SECURITY AND TECHNOLOGY PROGRAMME

Stemming the Exploitation of ICT Threats and Vulnerabilities

An Overview of Current Trends, Enabling Dynamics and Private Sector Responses

Camino Kavanagh

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

ACKNOWLEDGEMENTS

UNIDIR acknowledges the generous support received from the Government of France to conduct this research.

The author would like to thank to Evgeny Scherbakov (Ph.D candidate, King's College London and Research Associate, International Programme, Carnegie Corporation of New York), Nicolas Mazzucchi (Research Director, Fondation pour la recherche stratégique), and Ashley Sweetman (PhD Candidate, King's College London) for their contributions to this research, as well as Madeline Carr (University College London), John Mallery (MIT), Nathalie Van Raemdonck (EUISS), Oleg Demidov and Kerstin Vignard (UNIDIR) for reviewing different iterations of this report.

ABOUT THE AUTHOR

Dr. Camino Kavanagh is a non-resident researcher at UNIDIR and a Visiting Fellow at the Department of War Studies, King's College London. She also works as an independent consultant.

Kavanagh served as consultant to the 2016–2017 United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and lead consultant to the Organization for Security and Co-operation in Europe on an initiative relating to confidence-building measures, conflict prevention and information and communications technology (ICT). Beyond current consultancy projects with organizations such as the United Nations and the Organization of American States, she is involved in a number of policy and research initiatives on ICT and emerging technologies as they relate to conflict, terrorism and crime.

Kavanagh received her PhD from the Department of War Studies, King's College London, in 2016 and focused on information technology, sovereignty and the State, a topic that remains a core focus of her research activities.

ABOUT THE INSTITUTE

The United Nations Institute for Disarmament Research (UNIDIR) is an autonomous institution within the United Nations that conducts independent research on disarmament and related problems, particularly international security issues. The vision of UNIDIR is a stable and more secure world in which States and people are protected from threats of arms-related violence. The role of UNIDIR is to support Member States, the United Nations and policy and research communities in advancing ideas and actions that contribute to a more sustainable and peaceful world.

NOTE

CONTENTS

EXECUTIVE SUMMARY

What are the recent trends in threats and vulnerabilities and how are they being exploited? What are the dynamics that enable the spread of these threats and vulnerabilities? And what steps are the private sector—technology companies in particular—taking to tackle these threats and vulnerabilities, stem their spread and manage or counter some of the enabling dynamics?

As we approach the end of the second decade of the twenty-first century and as our societies—and our conflicts—become more dependent on digital technologies, private technology companies undoubtedly have roles and responsibilities to play in shaping and implementing international security policy. This is certainly the case when it comes to stemming the spread of information and communications technology (ICT)-related threats and vulnerabilities, the exploitation of which increasingly have a bearing on national and international security matters.

The first section of this report focuses on current trends in ICT threats and vulnerabilities and their relation to national security. It highlights the most predominant tools used by attack groups and the security vulnerabilities exploited to this end. The second section discusses some of the dynamics that continue to enable the spread of malicious tools and techniques. These include criminal/black market dynamics, geopolitical and national security dynamics, and dynamics relating to the actual IT market itself. Discussions of these different enabling dynamics have been underway for some time and go to the heart of public policy making, yet responses to date, both public and private, appear to fall short. The final section discusses how the technology sector is responding to the threats and vulnerabilities discussed in the report, approaching the question from the perspective of *reactive* and *productive* responses: the former more operational in character, the latter more normative and gaining significant currency as certain companies seek to influence State and industry behaviours in order to protect their interests and, by extension, their users.

The main findings of the policy brief suggest that, first, there is an urgent need to determine whether *additional public and private structural levers* are required to manage the scale and scope of ICT threats and vulnerabilities and the associated enabling dynamics. This includes those levers that can ensure greater security in the design and development of digital products and services, as well as those that can more effectively address the criminal, geopolitical/national security and IT market dynamics discussed in the paper.

Second, we need better mechanisms for *deepening reflection on, and the transparency of*, *the different industry-backed initiatives* aimed at responding to ICT threats and vulnerabilities currently being implemented or proposed. Such an approach would

contribute to building trust, convincing users, governments and other affected parties of the value of the initiatives. It might also help identify existing and emerging loopholes in current policy, regulation and practice, which in turn can help determine whether additional structural levers, including regulation or legislation, are actually required or not, as well as inform or contribute to international and regional inter-governmental processes.

Finally, the brief calls on both public and private actors to ensure their responses remain tethered to the greater common good as a means to strengthen international peace and security. Although this recommendation is particularly complicated given the current state of international affairs, it is one that should be given priority.

INTRODUCTION

Over the past decades the private sector has become increasingly relevant to international security policy. This is due to a number of factors. First, globalization and the resulting increase in transnational flows of capital, goods, services, people and information, has challenged the role of the State on several fronts. The private sector in particular, has assumed new roles and expanded its normative influence. Second, the character of modern conflict means that businesses across the globe are increasingly affected by political-military crises and in many instances, their operations are exposed to high risk. Equally, it is well-documented that private sector companies can also cause or enable conflict through their own behaviours.

Evidently, it is difficult to discuss the 'private sector' in generic terms, not least because it means different things to different actors. In many instances the lines between private and State actors is becoming increasingly blurred. This is particularly the case in matters relating to digital technologies and international security. Moreover, the extant or potential roles that private sector actors assume in this area will more often than not be strongly influenced by national and jurisdictional factors as well as size, scope, culture, and relationship with the State in which they operate.

This policy paper is principally concerned with private technology companies and their response to information and communications technology (ICT)-related threats and vulnerabilities stemming from or associated with their products and services. As our societies have become increasingly dependent on ICT, technology companies have become highly influential and powerful actors, with some reporting profits that can dwarf the economy of many countries across the globe. In many instances and contexts, these companies complement, if not replace, traditional functions of the State. However, their products, services and infrastructure are also becoming central to inter-state conflict, as are the companies themselves.

With greater power comes greater responsibility, particularly in the realm of international security. In this regard, several international and regional inter-governmental processes have recognized the importance of engaging the private sector in matters relating to ICT and international security and stability. For instance, the United Nations Groups of Governmental Experts (GGEs) on Developments in the Field of Information and Telecommunications in the Context of International Security have warned of the risks accompanying the immense economic opportunities driven by ICT. They have, however, also highlighted the need to engage the private sector in the cooperative and trust-building responses to ICT-related threats and vulnerabilities that are formulated at national and international levels. So, too, has the Organization for Security and Co-

operation in Europe (OSCE) in its work on confidence building measures. Meanwhile, seeking to claim their space, private sector actors have directly engaged in initiatives such as the Global Commission on the Stability of Cyberspace, helping to both identify emerging challenges and participate in shaping and implementing responses.

As part of UNIDIR's research into the extant and emerging roles of the private sector in international security policy, this policy brief identifies current trends in ICT threats and vulnerabilities and highlights some of the worrying dynamics—criminal, geopolitical/national security and IT market dynamics—enabling the persistence of these threats and vulnerabilities and their exploitation.

The policy brief concludes with some observations on the roles of technology companies in responding to these trends and enabling factors. Drawing extensively on desk research, it provides a sample of the roles that some technology companies are assuming to shape the behaviours of different actors as well as the IT market itself. In this regard, the concluding section questions whether self-regulation and the recent expansion of principled declaratory initiatives involving the technology sector are sufficient to manage the scope and scale of the challenges and risks at hand. Or, perhaps, it is time for greater and more responsible investment in the necessary structural levers (technical, political, regulatory and financial) to ensure greater security in the design, development and use of IT products and services. Deeper discussion on (and transparency of) the impact of existing self-regulatory initiatives would likely go a long way in helping identify existing gaps, while also helping inform and contribute to inter-governmental processes such as the up-coming Open-Ended Working Group and the Group of Governmental Experts.

CURRENT TRENDS IN THREATS AND VULNERABILITIES

Today's ICT environment is characterized by "ubiquitous connectivity between heterogenous networks and diverse systems and devices".[1] This shared, highly complex and interconnected space supporting multiple models of use, connectivity and access has become a vital substrate for economic, social, cultural and political interactions across the globe.[2] While the benefits are significant, so too are the risks to the global economy, individual privacy and the maintenance of international peace and security. And central to these risks are ICT flaws and vulnerabilities that different actors exploit—often in highly creative ways—for malicious purpose, as well as the challenges to stemming such behaviour.[3] This section discusses some current trends in threats and vulnerabilities and how they are being exploited, particularly those that have (or may have) a bearing on international security.

The exploding demand for interconnectivity, integration and platform compatibility makes hardware and software both more complex and more homogenous. These characteristics expand the potential for cyber threats to become more widespread, presenting serious challenges to both industry actors and governments, with the main costs borne by users.

Over the past decade, a number of groups have devised detailed models, taxonomies or frameworks for categorizing different cyber threats and trends. They represent a spectrum of approaches and methodologies used by government entities,[4] regional organizations,[5]

---

[1] C. Vishik, M. Matsubara and A. Plonk, "Key Concepts in Cybersecurity: Towards a Common Policy and Technology Context", in H. Roygas and A. Osula (eds), *International Cyber Norms: Policy, Legal, and Industry Perspective*, 2016.

[2] C. Demchak, "Resilience, Disruption, and a Cyber Westphalia: Options for National Security in a Cybered Conflict World", in N. Burns and J. Price (eds), *Securing Cyberspace: A New Domain for National Security*, 2012; J.S. Nye Jr., "Normative Restraints on Cyber Conflict", Belfer Center for Science and International Affairs, 2018.

[3] The United Nations Group of Governmental Experts on ICT in the Context of International Security identified this risk in its 2015 report, recommending that "States … seek to prevent the proliferation of malicious ICT tools and techniques". While these and other normative recommendations were directed at States, industry actors and their actions are key to its implementation.

