulnerable functions or security subversions either in hardware or in software. Concrete examples include backdoors and missing details.

3) Counterfeit. Counterfeits are faulty or unfit hardware or software products passed as genuine. They are often caused by cutting costs in the wrong places, such as compatibility testing.

4) Chain-interaction vulnerabilities. These vulnerabilities result from interaction with incapable organisations or from unsatisfactory cooperation.

[2] Schmidt, Andreas. 2013. 'Hierarchies in Networks. Emerging Hybrids of Networks and Hierarchies for Producing Internet Security'. In Kremer, Jan-Frederik & Müller, Benedikt (eds.), *Cyberspace and International Relations. Theory, Prospects, and Challenges*. New York: Springer.

[3] Lake, David. 2009. 'Hobbesian hierarchy: The political economy of political organization'. *Annual Review of Political Science*, 12, 263–283.

[4] See Mueller, M. 2017. *Will the Internet Fragment?* Cambridge, UK: Policy Press.

[5] Passwords or other secrets in source code embedded in a non-encrypted text. Often referred to as embedded credentials.

Vulnerabilities of digital infrastructure and systems critically dependent upon it

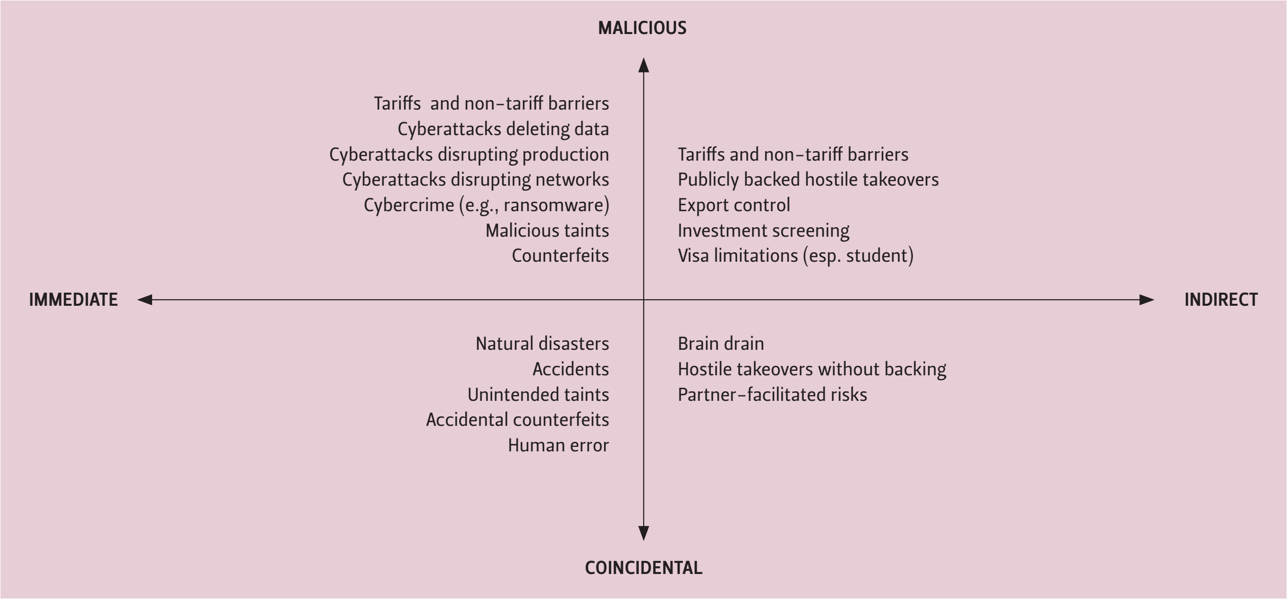
MALICIOUS
Tariffs and non-tariff barriers
Cyberattacks deleting data
Cyberattacks disrupting production
Cyberattacks disrupting networks
Cybercrime (e.g., ransomware)
Malicious taints
Counterfeits
Tariffs and non-tariff barriers
Publicly backed hostile takeovers
Export control
Investment screening
Visa limitations (esp. student)
IMMEDIATE
INDIRECT
Natural disasters
Accidents
Unintended taints
Accidental counterfeits
Human error
Brain drain
Hostile takeovers without backing
Partner-facilitated risks
COINCIDENTAL

Figure 1. Vulnerabilities of digital infrastructure and systems critically dependent upon it.
Source: Author's own construction.

