Löwinder, Anne-Marie Eklund, and Anna Djup. "Cyberwarfare and the internet: The implications of a more digitalized world ." *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*. By Mikael Weissmann, Niklas Nilsson, Björn Palmertz and Per Thunholm . London: I.B. Tauris, 2021. 145–153. *Bloomsbury Collections*. Web. 26 Apr. 2023. <<http://dx.doi.org/10.5040/9781788317795.0016>>.

Downloaded from Bloomsbury Collections, www.bloomsburycollections.com, 26 April 2023, 10:22 UTC.

Copyright © Mikael Weissmann, Niklas Nilsson, Björn Palmertz and Per Thunholm 2021.
Released under a CC BY-NC-ND licence (<https://creativecommons.org/licenses/by-nc-nd/3.0/>).
You may share this work for non-commercial purposes only, provided you give attribution to the copyright holder and the publisher, and provide a link to the Creative Commons licence.

Cyberwarfare and the internet

The implications of a more digitalized world

Anne-Marie Eklund Löwinder and Anna Djup

Introduction

The creation of the internet has allowed the world to become more globalized and interconnected, producing an environment where organizations are dependent on data flows to conduct their everyday business, affecting everything from operability to business models. In an article from *The Economist* in 2017, it was argued that data is becoming as crucial to the society as oil¹ since the growing reliance on interconnected information makes it impossible to disconnect. This connectivity has in turn made information highly valuable and opened up for new attack vectors, generating a market for hacking and data theft.

If 'data is the new oil'², the growing market for cyber theft could potentially jeopardize the future digital society. For the open internet to continue to exist as a platform for social and economic growth, users must be able to trust that organizations can protect the systems governing the society and have the capacity to safeguard personal information. However, several cases over the years have proved that neither governments nor businesses possess the ability to mitigate imminent cyber threats.

Due to the nature of cyberattacks, it is difficult to ascertain who the actor is and what their intentions are. Cyberattacks are inherently asymmetric in nature as an actor with few means can do much harm to a single individual, organization or nation. Fuelled by the continued trend of organizations and companies connecting to the internet, actors can now easily exploit existing bugs and vulnerabilities in connected devices and networks to achieve their goals.

The much-feared cyber havoc or digital Pearl Harbor³ becomes possible as critical infrastructure is accommodating to the needs of a more digitalized society. To create a digital Pearl Harbor, threat actors will direct an attack against industrial control systems responsible for critical infrastructure. The systems are suitable targets given that the systems were not designed for a digital world, are often out of date, inadequately maintained and difficult to patch. The situation gets even direr as threat actors are using digital tools such as targeted advertising and deep fakes to conduct invisible manipulation of public opinion and election outcomes.

The combination of poorly designed systems, together with new technologies, expands the scope and severity of global cyber threats, and how to tackle these threats will have far-reaching consequences for the future of the internet.

The internet architecture and its vulnerabilities

The internet consists of a layered and distributed architecture, starting at the physical level and then ending with users and applications. At the most fundamental level, the infrastructure includes hardware, physical infrastructure, interconnection, software, protocols, information services and human resources.

Networks, or autonomous systems, connect to components in the physical layers, carrying data via a set of protocols to the desired destination through logical addressing schemes. This enables operators to troubleshoot and take immediate action if problems arise as a delayed response could cause disruptions and severely affect the functionality of the internet. Between those layers, the internet is comprised of various components needed to ensure reliability, resilience and robustness.

At each level, various risks and vulnerabilities become apparent, which different actors can exploit to their advantage. These include, among others routing threats or attacks against the Domain Name System (DNS). The DNS-system represents one of the cornerstones of the internet as the system enables the translation of URLs into IP-addresses, creating a directory for every connected node, device, computer or resources available on the internet.

An attacker can exploit the system through DNS-hijacking or DNS-spoofing, whereby an attacker intercepts a user's DNS-request and redirects them to a compromised DNS-server or infects the user's device with malicious code through a phishing mail, infested link or other malicious activity. The malware then changes the victim's settings and redirects DNS-requests to the attacker's DNS-server. One such case was Roaming Mantis, which infected Android-based tablets and smartphones globally in 2018.⁴ Routing threats are just severe DNS-attacks as routers provide the basis for the robustness of the internet. An attacker can hi-jack, re-configure or intercept assigned numbers, addresses or namespaces to influence or undermine the operation of one or several interconnected networks.⁵