[4] For example, the cybersecurity authorities of Australia, Canada, New Zealand, the United Kingdom and the United States (the so-called 'Five Eyes') recently published a report in which they outlined five publicly available and commonly used tools and techniques used for malicious purpose in recent cyber incidents around the world. They include remote access trojans (RATs), web shells, credential stealers, lateral movement frameworks, and command and control obfuscation tools. The report provides an overview of the threat posed by each tool, along with insight into where and when it has been deployed by hostile actors. Measures to aid detection and limit the effectiveness of each tool are also described. The report concludes with general advice for improving network defence practices. See *Joint Report on Publicly Available Hacking Tools: Limiting the Effectiveness of Tools Commonly Used by Malicious Actors*, October 2018, https://www.ncsc.gov.uk/joint-report.

[5] The European Union Agency for Network and Information Security (ENISA), for instance, has developed its Threat Taxonomy, and produces an annual Threat Landscape Report. The ENISA model, for instance, uses the following structure to describe cyberthreats: a short description of the cyberthreat as it has manifested during the reporting period; a list of interesting points with remarkable observations for the specific cyberthreat; trends and main statistics including geographical information; top incidents within the specific threat category; specific attack vectors used to launch the threat; specific mitigation actions; kill chain for the specific cyberthreat; and authoritative references. See "ENISA Threat Landscape Report 2019", https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape.

private sector companies and associations, as well as technical bodies.[6] Major cybersecurity companies such as Symantec, Trend Micro, Kaspersky Lab and others also produce their own analysis of current trends and breakdown of cyber threats.

Recent threat trends include malware, web-based and web-application attacks, phishing, denial or distributed denial of service, spam, botnets, data breaches, ransomware, and cyber espionage.[7]

Malware, defined by the International Telecommunication Union as "software which intentionally performs actions which can damage data or disrupt systems",[8] continues to be a prevalent tool used by attack groups ("sets of related intrusion activity that are tracked by a common name in the security community").[9] There are many types of malware, which can be broken down into 'families' such as ransomware, cryptojacking, botnets, remote access trojans (RATs), backdoors, etc.

Oftentimes, security vulnerabilities are availed of to deploy such tools. Vulnerabilities refer to weaknesses in operating systems, applications or hardware, or weaknesses enabled by humans or organizations themselves either knowingly or unwittingly. An exploit, in turn, is a software tool designed to take advantage of a security vulnerability to compromise the confidentiality, integrity and availability of the affected systems via the injection of different tools such as malware. The latter can generate broader effects across the ICT network or the monitoring and control of cyber–physical processes (via so-called Operational Technology).[10] Sometimes, however, the objective of an exploit is to simply demonstrate the actual existence of the vulnerability.

The principal threat actor groups operating in 2017–2018 include criminal groups (and increasingly organized criminal groups), States, insiders (be they malicious, negligent or compromised), terrorists, hacktivists, and script kiddies.

The following provides a sample of some of the threats and attack tools, techniques, exploits and attack vectors that have recently been in the headlines.

---

[6] For example, see Common Attack Pattern Enumeration and Classification (CAPEC) framework by MITRE Corporation (https://capec.mitre.org/), Open Threat Taxonomy by Enclave Security (https://www.auditscripts.com/resources/open_threat_taxonomy_v1.1a.pdf), A Taxonomy of Operational Cyber Security Risks by Carnegie Mellon University (https://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_91026.pdf) and others.

[7] For an example of a recent trend analysis, see ENISA, *Threat Landscape Report 2018*, 2019, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018.

[8] ITU, "Definitions of terms related to quality of service", Recommendation ITU-T E.800, 2008, p. 10, https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.800-200809-I!!PDF-E&type=items.

[9] As discussed by MITRE, there are variations of the term 'attack group' terms such as 'threat groups, activity groups, threat actors, intrusion sets, and campaigns'. Analysts use different methodologies to "track clusters of activities" and assign one or other of these terms to those responsible. Sometimes, certain groups are assigned "multiple names associated with similar activities due to various organizations tracking similar activities by different names". How one organization defines a group can result in a partial overlap with how another organization designates a group. Furthermore, disagreement on designations and specific activities might also emerge. See MITRE Att&ck's explanatory note on 'Groups', https://attack.mitre.org/groups/.

[10] GFCE, "Coordinated Vulnerability Disclosure", 2016, https://www.thegfce.com/initiatives/r/responsible-disclosure-initiative-ethical-hacking.

Zero-day exploits

One of the malicious techniques receiving most attention in recent years involves the 'zero-day exploit' (commonly called 'zero days'), an informal term used to describe an exploit of a vulnerability in software not yet known to the software vendor, manufacturer or end user. The non-disclosure of zero-days is often perceived to pose the most risk: if they are not responsibly reported to the vendor or manufacturer, they can be discovered and used by other actors (governmental or non-governmental).

Some claim that the Stuxnet virus used to attack the Natanz nuclear facility in Iran was the first publicly documented use of a zero-day exploit by a State to target the assets of another State. Government agencies have demonstrated a keen interest in zero-day vulnerabilities, and are investing significant resources to discover, retain and exploit them. However, until recently this has generally taken place absent a process "to properly consider the trade-offs".[11] Attack groups use these exploits to launch a wide range of operations, resulting in increasing levels of disruption at significant cost to the global economy and a growing source of tension between States.[12] According to a number of sources, however, the number of zero-days has reportedly dropped since 2017, allegedly due to reduced availability. This has not, however, stopped overall targeted activity.[13]

Ransomware (and wiper attacks disguised as ransomware)

Simply put, ransomware attacks use advanced cryptography to lock a user's device and access to the data on the until a ransom is paid. Wiper attacks, in contrast, are generally not designed for financial gain but rather use the guise of a ransom attack to irreparably wipe data from a device. Ransomware attacks have been around for some time although the Locky attack in 2016 received particular attention as it successfully extracted a USD 17,000 ransom from a hospital in the United States. In addition, designers of the Locky malware regularly updated it to avoid detection and included innovative functionalities such as a multilingual ransom demand capacities. The scale, scope and effects of ransomware attacks increased in 2017, exemplified by the headline-generating Wannacry and Petya attacks.

---

[11] K. Charlet, S. Romanosky and B. Thomson, "It's Time for the International Community to Get Serious about Vulnerability Equities", lawfareblog.com, 15 November, 2017, https://www.lawfareblog.com/its-time-international-community-get-serious-about-vulnerability-equities; P. Stockton and M. Golabek-Goldman, "Curbing the Market for Cyber Weapons", *Yale Law and Policy Review*, vol. 32, no. 1, 2013.

[12] For instance, the US Council of Economic Advisors calculated the cost of malicious cyberactivity cost the US economy between USD 57 billion and USD 107 billion in 2016; see "The Cost of Malicious Cyber Activity to the US Economy", February 2018, https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

[13] ENISA, *Threat Landscape Report 2018*, 2019, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018; Symantec, "2019 Internet Security Threat Report", https://www.symantec.com/security-center/threat-report.

WannaCry was particularly ruthless, targeting vulnerabilities in the Microsoft Windows operating systems by encrypting data and demanding ransom payments in Bitcoin cryptocurrency. It used two powerful exploits: EternalBlue and DoublePulsar. The first, EternalBlue, refers to an exploit created by the US National Security Agency (NSA) and subsequently leaked following a data breach earlier in 2017.[14] This particular exploit was designed to take advantage of a vulnerability the NSA discovered (and did not report) in a particular Windows protocol—the Server Message Block—giving hackers "free rein to remotely run their own code on any unpatched machine".[15] The other tool—DoublePulsar, a backdoor implant also created by the NSA—was then used to install and execute the ransomware code.

Microsoft had released patches for these vulnerabilities prior to the propagation of the exploits, but many of the affected organizations had not applied them or were using legacy or pirated Windows systems. In some cases, for instance within the UK National Health System trusts, Microsoft's extended support for XP users agreed in 2014 expired a year later with many machines left unsupported.[16] In others, the "backdoors" installed via the DoublePulsar exploit also undercut mitigation efforts.

The NotPetya attack in 2017 is the best-known example of a wiper attack. Using a variant of the Petya ransomware, the malware involved in NotPetya was propagated through two very powerful vulnerability exploits: the same EternalBlue exploit used in the WannaCry attack, combined with a credential-stealing exploit called Mimikatz. The Mimikatz exploit was created as a proof-of-concept by a French security researcher to demonstrate password-related flaws in Windows systems. It could be used to pull passwords out of RAM and use them to hack into other machines—including on multiuser networks—that could be accessed with the same credentials.[17] This gave attackers the possibility to "infiltrate a target, exfiltrate massive amounts of data, encrypt the original data, and hold the stolen data for a bigger ransom".[18] NotPetya effectively improved on the original Petya ransomware's capability of encrypting the Master Boot Record by also encrypting the Master File Table and deleting the key. This in effect, rendered the ransomware a 'wiper', allowing it to overwrite and ultimately wipe—that is, erase—the affected system's hard drive. By targeting legitimate Ukrainian accounting software as the point of entry, harvesting Server Message Block and user credentials from the infected host and leveraging them to connect to other systems on the network, the malware quickly

[14] A. Greenberg, "The Untold Story of NotPetya, The Most Devastating Cyberattack in History', *Wired*, 22 August 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
[15] Ibid.
[16] S. Trendall, "NHS £150m Microsoft deal will banish Windows XP", PublicTechnology.Net, 22 May 2018, https://www.publictechnology.net/articles/news/nhs-£150m-microsoft-deal-will-banish-windows-xp.
[17] Ibid.
[18] Trend Micro, "Midyear Security Roundup: The Cost of Compromise", 2017, https://documents.trendmicro.com/assets/rpt/rpt-2017-midyear-security-roundup-the-cost-of-compromise.pdf.