A critical partner providing faulty products is a good example, and faulty interaction caused by cutting costs in gateway coding (between networks) is a common one.

5) Human error. Lastly, there is always the human factor and vulnerabilities resulting from mistakes, carelessness, or bad maintenance. For example, as the COVID-19 pandemic forced more people to use internet tools, human errors and system misconfigurations spiked to the extent that during 2020 they became the most common source of cyber vulnerability.[6]

It is important to remember that data, including software, is physical and always located somewhere. Even when packed in wavelengths of light, data has a material aspect in the sense that it is always stored and transmitted in a physical medium. For this reason, it is often reasonable to treat software as a part of hardware.

From the perspective of the tech stack, capabilities to counter cyber vulnerabilities and attempts to exploit them include, among other things, "[…] vulnerability identification and disclosure, malware analysis, incident response, network and software maintenance, monitoring and updating, risk assessment and insuring, internal policy development, and hiring and training".[7]

This list reminds us that cyberattacks do not always target data. Critical systems like pipelines, electricity networks, hospitals, and the internet itself can also be, and often are, targets of disruptive operations. Recovering from these disruptions requires secure access to resources, which in turn requires adaptive supply chains.

2. TECH SUPPLY CHAIN MANAGEMENT

A supply chain can be loosely defined as a network between a company and its suppliers to produce and distribute a specific product for the final customer(s). Hardware and software solutions for data production and advanced analysis both rely on international supply chains. At the same time, related security interests are often framed nationally. From the national tech stack's security of supply perspective, it is important to understand what can be nationally accounted for and what must rely on other nations.

Supply chains systematically involve inputs and outputs between constituent parts that may vary considerably as relationships change. For this reason, supply chain mapping rarely works for preparedness purposes. Instead, a more flexible approach is required, the aim of which is resilience and adaptiveness, not security and sturdiness.

While protecting data (including code) and infrastructure is in the best interests of every company, much of the capability to do so lies far out of their reach. As cybersecurity must be maintained in all parts and at all levels of society's vital functions and critical infrastructure, a centralised defence system is not an option. Instead, responsibility for resilience

[6] European Union Agency for Cyber Security. 27.10.2021. 'ENISA Threat Landscape 2021', ENISA, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

[7] Pandey, Shipra; Singh, Rajesh; Gunasekaran, Angappa; & Kaushik, Anjali. 2020. 'Cyber security risks in globalized supply chains: conceptual framework', *Journal of Global Operations and Strategic Sourcing*, p. 5.

Cyber vulnerabilities

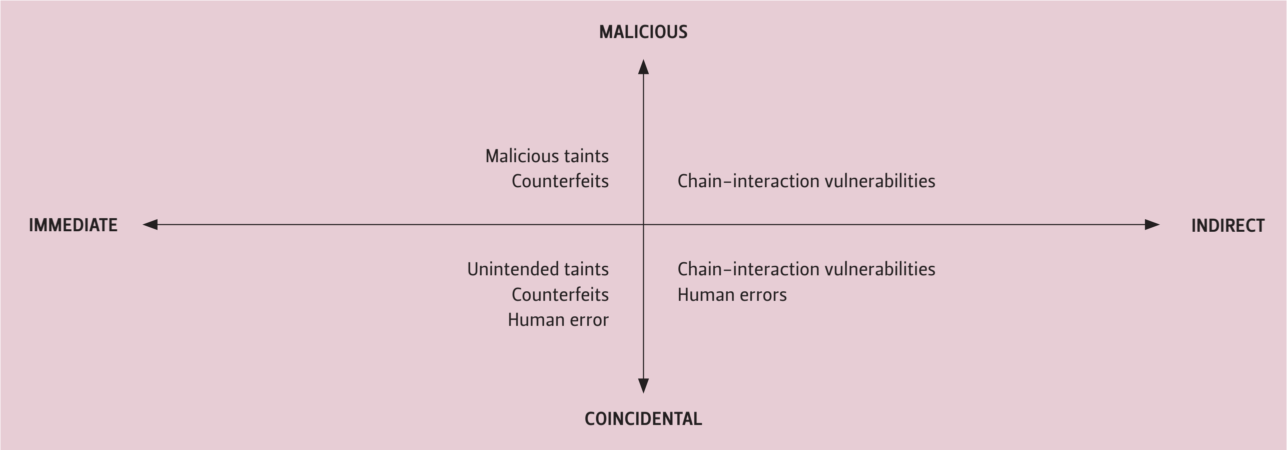

Figure 2. Cyber vulnerabilities.
Source: Author's own construction.

should be spread evenly along the supply chain as much as is feasible, while remembering that open and competitive markets are naturally resilient. The responsibilities should align with the market interests of companies, and implementing resilience-increasing policies should be made as easy as possible.