Moreover, threat actors can execute denial-of-service (DoS) attacks. DoS attacks are characterized by an explicit attempt by attackers to prevent legitimate use of a service. There are two general forms of DoS attacks, those that crash services and those that flood services. The most serious attacks are distributed (DDoS). In order to execute a DDoS attack, you need control of a large number of connected devices, which can be managed by a command and control centre (C&C). In a DDoS attack the goal is to make a device or network unavailable to its intended users. Attackers usually target sites or services hosted by high-profile web servers such as banks, credit card gateways, DNS name servers or root name servers. Targets of recent DDoS attacks include the DNS providers Cloudflare and Akamai, resulting in disrupted operability for the providers and all their customers. The biggest DDoS attack to date happened in

February 2018 when threat actors targeted GitHub, a platform popular for online code management and used by millions of developers. At its peak, the platform experienced 1.35 terabytes of traffic per second,⁶ which indicates what enormous power some threat actors can wield at any given time.

Furthermore, as the complexity and scale of the internet architecture deepen, so does the dependencies between open source, software development kits, scripting and programming frameworks, resulting in additional risks and vulnerabilities. What previously needed to be a complex, intensive and highly targeted operation by a threat actor can now be done with much less effort. Historically, you needed some type of insider to create a backdoor for an actor to gain access to an organization's network, which meant that each operation was labour intensive and very costly. Only nation-states had that capability and resources to execute such operation and, therefore, carefully selected their targets. One example is Backdoor Reign, which was an extremely complex backdoor Trojan used by nation-states to conduct surveillance activities against selected targets.⁷

In a recent report published by the company Synopsys, researchers discovered that approximately 77 per cent of the code-base in IoT-devices came from open-source components with an average of 677 vulnerabilities per application.⁸ As most software now is a mash-up of code from different libraries, and continuously being updated by developers via delivery models, it becomes difficult to audit and allows threat actors to insert malicious code into the environment. However, the positive effects of open-source software are the application of the 'many-eyes'-principles, which reduces the risk of security by obscurity in comparison with proprietary code, that is, closed source software.

As most software now is a mash-up of code from different libraries and is continuously being updated by developers via delivery models, it becomes difficult to audit and allows threat actors to insert malicious code into the environment.

Moreover, the threat of backdoors keeps expanding and now presents a real danger to organizations, businesses and governments alike. During the first half of 2018, 3.1 per cent of all attacks directed at industrial automation systems stemmed from backdoors, which was a 50 per cent increase from the previous year,⁹ and businesses saw a 173 per cent increase year-on-year for backdoor detections.¹⁰ Worrying examples of backdoor vulnerabilities had become particularly apparent since 2017 when WannaCry and NotPetya emerged and raised havoc around the world.

A hacker group named Shadow Brokers was taking advantage of hitting unpatched systems all over the globe with the WannaCry attack, which used an exploit known as 'EternalBlue', spread across 150 countries. The threat actors exploited vulnerabilities in Microsoft's SMBv1 server protocol, which affected not only Microsoft's operating systems such as Windows XP and Windows 10 but other systems running on Microsoft's SMBv1 server protocol.¹¹ The vulnerability allowed for an attacker to remotely execute arbitrary code on a targeted system by sending crafted messages to an SMBv1 server. Microsoft patched a number of the vulnerabilities in 2017, but patching was not performed as quickly as needed. And then the world was hit by NonPetya.¹²

As of yet, the majority of the world's governments have not spent enough time evaluating the security and risks of the internet infrastructure, leading to different

approaches and levels of security. Many governments are currently selling off or outsourcing large parts of their critical infrastructure without a thorough risk analysis of third parties and private actors, leaving them vulnerable to attacks that may disrupt critical societal services. This could potentially create a situation of uncertainty when assessing third parties and private actors as their goals and interests may not be aligned with the host country.

The fragility of the system becomes apparent when looking at the last two decades. Between the 1980s and the 1990s, the development of fibre-optic technologies and deregulation of the telecommunications market significantly changed how networks operated. As many fibre-optic cable projects became deregulated and privatized, the ventures focused on making a profit rather than meeting forecasted demand, affecting the resilience and robustness of providing an internet connection. If an undersea communication cable were to be tampered with, it could severely cripple a nation or an entire region's access to the World Wide Web and hamper their information warfare capability.¹³

Although it appears to be a redundancy of physical fibre-optic cables according to the Infrapedia's Network Atlas,¹⁴ they are usually hard to protect and prone to disruptions due to their visibility and coverage of large geographical areas. This vulnerability can be illustrated with the case of a Georgian woman accidentally cutting off the main fibre-optic cable connecting Armenia to the rest of the world when she was scavenging for scrap metal.¹⁵ As Georgia provides around 90 per cent of Armenia's internet, the consequences of this unintentional disruption were disastrous.