propagated across corporate networks to deploy its malicious payload, with crippling costs to companies across the globe.[19]

The number of ransomware attacks reportedly decreased in 2018, superseded by newer threats such as cryptojacking (the unauthorized use of a device to mine cyptocurrency).[20]

Supply chain attacks

The supply chain for the IT market is complex, involving hardware and software, as well as the humans and their organizations that manage the design, production, shipping, installation and maintenance of products and services. The long and complex global supply chain presents a wide range of opportunities for the insertion of malicious tools and it is exponentially more complex in interconnected, nested Internet of Things (IoT) systems.[21]

Software supply chain attacks in particular are on the rise, with Symantec reporting a 78 per cent increase in 2018 alone.[22] These kinds of attacks "compromis[e] software code through cyberattacks, insider threats, other close access activities at any phase of the supply chain to infect an unsuspecting customer".[23] In their simplest form, the aim is to modify a product's trusted codebase to insert malware early in the cycle before the code is compiled or electronically signed,[24] or to corrupt a vendor's patch site with malware designed to impersonate authorized patch codes (including security updates), thus evading, in many cases, anti-virus and anti-malware programs. Once inserted, the malware usually serves as the basis for further exploits, able to subvert a large number of computers (and their processes and products) with just the single attack.[25]

Software developers are a key source of supply chain attacks, in that attackers "steal credentials for version control tools" or "compromise[e] third-party libraries that are integrated into larger software projects".[26] These kinds of attacks are used for extortion, or to exfiltrate, manipulate and destroy data for criminal or strategic purpose.

---

[19] Symantec, "2019 Internet Security Threat Report", https://www.symantec.com/security-center/threat-report. See also "NotPetya Technical Analysis", LogRythm Labs, July 2017, https://logrhythm.com/pdfs/threat-intelligence-reports/notpetya-technical-analysis-threat-intelligence-report.pdf.

[20] ENISA, *Threat Landscape Report 2018*, 2019, see p. 115 for a visualization of the current threat landscape, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018.

[21] Lloyd's, "Networked World: Risks and Opportunities in the Internet of Things", https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/networked-world.

[22] Symantec, "Internet Security Threat Report", 2019, https://img03.en25.com/Web/Symantec/%7B1a7cfc98-319b-4b97-88a7-1306a3539445%7D_ISTR_24_2019_en.pdf?aid=elq_19296.

[23] NIS CSIRT, "Supply Chain Attacks", https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/ssca/2017-winter/NCSC_Placemat.pdf.

[24] Ibid.

[25] Ibid.

[26] Ibid.

Beyond software, attackers may also target ICT physical infrastructure such as microchips and routers during the manufacturing process, installing secret chips or exploits which become difficult to detect as they move down the supply chain because the hardware has been electronically signed by the manufacturer. Officials in the United States have been claiming for several years that the Chinese government has installed surveillance chips on ICT hardware sold by its major global firms; some suggest that US National Security Agency may have been doing the same thing.[27]

Furthermore, recent reports of a large-scale campaign to install hardware backdoors in servers assembled in China for a US company[28] illustrate the growing global concern about threats to supply chain integrity. Even though the media reports were controversial and officially denied by both the alleged perpetrator and victims,[29] the news still sent shockwaves through the IT markets and negatively impacted the share prices of Chinese technology companies due to the fear of losing access to US markets.[30] Current allegations that 5G mobile equipment developed by Chinese telecommunications giant Huawei could be used by the Chinese government for spying purposes has intensified debates on supply chain security and resilience.[31]

Routing attacks

Internet Protocol (IP) routing underpins the Internet and plays a central role in the reliable functioning of the Internet. Routing ensures "that emails reach the right recipients, e-commerce sites remain operational, and e-government services continue to serve citizens".[32] Yet, despite the number of routing best practices that have emerged, routing security remains a major challenge. The scope and scale of routing incidents is increasing annually, resulting in significant economic harms.[33]

The most common type of routing incident involves attacks against internet services, particularly Border Gateway Protocol (BGP) hijacking attacks.[34] BGP hijacking can cause

---

[27] G. Greenwald, "How the NSA Tampers with US-made Internet Routers', *The Guardian*, 12 May 2014, https://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden.

[28] J. Robertson and M. Riley, "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies", *Bloomberg*, 4 October 2018, https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.

[29] G. Faulconbridge and J. Menn, "UK Cyber Security Agency Backs Apple, Amazon China Hack Denials", *Reuters*, 5 October 2018, https://www.reuters.com/article/us-china-cyber-britain/uk-cyber-security-agency-backs-apple-amazon-china-hack-denials-idUSKCN1MF1DN; BBC News, "Amazon and Apple Deny China Hack Claims", 5 October 2018, https://www.bbc.com/news/technology-45757531.

[30] The Straits Times, "Chinese Tech Firms' Shares Dive after 'Spy Chip' Report", 6 October 2018, https://www.straitstimes.com/business/companies-markets/chinese-tech-firms-shares-dive-after-spy-chip-report.

[31] R. Cellan-Jones, "Huawei and 5G: Decision Time", *BBC News*, 8 February 2019, https://www.bbc.com/news/technology-47160725.

[32] The Internet Society, "Routing Security for Policy Makers: An Internet Society White Paper", October 2018, https://www.internetsociety.org/wp-content/uploads/2018/10/Routing-Security-for-Policymakers-EN.pdf.

[33] Ibid.

[34] BGP governs how communications are routed over different autonomous systems (i.e., a large network or group of networks managed by a single organization) allowing traffic to travel from one network address to another as efficiently as possible.

internet traffic to go the wrong way, be monitored or intercepted, 'black holed' (in that it goes nowhere), or directed to fake websites as part of a man-in-the-middle attack[35]. BGP hijacking, or the network of an autonomous system that practices BGP hijacking, can also be used to spoof legitimate IP addresses for spamming purposes to leak or steal data.

In 2017 alone, the Internet Society reported just under 14,000 router-related outages or attacks such as route hijacks or leaks.[36] Some of these attacks also affected encrypted technology. For instance, the Enthralled exploit, discovered in April 2018, hijacked an insecure SSL certificate to redirect Ethereum users to a server which emptied their encrypted wallet.[37] They can also be leveraged for botnetting purposes whereby a number of Internet-connected devices are hijacked and coordinated to perform a specific task, including distributed denial of services attacks. Indeed, in 2018, Akamai, the cloud service provider and content delivery network, reported that the EternalBlue vulnerability was now being used to compromise some 45,000 routers. Attackers had apparently compromised the routers by "targeting vulnerable implementations of Universal Plug and Play (UPnP), a widely used [and widely hacked] protocol that enables devices to automatically recognize each other across a local network", infecting hundreds of thousands of devices. The objective of the attack was unclear, but researchers were concerned that the infected routers could be used for ransomware attacks or to gain "a persistent foothold on the network" for later exploitation.[38]

Reports for 2019 will likely highlight the recent trend in Domain Name System (DNS) hijacking attacks for espionage purposes. ICANN (the global multi-stakeholder body responsible for coordinating the Internet DNS, IP addresses and autonomous system numbers), the US government and several private companies issued alerts in February 2019 relating to a serious DNS system-related espionage threat. Reportedly, attackers had hijacked DNS servers used by governments and private companies, redirecting troves of sensitive email and VPN traffic to an internet address they controlled. As noted by security researcher Brian Krebs, the DNS hijacks also allowed attackers to obtain SSL encryption certificates for the targeted domains, in turn allowing them "to decrypt the intercepted email and VPN credentials and view them in plain text". Security researchers have associated the so-called 'DNSpionage campaign' with Iranian hackers. According to ICANN, mitigation efforts were difficult since DNS infrastructure is "rarely monitored for

[35] Man-in-the-middle attacks are a common form of cyberattack allowing attackers to either eavesdrop or modify communications between two legitimately communicating hosts.

[36] A. Robachhevsky, "14,000 Incidents: A 2017 Routing Security Year in Review", Internet Society, 9 January 2018, https://www.internetsociety.org/blog/2018/01/14000-incidents-2017-routing-security-year-review/.

[37] Microsoft, "The Cybersecurity Tech Accord Endorses the MANRS Initiative, Joining Efforts to Eliminate the Most Common Threats to the Internet's Routing System", 9 August 2018, https://cybertechaccord.org/cybersecurity-tech-accord-endorses-manrs/.

[38] Akamai, "UPnProxy: EternalSilence", 28 November 2018, https://blogs.akamai.com/sitr/2018/11/upnproxy-eternalsilence.html.

suspicious changes" and organizations seldom follow existing good practices that would make hijacking a target's domains or DNS infrastructure much more difficult.[39]

IoT-related attacks

The Internet of Things refers to a vast range of devices—from simple sensors to smartphones, home appliances and wearables—connected to the Internet, which collect data and use that data to operate through a range of products and services.[40] IoT attacks can be analysed from different perspectives. For instance, they can relate to network attacks that use different tools to exploit vulnerabilities in IoT networked devices, disrupting them offline or aggregating them into botnets to attack further targets. These kinds of attacks are usually associated with manipulation or disruption of network traffic.