To this end, the United States has created a National Vulnerability Database that tracks and scores cyber vulnerabilities along the supply chain. The key benefit of such a system is that companies have easy access to unbiased security information when making component or software purchases and are thus able to adjust those purchases or counter the vulnerability elsewhere. Furthermore, the existence and utilisation of such a database does create an incentive to improve products and sell tools for countering them.

In Europe, the annual report on the threat landscape by the European Union Agency for Cybersecurity (ENISA), and the many reports and updates by the EU's Computer Emergency Response Team (CERT-EU) are a step in the right direction, but further cooperation is needed. Systemic vulnerability mapping would be beneficial for all European ICT actors. It is better to know about and prepare for vulnerabilities than attempt to hide them. Information sharing is key.

However, resilience-building competition and cooperation are likely to develop only under a well-regulated governance environment that protects weaker actors from exploitation and thus prevents monopolisation.

3. INTERNET GOVERNANCE

The "governance" in internet governance not only refers to regulation, but to a multitude of public and private sector institutional and normative mechanisms to steer technology development and deployment.[8]

The benefits that the internet offers create competition, which in turn creates further challenges because internet dependency is unevenly distributed, as are the capabilities. The resulting asymmetric dependency in turn creates opportunities to utilise geoeconomic and monopolistic measures,[9] and highlights the importance of shared rules and trust.

National tech stacks are never built in a vacuum, nor can they thrive without a reliable international flow of information. In practical terms, this requires 1) trustworthy hardware and software, 2) access to information located in data storage facilities located in other countries (e.g., about other countries' companies and their products), 3) access to raw materials and products, 4) access to international banking and financing services, 5) access to web navigation services, which are often provided by US companies on servers located on US soil, and 6) access to expertise and critical expert services in other countries.

The conditions under which technological governance is conducted are negotiated by governments even if the agreements in question were not originally designed to regulate data traffic. In fact, many areas of practical internet governance are outside the scope of international agreements, in which case companies

[8] See Solum, Lawrence, B. 2008. 'Models of Internet Governance', Illinois Public Law Research Paper No. 07-25.

[9] See Wigell, M., Scholvin, S. & Aaltola, M. (ed.) 2018. *Geo-Economics and Power Politics in the 21st Century: The Revival of Economic Statecraft*. London and New York: Routledge, 219-227.

need to account for national regulations that often conflict with one another. In these cases, prioritisations are made, usually in favour of the largest regimes. For this reason, a strong regulatory network and trustworthy international relations are of key importance to small nations' digital resilience. In other words, binding agreements build digital resilience.

There are many international regulatory organisations that attempt to govern the internet, often according to conflicting political interests and technological solutions aimed at furthering those interests. Some of the most important ones are the Internet Corporation for Assigned Names and Numbers (ICANN), the World Intellectual Property Organization (WIPO), the Internet Assigned Numbers Authority (IANA), and the Internet Engineering Task Force (IETF).

However, the natural temporal cap between technologies and the regulations governing them often results in a situation in which much of the internet governance is carried out by those private companies that design and deploy new technologies. Thus, states must often go through companies to reshape the internet's topology (even if some of those companies are state-controlled).[10]

Due to systematically different perspectives, the result is that often public governance (both national and international) and private governance find themselves at odds. For this reason, public governance should be willing and able to take technical and market realities into consideration. Yet at the same time, private companies should remember to account for geostrategic realities so that geostrategic measures would not come as a surprise.

Yet not all regulation is beneficial. The key is to make rules clear, create an environment for fair market competition, and create incentives for companies to keep providing critical services for all of their customers also in times of disturbances. This way, companies do not have to guess whether their solutions will remain legal or their various country operations viable.