The interdependencies created between the internet and critical infrastructure make it susceptible to cyberwarfare. One example is the dependency between the internet and electrical power. The internet is dependent on electrical power for its functioning, and electrical power grids are dependent on the internet for their operability. Modernizing and automating electrical power grid networks via the internet produces a more efficient and cost-effective way of distributing power; however, it introduces several new vulnerabilities and risks that were non-existent decades ago. Several governments globally are now worried about cyberattacks targeting their power grids. According to a Wired article from 2009,¹⁶ China and Russia have successfully infiltrated the US electrical grid and implemented malicious software that could create massive outages and disrupt the US economy. One example of how devastating it can be was the blackout in Ukraine in 2015 and 2016.

We will most certainly need a new paradigm: We are all hacked. And act accordingly.

Cyberwarfare as a mean

The definition of cyberwarfare is highly contested internationally, as no single concept has been widely accepted. Several definitions have been proposed over the years, such as the 'actions by a nation-state to penetrate another nation's computer or networks for the purposes of causing damage or disruption'¹⁷ by Richard A. Clarke, a former US government official and National Coordinator for Security, Infrastructure Protection

and Counter-terrorism. Martin C. Libicki¹⁸ offers another explanation and defines it as two types, strategic and operational, where the strategic type is 'a campaign of cyberattacks one entity carries out on another', while the operational type 'involves the use of cyberattacks on the other side's military in the context of a physical war'. It can also be explained as the actions made by an actor to attack or attempt to damage an adversary's computer or information network through malicious code, targeting online control systems governing logical and physical networks.

As the internet becomes intertwined with states' national security, offensive and defence cyber strategies will shape the future internet for users and industry alike. Cyberspace is now considered to be the fifth domain of warfare, joining land, sea, air and space, but unlike the other domains, the conflicts in cyberspace will not be like traditional warfare. Instead, nation-states, criminal organizations, hacktivists¹⁹ and terrorist groups will utilize existing vulnerabilities in computer and network systems governing civilian populations and society as a whole. Actors will target all aspects of the internet infrastructure, including physical and logical infrastructure, internet service providers, to different platforms, data communication mediums and network equipment. As a result, nation-states around the globe have been developing cyber capabilities and engaged in cyber conflicts, including the United States, China, Russia, Israel, the United Kingdom, Iran and North Korea, making cyberwarfare an integrated part of their overall military strategy.

As societies become more digitalized, cyberwarfare as a means to achieve strategic goals has never been easier. Nation-states and criminal organizations alike can potentially use clandestine means within the cyberspace to attain secret information as exhibited by the United States' National Security Agency (NSA) tracking of cell phone conversations made in the Bahamas without the permission of the Bahamian government or the data breach against the US Office of Personnel, which was allegedly done by China.

Cyberspace also provides an excellent venue for sabotage, economic disruption and influence campaigns. The asymmetric nature of internet-based attacks makes it difficult to determine motivating factors and attribute the attack to a specific actor, producing an environment of uncertainty and whether a specific act can be considered as an act of war.

In mid-July 2010, security experts discovered a malicious software programme named Stuxnet, which had infiltrated computers at an Iranian nuclear facility delaying Iran's ability to develop a nuclear capability. The *New York Times* regarded the attack to be 'the first attack on critical infrastructure that sits at the foundation of modern economies'.²⁰ In 2017, the world experienced WannaCry and NotPetya, two cases of malicious code masquerading as ransomware, which severely affected the UK's National Health Service and the shipping company Maersk.²¹

Examples of influence campaigns with underlying cyberwarfare components can be seen in 2008 when Russia attacked the Georgian government website or when the Chinese attackers targeted the media company CNN as the company reported on Chinese repression in Tibet.

Stuxnet, WannaCry and NotPetya highlight not only the vulnerabilities of connecting critical infrastructure to the cyberspace but also how malware developers effectively

can influence global politics and governments by sharing exploits and developments to others. This allows lesser hackers to become proficient in executing large-scale attacks, which only a few were able to do previously. The sharing of information has also created a form of online arms proliferation as techniques and malware are being sold to the highest bidder through black markets.

According to Clarke, the civilian population is also at risk of being exposed to cyberattacks, noting that attackers have gone beyond stealing credit card numbers to also include attacks against societal services or the stock market.²² Cyberwarfare represents a multitude of threats as cyberattacks can have a supporting role in traditional warfare. Considering 'hard threats' and 'soft threats', a well-executed cyberattack can either enable the tampering with a country's air defence systems in order to facilitate an attack from the sky, cut off all power to a country or facilitate cyber espionage activities and influence campaigns.