Take, for instance, the Mirai malware which infects smart devices that run on certain processors. This self-propagating botnet is one of the most well-known IoT-related viruses and continues to affect devices across the globe. The botnet 'enslaved' scores of different types of hacked IoT devices (routers, security cameras and digital video recorders) vulnerable to hacking due to weak, default or hard-coded passwords.[41] While the initial attack in 2016 was eventually halted, the source code was publicly released and elements of it used in other botnet attacks, including the massive one that collapsed the domain registration services provider, Dyn, just a few months later. According to Symantec, attack groups have since developed numerous variants of Mirai and are "persistently adding new exploits to increase the success rate for infection, as devices often remain unpatched".[42] The subsequent discovery of the VPNFilter malware in 2018, and later models (e.g., Ssler), suggest the scale and variability of disruption that can be generated by IoT-related threats and vulnerabilities.[43]

Other types of IoT attacks include those targeting cloud-assisted IoT-based supervisory control and data acquisition (SCADA) systems or the industrial control systems (ICS) of various facilities, engineering and manufacturing systems or infrastructure objects, all of which are increasingly connected on the Internet, predominantly through IoT-based

---

[39] "Deep Dive on the Recent Widespread DNS Hijacking Attacks", February 2019, https://krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-dns-hijacking-attacks/.

[40] M. Burgess, "What is the Internet of Things? Wired Explains", *Wired*, 16 February 2018, https://www.wired.co.uk/article/internet-of-things-what-is-explained-iot; see also Lloyd's, "Networked World: Risks and Opportunities in the Internet of Things", https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/networked-world.

[41] "KrebsOnSecurity Hit with Record DDoS", 21 September 2016, *https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/*.

[42] Symantec, "Internet Security Threat Report", 2019, https://img03.en25.com/Web/Symantec/%7B1a7cfc98-319b-4b97-88a7-1306a3539445%7D_ISTR_24_2019_en.pdf?aid=elq_19296

[43] According to Symantec, VPNFilter is the "first widespread persistent IoT threat". It affected more than 500,000 routers across 54 countries and included a number of "potent payloads". Symantec, "Internet Security Threat Report", 2019, p. 20, https://img03.en25.com/Web/Symantec/%7B1a7cfc98-319b-4b97-88a7-1306a3539445%7D_ISTR_24_2019_en.pdf?aid=elq_19296.

solutions. Such activities go beyond mere network disruption and, in an increasing number of cases, involve a convergence with cyber–physical attacks.[44] Undoubtedly, the near-total digitalization of critical infrastructure process control systems will continue to be problematic. Furnaces, cooling systems, centrifuges, air traffic control lights, power generators and many other critical systems are now operated with the help of digital systems. With smart and efficient interconnected digital ICS, converging cyber–IoT threats are now evident at the process control level whereby cyberattacks can target IoT devices generating real physical effect, and greatly extending the attack perimeter as new vulnerabilities are identified for exploitation.

Design flaw exploits

In January 2018, academic and security researchers discovered two vulnerabilities—Spectre and Meltdown—enabled by security flaws that abuse speculative execution in processing chips from leading manufacturers such as Intel, AMD, and ARM.[45] Meltdown, a security vulnerability that "basically melts security boundaries which are normally enforced by the hardware", affected desktop, laptop and cloud computers.[46] Spectre, in turn, "breaks the isolation between different applications, allowing an attacker to trick error-free programs, which follow best practices into leaking their secrets".[47] It also affected desktop, laptop and cloud computers, effectively rendering vulnerable almost all modern processors.[48] The vulnerabilities enabled the theft of all kinds of data processed on a computer or related system. Many of the software fixes initially rolled out by chip manufacturers gave rise to performance issues, again affecting computers and systems across the globe.

What is unprecedented about these vulnerabilities is that they gathered sensitive data from computing devices that were actually "operating as designed", rather than exploiting flaws or vulnerabilities in computer software or hardware.[49] In other words, it was the very design of the operating technology that was flawed. Indeed, ongoing research has revealed central security weaknesses in the manner in which chips have been designed

---

[44] See C. Greer et al., "Cyber-Physical Systems and Internet of Things", NIST, 2019, https://www.nist.gov/publications/cyber-physical-systems-and-internet-things; see also Y. Pa et al., "Taxonomies for Reasoning About Cyber-physical Attacks in IoT-based Manufacturing Systems", *International Journal of Interactive Multimedia and Artificial Intelligence*, vol. 4, no. 3, 2017.

[45] Speculative execution is the practice of allowing processors to perform future work that may or may not be needed while they await the completion of other computation; L. Hay Newman, "The Elite Intel Team Still Fighting Meltdown and Spectre", *Wired,* 3 January 2019, https://www.wired.com/story/intel-meltdown-spectre-storm.

[46] See https://meltdownattack.com/.

[47] Ibid.

[48] L. Hay Newman, "The Elite Intel Team Still Fighting Meltdown and Spectre", *Wired,* 3 January 2019, https://www.wired.com/story/intel-meltdown-spectre-storm; see also C. Williams, "Kernel-memory-leaking Intel Processor Design Flaw Forces Linux, Windows Redesign," *The Register*, 2 January 2018, https://www.theregister.co.uk/2018/01/02/intel_cpu_design_flaw/.

[49] Intel, "Intel Responds to Security Research Findings", 3 January 2018, https://newsroom.intel.com/news/intel-responds-to-security-research-findings/#gs.AbK4rdO7.

over the past two decades. For instance, in early 2019, researchers discovered a new flaw—Spoiler—affecting all Intel chips. Like Spectre, the flaw could potentially be used to abuse speculative exploitation in Intel chips, although Intel has stressed that Spoiler does not reveal data such as passwords. Worryingly though, it apparently lowers the bar for other memory-leaking attack techniques and, importantly, side-channel attacks.[50] Such vulnerabilities have triggered not only a massive investment in the discovery of further vulnerabilities, but also a fundamental review of how processors are designed.

[50] L. Tung, "Intel Finally Issues Spoiler Attack Alert: Now Non-Spectre Exploit Gets CVE But No Patch", *ZDnet*, 10 April 2019, https://www.zdnet.com/article/intel-finally-issues-spoiler-attack-alert-now-non-spectre-exploit-gets-cve-but-no-patch/.

DYNAMICS ENABLING THE SPREAD OF MALICIOUS ICT TOOLS AND TECHNIQUES

The existence of these threats and vulnerabilities and the tools and techniques used to exploit them has been, and remains, very difficult to manage (let alone prevent) due to complex overlapping dynamics that go to the heart of public policymaking.

The fundamental dynamic is society's ever-growing reliance on cyberspace and the Internet in most aspects of economic, social and political life at a time when important shifts in the international order are taking place. As of June 2018, the number of Internet users was 4.2 billion—55 per cent of the global population (with future growth concentrated in countries where cybersecurity capacity and resources are low).[51] The central role of ICT/cyberspace as a substrate of global economic, social and political life has, in turn, attracted the interest of criminal actors seeking to exploit new opportunities, and State actors, particularly the major powers, using ICT capacities and capabilities to gain advantages in competition against each other. Wedged between the two are the private corporations building and profiting from the Internet and other IT markets and where, with few exceptions, business models have tended to reinforce and favour insecurity and push risk downstream to users.

Criminal and black-market dynamics

Criminal actors have always been early adopters of information technologies and today they excel at it.[52] The cybercrime market, which lives off a lively exchange of malicious tools and techniques, is reportedly thriving, ranking third in dollar value globally, after illicit activity such as government corruption and narcotics trafficking.[53] A report by McAfee and the Center for Strategic and International Studies (CSIS) estimated that the annual cost of cybercrime had grown to USD 600 billion (0.8 per cent) of global GDP in 2017, up from USD 500 billion in 2014.[54] Additionally, some 2 billion individuals have had their personal information stolen or compromised and countless more have had their privacy violated.

Incentives such as enormous profits, low risks and free publicity are driving the professionalization of, and the growth in, the kinds of criminal services offered, as well as the expansion of sales hubs—many connected to existing organized crime and mafia

[51] See https://www.internetworldstats.com/stats.html; see also UN News, "Internet Milestone Reached, As More Than 50 Per Cent Go Online: UN Telecoms Agency", 7 December 2018, https://news.un.org/en/story/2018/12/1027991.

[52] C. Kavanagh, "IT and Cyber Capabilities as a Force Multiplier for Transnational Crime", in V. Comolli (ed.), *Organized Crime and Illicit Trade: Responding to Strategic Challenges in Old and New Domains*, 2018.

[53] G. Gross, "The Cost of Cybercrime", Internet Society, 25 February 2018, https://www.internetsociety.org/blog/2018/02/the-cost-of-cybercrime/; see also J.A. Lewis, "Economic Impact of Cybercrime: Not Slowing Down", McAfee and CSIS, 2018.

[54] Ibid.

groups—across various regions.[55] This thriving online and offline underground universe allows actors to exchange information and ideas about potential targets; develop, buy, sell or deploy malware, vulnerability exploits or obfuscation and evasion tools; provide services ranging from specialized tasks (fake website design, password cracking) to outsourcing (hackers for hire, rent-a-botnet, DDoS-as-a-service) of more complex, destabilizing activities; and buy and sell digital assets, personal information, and login credentials.[56] These criminal actors "exchang[e] business models and information, compet[e] for access to and provision of services" and increasingly rely on regulatory loopholes surrounding blockchain technologies to monetize their activity.[57]

The publicity surrounding high-profile targeting attacks and their value have also served as a formidable marketing tool for criminal actors. Take, for instance, the zero-day market: although in 2007 security practitioners had trouble finding buyers for zero-days they discovered, by 2012 reports profiling the hackers that were trading zero-days in the online underground world brought the practice into focus.[58] The reports also revealed how much the zero-days were worth.