It is important to note that a decision not to take anti-international resilience measures, such as aiming at autarchy, does in itself build digital resilience. For a nation to rely on access to foreign services that are critical to them, it needs to ensure that those foreign nations have access to its critical services in return. This goes beyond mere interdependence. Mutual reliability and goodwill can and should be strategically developed.

All forms of internet governance, such as technical standards, internet hierarchies, immaterial rights protection, coordination of access and interconnection (e.g., Internet Exchange Points), should also be strategically developed to make them more effective, resilient, and interchangeable. Interconnected tech stacks driven by fair competition, common rules and the free flow of information are naturally resilient.

These principles apply to domestic as well as international governance. As legislation can never keep pace with technological development, regulation, such as law(s) protecting personal data, needs to bind actors irrespective of the technologies utilised.

4. EXPERTISE

Reliable and competitive infrastructure, supply chain networks, and the governance framework all require a wide range of expertise. Therefore, for nations interested in improving both their tech stack's capability and their digital resilience, a constantly growing and increasingly skilful labour force is key.

Without constantly improving expertise, national tech stacks weaken, digital resilience deteriorates, and national autonomy diminishes. Building capability in a rapidly developing technology environment is a complicated process that requires nations to consider the whole of society, especially science, research and development, and education policies.

Most education and R&D programmes developing new technologies are funded by national tax revenues,[11] while high-tech labour pools are increasingly international. This international aspect is very beneficial from the perspective of expertise. International interaction makes ideas and concepts collide, which generates innovation. The free movement of people and ideas offers the benefits of pooling innovation resources without the devastating downsides of monopolisation, such as the tendency to smother competing concepts and ideas.

On the other hand, a lack of relevant expertise has a compound effect on physical infrastructure as well as vice versa. Once a nation starts to produce infrastructure debt – a technical term for not updating infrastructure — its know-how in the field starts to erode. Innovations based on old technologies are far less important than those based on new ones.

In addition, knowledge of how to build, repair, or rebuild cannot be quickly replaced once lost. Without

[10] Sherman, Justin. 2021. 'Cyber Defense Across the Ocean Floor: Geopolitics of Submarine Cable Security'. Washington: Scowcroft Center for Strategy and Security, p. 9.

[11] Mazzucato, Mariana. 2011. *The Entrepreneurial State*. London: Demos.

the expertise, the disrupted systems cannot be quickly repaired or replaced either.

It is in the strategic interests of all nations that the competitiveness of the digital sector is maintained. Sufficient competition extends to supporting the fluidity and attractiveness of labour markets. As a part of this, expert networks should be built strategically. Moreover, investing in public-private partnerships and cooperation increases resilience.

CONCLUSION: DIGITAL RESILIENCE IN THE 21ST CENTURY

During the past decade or so, it has become increasingly apparent that strategic competition among states has also spread into the cyber domain. US cyber operations against uranium enrichment facilities in Iran that started in 2012, the so-called Snowden revelations in 2014, and Russia's interference in the US election in 2016 are notable cases in point. The competition has only intensified since then, and capabilities to effectively participate in it have spread widely, which in turn increases the frequency of disturbances.[12] These developments are not likely to be reversed in the foreseeable future.

At the same time, the frequency of disruptive natural disasters will likely increase as the climate catastrophe deepens. This, in turn, is likely to further increase geopolitical tensions. As the challenges mount, the internet becomes ever more important.

Increasingly, the vital functions of society and critical infrastructure are becoming crucially dependent on the internet and competitive computing technologies. With the introduction of the next general-purpose technology, Artificial Intelligence, this development is likely to speed up significantly.

Isolation cannot be the answer to these challenges. Separate networks are not invulnerable, and all the updates would have to be developed internally, without the commercial benefit from innovation. Instead, resilience has to be built by diversifying digital infrastructure solutions and supply chains, by strategically building trust between actors, and by investing in even-handed binding regulation.

Most importantly, all digital resilience solutions require constantly increasing expertise. The aforementioned actions also serve to strengthen national tech stacks, which further underlines the importance of taking these actions. A failing tech stack not only increases vulnerability, but also the probability of missing out on what is likely to continue to be the most important economic sector of the 21st century./

[12] Segal, Adam. 2016. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. New York: Public Affairs.