Conclusion

With the increased threat of cyberattacks from nation-states, hackers and criminal organizations alike, it has started to affect the way the world views the internet. Inadequate management of cyber threats puts users at risk, erodes the trust in the platform and jeopardizes its ability to be a driver for economic and social innovation.

Misinformed and disproportionate government responses can potentially threaten internet freedom and create a climate of fear, uncertainty and doubt. The future of the internet and the continued growth of the platform will be determined by how governments and organizations collectively respond to the volume and scale of cyberattacks. As governments come under pressure to mitigate the effects of cyberattacks, there is a growing risk that online freedoms and global connectivity will be severely restricted in favour of national security. New models for incentives, accountability and liability are urgently needed to increase cybersecurity readiness, reduce vulnerabilities and to ensure end-user security. The complexity and scope of cyberattacks necessitate multi-stakeholder and expert-driven responses for the digital economy to continue to thrive and for the trust in the internet to be rebuilt.

Neither governments nor the private sector have the ability to deal with the scope and the scale of cyber threats alone. Due to the interconnected nature of the internet, actions made by lone stakeholders will do little to mitigate or eliminate cyber threats. Driven by the need to be seen as 'doing something' in the face of increasingly complex cyberattacks, it is expected that government responses to emerging cyber threats will be increasingly reactive. However, such reactive responses will not effectively mitigate the threat, but rather result in excessive overregulation. Effective action and network resilience against cyber threats can only emerge through information sharing, strategic thinking and collaborative efforts among stakeholders.

It is also important to emphasize that the way stakeholders adapt to future cyberattacks may change the internet from being a platform of openness and collaboration to a fragmented, closed and secure network environment. A fundamental

change to the architecture and the underlying principles of the internet could deliver a dystopian future of a secured walled garden, filtering access and with no encryption, anonymity or privacy. The national security of national states would overshadow the freedoms and rights we now take for granted, causing a struggle between perceived national security interests and end-user security measures.

The long-discussed need for a global culture on cybersecurity will take on new relevance and urgency as cybersecurity becomes the responsibility of everyone. No system will be immune to cyberattacks and cybercrime in the future, and these threats will affect all aspects of society. The idea that a 'network is only as strong as its weakest link' will take on a new meaning in a hyper-connected world, as connected devices can undermine an entire nation. It will become imperative to raise the awareness of the importance of security on all levels, either through security literacy or by developing secure connected devices. To meet the future needs, a market for security needs to be established in order to ensure overall network and device security. This can be done by either implementing liability models or improving governments' procurement practices.

Cyber governance can no longer remain solely in the hands of governments as the risk of being exposed to a cyberattack continuously increases. Much of the global internet infrastructure today are being developed, owned and maintained by private actors, and because of the complexity and scope of cyberattacks, governments alone are unable to provide inclusive and expert-driven regulatory responses, and thus need to encourage private actors to join the discussions on the future of the internet.

As cyberattacks become more advanced and a tool for nation-states to extract information, influence elections and disrupt critical infrastructure, the threat has grown to immense proportions. Private actors are now calling on governments to implement norms that would protect civilians in times of peace and are trying to encourage the international community to establish an international organization with the mandate to investigate state-sponsored cyberattacks. There are also calls for private tech-companies to pledge to protect their users from all cyberattacks regardless of origin and never assist a nation-state in carrying out offensive operations in cyberspace. Governments around the world will need to work together to fix software vulnerabilities – not stockpile them to use against each other.

Notes

- 1 Economist, 'The World's Most Valuable Source Is No Longer Oil, but Data', *The Economist*, 6 May 2019. <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>.
- 2 Samuel Flender, 'Data Is Not the New Oil: About the Reality of Working with Data', *Towards Data Science*, 10 February 2019. <https://towardsdatascience.com/data-is-not-the-new-oil-bdb31f61bc2d>.
- 3 Dave Weinstein, 'Stop Saying "Digital Pearl Harbor"', *DARKReading*, 2 October 2018. <https://www.darkreading.com/threat-intelligence/stop-saying-digital-pearl-harbor/a/d-id/1332932>.