The trend of rising prices documented over the decade (see Table 1) has continued to evolve. By illustration, in January 2019, ArsTechnica reported "a higher demand for exploits that reliably compromise targeted devices or applications without a user being aware".[59] Leading exploit broker Zerodium had just offered up to USD 2 million for zero-click jailbreaks of Apple's iOS, USD 1.5 million for one-click iOS jailbreaks and USD 1 million for exploits that take over messaging apps WhatsApp and iMessage. Zerodium also announced important increases in the cost of a number of other exploits, including some of those in the list above.[60]

---

[55] *UNIDIR,* "*Preventing and Mitigating ICT-Related Conflict: Cyber Stability Conference 2018 Summary Report",* http://unidir.org/files/publications/pdfs/preventing-and-mitigating-ict-related-conflict-cyber-stability-conference-2018-summary-report-en-724.pdf

[56] J. Friedmann and M. Bouchard, "The Definitive Guide to Cyber Threat Intelligence: Using Knowledge About Adversaries to Win the War Against Targeted Attacks", ISight Partners, 2015, https://cryptome.org/2015/09/cti-guide.pdf.

[57] UNIDIR, "Preventing and Mitigating ICT-Related Conflict: Cyber Stability Conference 2018 Summary Report"; see also Digital Shadows, "A Tale of Epic Extortions: How Cybercriminals Monetize Our Online Exposure", https://resources.digitalshadows.com/whitepapers-and-reports/a-tale-of-epic-extortions-how-cybercriminals-monetize-our-online-exposure.

[58] C. Miller, "The Legitimate Vulnerability Market: Inside the Secretive World of 0-day Exploit Sales" Workshop on the Economics of Information Security, 2007; A. Greenberg, "Meet the Hackers Who Sell Spies the Tools to Crack Your PC (And Get Paid Six-Figure Fees)", *Forbes*, 21 March 2012.

[59] D. Goodin, "Zeroday Exploit Prices Are Higher than Ever, Especially for iOS and Messaging Apps", *ArsTechnica*, 8 January 2019, https://arstechnica.com/information-technology/2019/01/zeroday-exploit-prices-continue-to-soar-especially-for-ios-and-messaging-apps/.

[60] Jailbreaking refers to the escalation of privileges for the purpose of removing software restrictions imposed by Apple on iOS devices. On the increase in zero-day exploits, see ibid.

Table 1. Zero-Day Market Dynamics[61]

Service	Price per Zero-Day Vulnerability	Year
Microsoft Excel	> $1,200	2007
Mozilla	$500	2007
Vista exploit	$50,000	2007
Windows Metafile exploit	$4,000	2007
Adobe Reader	$5,000 - $30,000	2012
Android	$30,000 - $60,000	2012
Chrome or Internet Explorer	$80,000 -$200,000	2012
iOS	$100,000 - $250,000	2012
Microsoft Word	$50,000 - $100,000	2012
Windows	$60,000 - $120,000	2012
WeChat	$500,000	2018
Facebook Messenger	$500,000	2018
Apple iPhone	Up to $1,500,000	2018

Concerned about these developments, security researcher Bruce Schneier predicted that the rise of the market in zero-days would have negative consequences for software security, undercutting emerging practices in the security research world.[62] When independent researchers uncovered vulnerabilities, they could expect to be rewarded with notoriety, a so-called 'bug bounty' (finder's fee), or in some cases a consultancy or position from the company owning the vulnerable product. In each of these cases, the vulnerability itself would be ultimately patched and secured. The zero-day market, however, began a trend of rewarding non-disclosure: researchers who found vulnerabilities would be better rewarded by buyers—companies, governments, or a dark-net alternative—that often stockpile vulnerabilities rather than disclose and secure them, since this evidently pushes the price up. This was reportedly the case with the EternalBlue vulnerability, which according to Microsoft was only disclosed by the NSA after it had been leaked (along with a trove of other NSA vulnerability exploits).[63] Undoubtedly other governments are using (or seeking to use) zero-days too, although in some instances there is a shift to more responsible use via coordinated vulnerability disclosure or the establishment of domestic vulnerability equities processes.[64] Other factors driving the price surge in zero-days include the fact that the targets are becoming harder to exploit

[61] Table developed by Evgeny Scherbakov. See L. Ablon, M. Libicki and A. Golay, "Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar", RAND Corporation, 2014; Zerodium, https://zerodium.com; and K. Huang, M. Siegel, and S. Madnick, "Systematically Understanding the Cyber Attack Business: A Survey", Cybersecurity Interdisciplinary Systems Laboratory, Sloan School of Management, MIT, July 2018, http://web.mit.edu/smadnick/www/wp/2018-08.pdf.

[62] B. Schneier, "The Vulnerabilities Market and the Future of Security", *Forbes*, 30 May 2012.

[63] Earlier examples of undisclosed vulnerabilities include the Conficker Microsoft worm and the Welchia remote code execution released into the wild in 2008 and 2003, respectively; Wired, "The Leaked NSA Spy Tool that Hacked the World", 7 March 2018, https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/.

[64] On vulnerability equity processes and coordinated vulnerability disclosure see *supra* note 11 and notes 96 and 98 below.

due to increased pressure on companies to design more secure products, as well as demand increases from government agencies.

Geopolitical and national security dynamics

Information technologies have always been viewed as critical components of States' security and defence, for secure communications between and coordination of military assets in the field, remote monitoring of the resources and capabilities of other States, and collecting information about potential adversaries. Today, ICT and the national and global infrastructures it supports have become critical elements of economic, political and military power and thus strategic targets in competition among States. For nearly three decades this competition has been driving major shifts in military doctrine and strategy. Today it is evident that many States are developing offensive capabilities in which malicious tools and techniques play a central role, and critical infrastructure (defence, energy, finance, health, information) and political institutions and processes such as elections and media platforms become ever more attractive targets.

Linking to the software and hardware vulnerabilities discussed above, it is increasingly evident that some States use discovered flaws and vulnerabilities to develop exploits for intelligence, and defensive or more active offensive purposes instead of immediately reporting the vulnerabilities or flaws to vendors or the relevant party. The Snowden leaks confirmed this as did the more recent NSA breach which led to the leak and subsequent deployment of some of its vulnerability exploits.

In many instances, States rely on black markets to buy exploits and other malicious tools and techniques or to pay for the services of criminal proxies to deploy them.[65] The United Nations Groups of Governmental Experts working on ICT and international security issues recognized the use of proxies by States "in the conduct of malicious ICT actions", tethering the issue to international law and questions of State responsibility.[66] There are allegations that other States have directly or indirectly encouraged the emergence of specialized groups—'cyber-mafias' or 'patriot hackers'—to provide attack skills (e.g., Russian Business Network), sell and propagate zero-day exploits (e.g., the Shadow Brokers), including to other States or State-sponsored actors, to serve as a decoy or to give the impression of popular support.

State-directed or -supported cyber operations can affect critical infrastructure or essential services to the public with significant direct and indirect costs to the global economy. The

[65] The Tallinn Manual underlines that a cyberattack conducted by non-State actors could be attributed to a State if the latter is considered exercising "effective control" over the former. See M. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2017, p. 81.

[66] Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security 2013 (document A/68/98*, June 2013, pp. 4, 6 and 8) and 2015 (document A/70/174, July 2015, p. 13).

WannaCry attack which, at the time, was called one of the "largest cyber-disruptions the world has ever seen" indiscriminately affected some 300,000 computers across 150 countries.[67] Car manufacturing plants were forced to stop production while healthcare facilities had to cancel thousands of medical appointments and procedures. The WannaCry attack is said to have cost the British National Health Service almost GBP 100 million, in addition to the direct and indirect costs of 19,000 appointment cancellations.[68] Industries and services across China and the Russian Federation were also hit hard. In all, Trend Micro estimates that global losses from the attack, "including the resultant reduction in productivity and cost of damage control", amounted to USD 4 billion.[69] There are questions about how these different costs are calculated and some suggest that the attack was more inconvenient than costly. Whether costly or inconvenient, in December 2017 the UK Government attributed the attack to the Democratic People's Republic of Korea-backed Lazarus Group (also blamed for the 2014 Sony Pictures hack).[70] The United States soon followed suit, followed shortly by Australia, Canada, Japan and New Zealand.[71] Prosecutors in the United States later charged a national of the Democratic People's Republic of Korea for his involvement in creating the WannaCry ransomware (as well as for his involvement in the earlier Sony attack).[72]

Similarly, NotPetya—the wiper virus discussed above—reportedly incapacitated approximately 10 per cent of all computers in Ukraine and affected the work of scores of international companies, including FedEx and Durex, with US pharmaceutical giant Merck and the global shipping company Maersk reportedly the hardest hit.[73] The principal challenge of this specific malicious technique is its ability to permanently encrypt and wipe the hard drives of tens of thousands of business computers, costing companies hundreds of millions of dollars in clean-up costs and lost business. Cybersecurity companies in Eastern Europe dispelled initial opinion that it was a criminal-backed ransomware attack, linking it instead to a group known as Sandworm (or Telebots) that had been heavily involved in cyber operations against Ukraine.[74] In February 2018, the US government publicly attributed the attack to the Russian Federation's military intelligence

[67] A. Greenberg, "The Untold Story of NotPetya, The Most Devastating Cyberattack in History', *Wired*, 22 August 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[68] D. Palmer, "This Is How Much the WannaCry Ransomware Attack Cost the NHS", *ZDnet*, 12 October 2018, https://www.zdnet.com/article/this-is-how-much-the-wannacry-ransomware-attack-cost-the-nhs/.

[69] Trend Micro, "2017 Midyear Security Roundup: The Cost of Compromise", https://documents.trendmicro.com/assets/rpt/rpt-2017-Midyear-Security-Roundup-The-Cost-of-Compromise.pdf.

[70] UK Government, "Foreign Office Minister Condemns North Korean Actor for WannaCry attacks", 19 December 2017, https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks.

[71] White House, "Press Briefing on the Attribution of the Wannacry Malware Attack to North Korea", 19 December 2017, https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/.

[72] See https://www.justice.gov/usao-cdca/press-release/file/1091951/download.

[73] *The Register*, "Nothing Could Protect Durex Peddler from NotPetya Ransomware", 6 July 2017, https://www.theregister.co.uk/2017/07/06/notpetya_reckitt_benckiser/.

[74] A. Greenberg, "The White House Blames Russia for NotPetya, The 'Most Costly Cyberattack in History'", *Wired*, 15 February 2018, https://www.wired.com/story/white-house-russia-notpetya-attribution/.

agency, the GRU, noting that it had been "part of the Kremlin's ongoing effort to destabilize Ukraine … demonstrat[ing] ever more clearly Russia's involvement in the ongoing conflict". Its knock-on effects caused "billions of dollars in damage across Europe, Asia, and the Americas".[75] Russia has denied responsibility for the attack.

These trends are not likely to dissipate. As of 2016 some 30 States were reportedly developing offensive cyber capabilities in which vulnerability exploits and other malicious tools and techniques play a central role. Australia, France, Germany, the United Kingdom and the United States have since publicly disclosed development of offensive cyber capabilities for national defence purposes. It is largely assumed that all major and many middle powers are moving in the same direction.[76]

In response to persistent malicious activity affecting its national infrastructure and institutions, the United States has shifted gears, asserting in its Department of Defence 2018 Cyber Strategy that it would "defend forward to disrupt or halt malicious activity at its source, including activity that falls below the level of armed conflict".[77] It also committed (alongside Denmark, Estonia, the Netherlands and the United Kingdom) to use cyber capabilities for NATO's collective defence. For some, these doctrinal developments favouring offensive action over defence and resilience are long overdue and merited since existing efforts to promote responsible behaviour and greater restraint have not borne fruit. For others, however, they have set the scene for a more destabilizing and "conflictual online environment" and may render ineffectual ongoing diplomatic and para-diplomatic confidence- and trust-building activities.[78] Moreover, such an environment will, by logic, require a steady arsenal of malicious tools and techniques, possibly contradicting commitments by States to stem their spread, and also undermine the work of companies, researchers and engineers to develop more secure products and services.

Information technology market dynamics

Finally, a number of IT market dynamics also undermine security and the ability to manage (let alone prevent) the spread of malicious tools and techniques. Experts have described computers and related systems as 'fundamentally insecure' by design, particularly when networked. This challenge is linked to the failure of technology developers and companies to adhere to known computer security science dating from the 1970s, and the absence of

[75] White House, "Statement from the Press Secretary", 15 February 2018, https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/.
[76] T. Uren, B. Hogeveen and F. Hanson, "Defining Offensive Cyber Capabilities", Australian Strategic Policy Institute, 2018, https://www.aspi.org.au/report/defining-offensive-cyber-capabilities/.
[77] "Domain Trends", *The Military Balance*, vol. 119, no. 1; US Department of Defense, "Summary. Department of Defense Cyber Strategy 2018", https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.
[78] Ibid.; see also UNIDIR, "Preventing and Mitigating ICT-Related Conflict: Cyber Stability Conference 2018 Summary Report", http://unidir.org/files/publications/pdfs/preventing-and-mitigating-ict-related-conflict-cyber-stability-conference-2018-summary-report-en-724.pdf; and J. Mallery, forthcoming 2019.

any means (in terms of public policy) to ensure adherence. Highly vulnerable computer software and hardware (current and legacy), as well as fundamental design flaws in core components such as processors, and a low level of awareness of both software vendors and end users of respective IT products drive exponential problems as the technologies become increasingly integrated into large, interconnected systems. These engines of vulnerability "spread through the capital goods sector into critical infrastructures and government and enterprise computing".[79] More often than not, the fallout of their exploitation largely falls upon third parties rather than the actual vendor.

Compounding these challenges is the extreme diversity and complexity of supply chains for software and hardware. The reality of the current globalized, transnational and highly competitive IT market means that complete vertical integration of IT system supply chains has become impossible for any vendor or operator. Greater complexity of supply chains leads to higher chances for vulnerabilities in the code of IT products and makes comprehensive vulnerability auditing more challenging and time-consuming.

What drives technology firms to rush products to market before they are adequately secure? This is explained by a number of factors. The first lies in questions of secure design and the nature of the operating systems and programming languages being used. If, according to one expert, firms used competent operating system designs (e.g., separation of kernel and type-safe programming languages), a large number of persistent problems would be eliminated by design.[80] However, the sector "remain[s] committed to antiquated foundational technologies that are inherently insecure".[81] Contributing to this situation is backward compatibility to legacy codebases, and a work force poorly educated in secure programming.

The dynamics of dominant firm markets shed additional light on why commercial firms may rush insecure products to market.[82] Ross Anderson and Tyler Moore have identified several characteristics of digital product and service markets that value time-to-market over security.[83] First are *network effects*, according to which the value of a service appreciates proportionally to the number of users it has—this is a leading incentive for firms to stake a claim to market share quickly. Long before the emergence of the Internet, network effects were central to corporate strategies such as that of the American Telephone and Telegraph company (AT&T) as it expanded its reach across the United

[79] J. Mallery, forthcoming 2019. See also talk by J. Mallery, " Cyber arms control: risk reduction under linked regional insecurity dilemmas", IISS, 10 September 2018, https://www.iiss.org/events/2018/09/cyber-arms-control
[80] Ibid.
[81] Ibid.
[82] The OECD defines a "dominant firm" as one "which accounts for a significant share of a given market and has a significantly larger market share than its next largest rival. Dominant firms are typically considered to have market shares of 40 per cent or more". OCED Glossary of Statistical Terms, https://stats.oecd.org/glossary/detail.asp?ID=3199.
[83] R. Anderson and T. Moore, "Information Security Economics – and Beyond", in A. Menzes (ed.), *Advances in Cryptology*, 2007, https://link.springer.com/chapter/10.1007/978-3-540-74143-5_5.

States.[84] In the Internet era, network effects have been adapted and popularized as Metcalfe's law, which states that the effect of a telecommunications network is proportional to the square of the number of connected users of the system.[85] A telephone network becomes more valuable with every additional person who is connected to it in much the same way that the functional value of Facebook or Twitter increases with each new user.

Second, and closely related to network effects is the high cost of *switching* between often mutually exclusive virtual network services.[86] Windows and Apple operating systems, for example, adhere to two distinct and incompatible digital architectures. Switching between the two of them on a commercial level would entail burdensome and expensive procedures such as retraining relevant staff and re-engineering relevant protocols. On the consumer level, some products, such as Internet browsers, may not be incompatible but redundant.

Related to the above is the question of *interoperability between other platforms, services, and applications* in the initial stages of a product's existence, as well as *a lax approach to open source components*. Firms will seek to accommodate external applications by leaving a certain amount of flexibility in their coding. Indeed, young firms will likely do everything possible to court major vendors in order to accrue the benefits of increased visibility that they provide.[87] Some firms have put in place measures to prevent such lax behaviours. Regarding open source components, in 2017 an Open Source 360 Degree survey lamented the technology industry's increased use of open-source components to bolster its own software and systems. The issue was not with the open source components *per se,* as they can help cut back on costs, facilitate easy access, avoid onerous vendor lock-in systems, to customize code and fix flaws and vulnerabilities directly and boost business innovation. Rather, no effective security or risk management standards or procedures had been put in place as they were being incorporated. Some 80–90 per cent of modern applications use open-source software components to address the demands of increasingly technology-reliant societies, significantly augmenting risk.[88]

Finally there is the complex and thorny question of *regulation*. The technology industry is largely unregulated and those regulations that do exist largely conform to what have been described as the *ex ante* type.[89] These typically take the form of enforced compliance

[84] See, for instance, "1908: Annual Report of The Directors of the American Telephone & Telegraph Company to the Stockholders for Year Ending December 31, 1908", Boston, 1909, https://beatriceco.com/bti/porticus/bell/pdf/1908ATTar_Complete.pdf.
[85] B. Metcalfe, "There Oughta Be a Law", *New York Times,* 15 July 1996.
[86] C. Shapiro and H. Varian, "Information Rules: A Strategic Guide to the Network Economy", Harvard Business School, 1999, p. 11.
[87] T. Moore and R. Anderson, "Internet Security", in M. Peitz and J. Waldfogel (eds), *The Oxford Handbook of the Digital Economy,* 2012.
[88] Open source software can be adopted for the purposes of cost savings, easy access, no vendor lock-in systems, and the ability to customize code and fix bugs directly. It also reportedly boosts business innovation.
[89] R. Anderson and T. Moore, "Information Security Economics – and Beyond", in A. Menzes (ed.), *Advances in Cryptology*, 2007, https://link.springer.com/chapter/10.1007/978-3-540-74143-5_5.

rather than the external imposition of technical prescriptions due both to legitimate concerns about the impact a stringent safety regulation regime would have, for instance, on software innovation in the development phase and the difficulty of maintaining prescriptive regulations in a rapidly developing sector. Though *ex ante* regulations are the norm, the uninterrupted high rate of successful attacks nonetheless suggests that regulations are not effectively producing more security. This is due to a number of externalities to the IT market, including the fact that costs incurred by the exploitation of vulnerabilities are not borne by the vendors ultimately responsible for the vulnerability, but rather the users. It is also due to "the prevalence of liability dumping or shifting between different actors across the supply chains".[90]

For some, *ex post* liability regulation or legislation also poses challenges. It can slow the pace of innovation as companies stretch out development periods to focus on safety, with no assurances of a substantial increase in security given the unavoidable flaws or vulnerabilities in even the best-written software. Liability for supply chain risks—due diligence standards based on evolving industry best practices—might be more plausible. For example, Moore suggests a regulatory approach melding both forms of control: software companies should be required to provide evidence of rigorous security testing during software development while facing more robust legal liability for failing to meet testing standards.[91] For now, a number of promising policy initiatives that stop short of hard regulation are being tested. These include guidelines and labelling and certification schemes. Such initiatives are increasing in number, propelled in large part by emerging IoT-related risks and challenges. The European Cybersecurity Certification Framework and the UK Secure by Design code of practice are examples of such government-led efforts.[92] However, these initiatives are still at an early stage, are largely evolving in a single region or compete (and often conflict) with regulatory approaches emerging in others.