- 4 Suguru Ishimaru, 'Roaming Mantis Uses DNS Hacking to Infect Android Smartphones', *Kaspersky*, 16 April 2018. <https://securelist.com/roaming-mantis-uses-dns-hijacking-to-infect-android-smartphones/85178/>; Suguru Ishimaru, 'Roaming Mantis Dabbles in Mining and Phishing Multilingually', *Kaspersky*, 18 May 2018. <https://securelist.com/roaming-mantis-dabbles-in-mining-and-phishing-multilingually/85607/>; National Cyber Security Center, 'DNS Hacking Activity', 25 January 2019. <https://www.ncsc.gov.uk/news/alert-dns-hijacking-activity>.
- 5 RFC 4593, Generic threats to routing protocols. <https://tools.ietf.org/html/rfc4593>.
- 6 Lily Newman Hay, 'GitHub Survived the Biggest DDOS Attack Ever Recorded', *The Wired*, 1 March 2018. <https://www.wired.com/story/github-ddos-memcached/>.
- 7 Symantec Security Response, 'Reign: Top-Tier Espionage Tool Enables Stealthy Surveillance', 23 November 2014. <https://www.symantec.com/connect/blogs/regin-top-tier-espionage-tool-enables-stealthy-surveillance>.
- 8 Taylor Armerding, 'The Future of Open Source Software: More of Everything', Synopsys, 24 January 2019. <https://www.synopsys.com/blogs/software-security/future-of-open-source-predictions/>.
- 9 Kaspersky Labs ICS-CERT, *Threat Landscape for Industrial Automation Systems H1 2019*, 30 September 2019. <https://ics-cert.kaspersky.com/reports/2019/09/30/threat-landscape-for-industrial-automation-systems-h1-2019/>.
- 10 Malwarebytes Labs, *2019 State of Malware*, 2019. <https://resources.malwarebytes.com/files/2019/01/Malwarebytes-Labs-2019-State-of-Malware-Report-2.pdf>.
- 11 SentinelOne, 'EternalBlue: The NSA-Developed Exploit that Just Won't Die', *SentinelOne*, 27 May 2019. <https://www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die/>.
- 12 Pradeep Kulkarni, Sameer Patil, Prashant Kadam and Aniruddha Dolas, 'EternalBlue: A Prominent Threat Actor of 2017–2018', *Virus Bulletin*. <https://www.virusbulletin.com/virusbulletin/2018/06/eternalblue-prominent-threat-actor-20172018/>.
- 13 Nicole Starosielski, *The Undersea Network* (Durham: Duke University Press, 2015). See also NATO CCDCOE, 'Strategic Importance of, and Dependence on, Undersea Cables', November 2019; John Filitz, 'Undersea Fiber-Optic Cable Security – Threats from Below', *Stable Sea*, 27 March 2019.
- 14 Infrapedia, <https://www.infrapedia.com/>.
- 15 Tom Parfitt, 'Georgian Woman Cuts Off Web Access to Whole of Armenia', *The Guardian*, 6 April 2011. <https://www.theguardian.com/world/2011/apr/06/georgian-woman-cuts-web-access>.
- 16 Wired, 'China and Russia vs. US Grid!', *Wired*, 4 August 2009. <https://www.wired.com/2009/04/china-and-russi/>.
- 17 Richard A. Clarke, *Cyber War* (New York: HarperCollins, 2010), 6. See also Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York: PublicAffairs, 2017); Kaplan Fred, *Dark Territory: The Secret History of Cyber War* (New York: Simon and Schuster, 2017); Robert Clarke and Robert E. Knake, *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats* (New York: Penguin Press, 2019).
- 18 Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND Corporation, 2009), 8. See also Jonathan William Welburn et al., 'Cyber Deterrence: How We Learned to Stop Worrying and Love the Signal', *Rand National Security Research Division*, July 2019; Jaspar Scott, *Strategic Cyber Deterrence: The Active Cyber Defense Option* (Lanham: Rowman and Littlefield, 2017).

- 19 Hacktivists use cyberattacks to promote a certain political or societal agenda. These attacks can easily be mistaken as cyberwarfare as they utilize their knowledge of computers and software tools to gain unauthorized access to computer systems to sabotage, manipulate or destroy information, in order to draw attention to their cause. Hacktivist groups such as Anonymous are often labelled as cyber-terrorists by the media as they deface websites, post sensitive information and threat to conduct further attacks if their demands are not met.
- 20 Riva Richmond, 'Malware Hits Computerized Industrial Equipment', *New York Times*, 24 September 2010. <https://bits.blogs.nytimes.com/2010/09/24/malware-hits-computerized-industrial-equipment/>.
- 21 Andy Greenberg, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History', 22 August 2018. <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>.
- 22 Clarke, *Cyber War*.