[90] ENISA, "Economics of Vulnerability Disclosure", December 2018, https://www.enisa.europa.eu/news/enisa-news/the-economics-of-vulnerability-disclosure/.

[91] R. Anderson and T. Moore, "Information Security Economics – and Beyond", in A. Menzes (ed.), *Advances in Cryptology*, 2007, https://link.springer.com/chapter/10.1007/978-3-540-74143-5_5.

[92] The objective of the EU proposal for a European ICT security certification and labelling framework is to build greater trust and security in ICT products and services through a comprehensive set of (non-binding) rules, technical requirements, standards and procedures. The certification framework is just one part of the broader EU Cybersecurity Act which builds upon existing instruments and presents new initiatives to further improve EU cyber resilience and response; see https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework/;
see also, UK Government, "Code of Practice for Consumer IoT Security", 2018, https://www.gov.uk/government/collections/secure-by-design/.

PRIVATE SECTOR RESPONSES TO STEMMING THE SPREAD OF MALICIOUS ICT TOOLS AND TECHNIQUES

The past five years have seen a significant shift in the role of different actors in addressing the different dynamics described above, enabling the spread of threats, vulnerabilities and the malicious ICT tools and techniques discussed here. These actions can be described as a mix of *reactive* and *productive* measures.[93] Reactive measures are manifest, for instance, in incident response and remediation, or industry cooperation with law enforcement to tackle cybercrime. The productive kind—those more normative in character—are generally aimed at protecting business interests by pushing back or lobbying against certain regulations or legislation, or promoting certain positions to protect market share. Of late, productive measures are apparent in a number of normative initiatives by technology companies and technology experts aimed at restraining the behaviours of State and non-State malicious actors. While not the subject of this report, productive measures might also be evident in recent decisions by insurance companies to reject insurance claims relating to major cybersecurity incidents that have been attributed to States, driving additional pressure for the development of standards and norms.[94]

Vulnerability disclosure

Vulnerabilities generate huge costs not necessarily borne by vendors or manufacturers. Nonetheless, several technology companies have been working on incident response and remediation for many years, as evidenced in the policies and practices of individual companies in regard to flaws and vulnerabilities affecting their own products and services (e.g., Intel's STORM and its Security First pledge,[95] Microsoft's Security Vulnerability Research Programme, and Google's Project Zero and its Vulnerability Disclosure Program).[96] Some have established bug-bounty programmes (e.g., Facebook's Bug Bounty and Google's Vulnerability Reward Programs) which in turn has led to the emergence of a bug-bounty industry. Others focus on the longer term, pushing for broader responsibility of and coordination between security researchers, technology companies and others in discovery and public disclosure of vulnerabilities (e.g., common principles and guidance on coordinated vulnerability disclosure), and efforts to promote more transparency and reduce the risks associated with the vulnerability equities policies

[93] P. Cornish and C. Kavanagh, "Geneva Dialogue on Responsible Behaviour in Cyberspace", Swiss Federal Department of Foreign Affairs, forthcoming 2019. The author is also grateful to discussions with Dennis Broeders within the context of the work of the Geneva Dialogue.

[94] J.S. Nye Jr., "Normative Restraints on Cyber Conflict", Belfer Center for Science and International Affairs, 2018.

[95] Intel, "Security-first Pledge", 2018, https://newsroom.intel.com/news-releases/security-first-pledge/; for a discussion on the establishment of Intel's STORM group, see L. Hay Newman, "The Elite Intel Team Still Fighting Meltdown and Spectre", *Wired,* 3 January 2019, https://www.wired.com/story/intel-meltdown-spectre-storm.

[96] For Microsoft's Security Vulnerability Research Program, see: https://www.microsoft.com/en-us/msrc/msvr; for Google's Vulnerability Disclosure Program, see: https://hackerone.com/google/.

and practices of governments.[97] These complement the equally important work of researchers and technical bodies such as computer emergency response teams (CERTs) that, for many years, have informed the development of guidance and recommendations on coordinated vulnerability mechanisms and vulnerability equities processes at national and international levels, although substantial challenges remain.[98] Sometimes, however, companies have conflicting approaches to vulnerabilities. The ongoing Microsoft–Google rivalry over vulnerability patching and ethics of disclosure is a case in point.[99] In addition, some responses, such as bug bounties, may often lead to new challenges and rivalries.[100]

Beyond vulnerability disclosure

Beyond vulnerability disclosure, companies and the technology community are engaging productively in *industry-wide* or *cross-sectoral initiatives* to reduce common threats, strengthen security of products and services, and establish minimum protocols and standards for protecting global ICT architecture and the global supply chains and users. All of these have implications for stemming the spread of malicious tools and techniques.

Early examples include the Mutually Agreed Norms for Routing Security (MANRS) involving network operators from across the globe. The initiative is managed by the Internet Society, the main objective of which is to "provide crucial fixes to reduce the most common routing threats", many of which were discussed earlier in the report.[101] Another is Domain-based Message Authentication, Reporting and Conformance (DMARC), an email authentication policy and reporting protocol established by "receiver, sender, intermediary and vendor" companies, with the aim of "helping prevent impersonation attacks via email".[102] More recent efforts can be viewed from the perspective of strengthening trust in ICT products and services as well as producing changes in behaviour. These include the Charter of Trust and the Cybersecurity Tech Accord, the former spearheaded by Siemens, the latter by Microsoft.[103] The Charter of Trust is aimed

[97] See K. Charlet *et al*, supra note 11.

[98] See, for example the Software Engineering Institute, "The CERT Guide to Coordinated Vulnerability Disclosure", Carnegie Mellon University", August 2017, https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf/.

[99] C. Betz, "A Call for Better Coordinated Vulnerability Disclosure", Microsoft, 11 January 2015, https://blogs.technet.microsoft.com/msrc/2015/01/11/a-call-for-better-coordinated-vulnerability-disclosure/; see also R. Brandom, "Google Just Disclosed a Major Windows Bug — And Microsoft Isn't Happy", *The Verge*, 31 October 2016, https://www.theverge.com/2016/10/31/13481502/windows-vulnerability-sandbox-google-microsoft-disclosure; and more recently T. Warren, "Google Discloses Microsoft Edge Security Flaw Before a Patch Is Ready", *The Verge*, 19 February 2018, https://www.theverge.com/2018/2/19/17027138/google-microsoft-edge-security-flaw-disclosure

[100] B. Schneier, "The Vulnerabilities Market and the Future of Security", *Forbes*, 30 May 2012; see also Cybellum, "The Bug Bounty Problem: How Mishandled Bounties Hurt the Industry", 16 October 2016, https://cybellum.com/bug-bounty-problem-mishandled-bounties-hurt-industry/.

[101] Mutually Agreed Norms for Routing Security (MANRS), https://www.manrs.org/.

[102] Domain-based Message Authentication, Reporting and Conformance (DMARC), https://dmarc.org/about/history/.

[103] See Siemens, "Time for Action: Building a Consensus for Cybersecurity", https://www.siemens.com/innovation/en/home/pictures-of-the-future/digitalization-and-software/cybersecurity-charter-of-trust.html; Cybersecurity Tech Accord, https://cybertechaccord.org/about/.

at establishing industry-wide standards and principle while the Cybersecurity Tech Accord promotes and endorses existing initiatives, norms, standards and practices and has a strong emphasis on shaping State behaviour. A third effort, the Global Cyber Alliance, is a cross-sectoral initiative involving scores of companies and entities and focused on "eradicating cyber risk".[104] Global cybersecurity company Kaspersky Lab, too, has sought to strengthen trust in its products and services, including through its Transparency Initiative. This has involved relocating data storage and processing as well as its software assembly infrastructure to Switzerland, where it has also opened a Transparency Centre.[105]

Some of these efforts also serve to further catalyse or rally support around other initiatives aimed at shaping more productive—rather than reactive—behaviours. For instance, the Cybersecurity Tech Accord recently endorsed the MANRS initiative and, together with the Global Cyber Alliance, endorsed DMARC. The Tech Accord has also provided inputs to the UN Secretary-General's High-Level Panel on Digital Cooperation on the principles and action items for protecting users and customers from digital threats, opposing cyber attacks on civilians and enterprises, empowering users and customers better protect themselves, and advancing cybersecurity cooperation.[106] Finally, the Tech Accord signatories recently published a summary of their views on cybersecurity confidence-building measures, positioned as "series of recommendations which leverage proposals made by authoritative organizations such as the [United Nations] and OSCE" and "could help fill existing gaps in [S]tates' approaches to cybersecurity", with a particular focus on the Organization of American States as potential addressee of the proposed ideas.[107]

Some companies have also played an important role in funding and participating in multi-stakeholder initiatives aimed, too, at promoting more productive behaviours on the part of State and non-State actors. Microsoft, for example, has stood steadily behind the push by the Global Commission on Stability in Cyberspace to promote a series of norms (some perhaps better described as good practices) that, if implemented, could contribute in a number of important ways to mitigating cyber threats and protecting global ICT supply chains.[108]

[104] The Global Cyber Alliance (GCA), https://www.globalcyberalliance.org/who-we-are/#mission-purpose.
[105] 'Kaspersky Lab relocates data processing to Switzerland'. Available at: https://www.kaspersky.com/transparency-center
[106] See Cybersecurity Tech Accord submission to the United Nations High Level Panel on Digital Cooperation, February 2019, https://digitalcooperation.org/wp-content/uploads/2019/02/Tech-Accord-HLP-Response.pdf/.
[107] See Tech Accord, "Promoting International Peace and Stability by Building Trust between States in Cyberspace: The Importance of Effective Confidence-Building Measures", April 2019, https://cybertechaccord.org/uploads/prod/2019/04/FINALOASWP.pdf/.
[108] See the Global Commission on the Stability of Cyberspace (GCSC), https://cyberstability.org; specifically, see https://cyberstability.org/research/global-commission-proposes-definition-of-the-public-core-of-the-internet/ and https://cyberstability.org/research/singapore_norm_package/.

Private sector efforts to shape State behaviour

Many companies engage on government-backed normative efforts with the objective of mitigating the potential longer-term negative effects of proposed rules, to pressure governments into respecting existing commitments or rules in their use of ICT, or to adopt new ones. Such private sector actions may be viewed as both reacting to an immediate threat (evidently, the threat to business interests, but also threats to cybersecurity and broader international security and stability), while also contributing to changes in the broader normative landscape and the behaviours of other actors.[109] Again, they complement the ongoing efforts of other actors such as engineers, security researchers and civil society.

For instance, a number of companies and associations are engaged with the European Union to inform the development of the Network and Information Security directive, as well the Cybersecurity Act, notably ENISA regulation revisions and the European ICT security certification and labelling framework.[110] The intention was not just to prevent hard regulation but to contribute to improving the proposals and their longer-term domestic and international effects.[111]

Many of these same companies also engage in efforts to influence the negotiating positions of their governments when ICT-related policies become part of trade or export control negotiations, again often to protect business interests, but also as a means to guard against potential risks and influence the normative landscape. In this vein, industry actors have engaged in debates sparked by Wassenaar Arrangement members to place restrictions on exports of certain intrusion software tools in order to prevent malware and vulnerability exploits from falling into the hands of repressive regimes. This would have required restrictions on exports for those technologies, software and systems that develop or operate intrusion software, including some of the very tools and techniques used by cybersecurity researchers and firms involved in legitimate activity such as penetration testing, vulnerability disclosure and incident response. Viewed as a form of "hacking technology regulation", the rule risked endangering the work of legitimate cybersecurity researchers with potential "dire and far-reaching consequences for the entire IT security industry".[112]

[109] A more extensive study on private sector roles and responsibilities might spend time looking at the complex and high-cost lobbying practices of global technology companies.

[110] The EU framework for cybersecurity certification for online services and consumer devices is "the first internal market law aimed at enhancing the security of connected products, internet of things (IoT) devices and critical infrastructure"; see T. Reeve, "EU Shakes up Cyber-Security with New Agency and Certification Framework", *SC Media*, 11 December 2018, https://www.scmagazineuk.com/eu-shakes-cyber-security-new-agency-certification-framework/article/1520888/.

[111] European Commission, "Review of ENISA Regulation and Laying Down a EU ICT Security Certification and Labelling", https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3436811/feedback_en?p_id=34664/.

[112] The Coalition for Responsible Cybersecurity, http://www.responsiblecybersecurity.org/latest/.

In the United States, initial steps by the Department of Commerce to write the proposed Wassenaar rule into national legislation were opposed by a number of cybersecurity companies who rallied together to establish the Coalition for Responsible Cybersecurity with the aim of preventing "harmful export control rules for cybersecurity products and services". [113] Following broader efforts of industry (including the Coalition and its members), academia and the research community, the Department of Commerce revised its proposed export control rules on cybersecurity tools and sought additional input from these actors to inform its negotiating position around changes to the original Wassenaar proposal. These changes were agreed at the Wassenaar Arrangement's annual plenary session in December 2017.[114]

Microsoft's strong push for a Digital Geneva Convention, its more recent Digital Peace Campaign and moves to establish a Digital Peace Institute are another important example of industry action relating to government-backed normative efforts that both react to existing threats (State behaviour, in particular regarding potential harm to citizens) and aim, in the longer term, to prevent the reoccurrence of such behaviours. These efforts have now become a central focus of the Paris Call for Trust and Security in Cyberspace, a French-government backed multi-stakeholder initiative gaining international traction.[115]

[113] Ibid.

[114] See "Wassenaar Arrangement List of Dual-Use Goods and Technology and Munitions List", December 2017, https://www.wassenaar.org/app/uploads/2018/01/WA-DOC-17-PUB-006-Public-Docs-Vol.II-2017-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf; see also S. Waterman "The Wassenaar Arrangement's Latest Language is Making Security Researchers Very Happy", cyberscoop.com, 20 December 2017, https://www.cyberscoop.com/wassenaar-arrangement-cybersecurity-katie-moussouris/.

[115] See "Paris Call for Trust and Security in Cyberspace", 12 November 2018, https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_cyber_cle443433-1.pdf

CONCLUDING OBSERVATIONS

The initiatives discussed above are all important. They demonstrate that technology companies are playing an increasingly important role in national and global governance issues, while also signalling that some companies are gradually assuming the roles and responsibilities that come with increased influence and power. These roles and responsibilities are complementary to the responsibilities of States, the technology community and other actors. They do not replace them.[116]

The question is whether these initiatives (together with the work of States and other actors) are sufficient to deal with the challenges at hand. Evidently, the initiatives discussed above are hardly exhaustive. Yet, these and the scores of others that exist do not seem to be producing more secure products and systems, or stemming the flow of malicious tools and techniques, even if the immediate remedies are at times effective and the normative objectives ambitious. As it is, companies face the looming prospect of regulation. This is evidenced, for example, in the range of measures the European Union is adopting within its broader Cybersecurity Act. In discussing vulnerability disclosure practices, ENISA's recent report on the Economics of Vulnerability Disclosure also suggests that further structural levers may be required "to help offset some of the negative consequences of the economic features of the information security market".[117]

Looking to the future, it will be important to both scale and frame many existing approaches to dealing with vulnerabilities and the spread of malicious tools and techniques within more coherent policy frameworks so as to enable their implementation across countries and regions and ensure the effects can be derived internationally. Indeed, for now, they are largely promoted by private sector actors and governments in North America and Europe, largely because until recently this is where most IT companies were based. This is no longer the case, and as with other major advances in technology adding complexity to governance issues, effort will need to be made to avoid regions of conflicting regulation, whether it be self-regulation on the part of industry actors, or regulation introduced by governments or a mix of both.[118] Hence, agreeing on complementary structural public and private levers is important. But what would such levers look like and how can such an approach be calibrated to ensure that it is neither too strong—stifling innovation and driving away business—nor too soft—sacrificing public interests in the pursuit of national or private interests? Responding to these questions will be undoubtedly difficult, given the complexity of the technologies

[116] See P. Cornish and C. Kavanagh, "Geneva Dialogue on Responsible Behaviour in Cyberspace", Swiss Federal Department of Foreign Affairs, forthcoming 2019.

[117] ENISA, "Economics of Vulnerability Disclosure", December 2018, pp. 5–6, https://www.enisa.europa.eu/news/enisa-news/the-economics-of-vulnerability-disclosure/.

[118] C. Kavanagh, *New Tech, New Threats*, Carnegie Endowment for International Peace, forthcoming.

themselves, as well as the current state of international affairs, yet it is precisely these kinds of responses that are urgently required.

Second, increased investment (political, financial and technical) must be made in ensuring greater security in the design, development and application of both products and services. This is an old issue but one that has not yet produced longer-term effects. Some alternative solutions have been suggested. For instance, the Global Commission on the Stability of Cyberspace has recommended a "reasonable level of diligence … that prioritizes security … and reduces the likelihood, frequency, exploitability and severity of vulnerabilities".[119] How 'reasonable' is defined, implemented and assessed in this complex environment is an open question, notably as cybersecurity issues spread or converge with the IoT and other advances in technology in the coming years.

Finally, it is difficult to ascertain what the different industry-backed initiatives are actually achieving, since they tend to only publish their objectives and information on past and up-coming activities or partnerships. Greater transparency in this regard could contribute to building trust, convincing users, governments and other affected parties of the value of the initiatives and identify existing and emerging loopholes in current policies and practices. This in turn can help to determine whether hard regulation or legislation is actually required or not. Transparency measures could involve more rigorous reporting and engagement on how the initiatives are meeting their objectives, against what criteria they are being assessed and by whom, their funding sources and persistent challenges to their implementation. The Paris Call, the Global Forum on Cyber Expertise, the G7 and G22 would be important platforms for presenting these results. So, too, will be the United Nations Open-Ended Working Group[120] (OEWG) and sixth United Nations Group of Governmental Experts[121] commencing work at the United Nations later this year. The OEWG resolution explicitly mentions the possibility of intersessional consultations with the private sector feeding into the work of the Group. Indeed, industry efforts that can be shown to be contributing to the implementation of relevant norms—including those relating to vulnerabilities and the spread of malicious tools and techniques—will likely be of interest to both Groups and an important contribution to their work.

[119] See Global Commission on the Stability of Cyberspace, 'Norm to Reduce and Mitigate Significant Vulnerabilities', in "Singapore Norm Package", November 2018, https://cyberstability.org/wp-content/uploads/2018/11/GCSC-Singapore-Norm-Package-3MB.pdf.

[120] See United Nations resolution A/RES/73/27 of 11 December 2018.

[121] See United Nations resolution A/RES/73/266 of 2 January 2019.

SECURITY AND TECHNOLOGY PROGRAMME

Stemming the Exploitation of ICT Threats and Vulnerabilities

An Overview of Current Trends, Enabling Dynamics and Private Sector Responses

As societies become increasingly dependent on digital technologies, private technology companies have new roles and responsibilities in regard to shaping and implementing international security policy—particularly in respect to stemming the spread of ICT-related threats and vulnerabilities. This policy brief explores recent trends in threats and vulnerabilities, outlines the dynamics that enable their diffusion, and considers the steps the private sector are taking to address them.

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH