Chapter 29

Cyber Attacks by Terrorists and other Malevolent Actors: Prevention and Preparedness

With Three Case Studies on Estonia, Singapore, and the United States

Shashi Jayakumar

The field of cyberterrorism has existed for as a long as it has been possible to interdict or compromise computer systems. While contributions of scholars, researchers, and practitioners have enriched discussions, there are longstanding and unresolved issues of definition which can give rise to confusion. Does cyberterrorism mean attacks only by individuals groups that fall within widely accepted definitions of "terrorist" or "terrorist organizations?" To what degree does the aim or intention of the malicious actor matter? For the purposes of the present volume, this study (without sidestepping these questions) examines attacks against computer infrastructure and Critical Information Infrastructure (CII) by all actors with capability, and not just groups such as Al-Qaeda or ISIS. As the author notes and establishes early in his discussion, this is necessary given that while conventional terrorist groups might have intent, they have not to date acquired the capability to carry out a genuinely destructive cyber-attack of the type that might lead to major loss of life or infrastructural damage. It is (for the most part) states which have this capability. Cyber prevention and preparedness covers a wide range. This three-part chapter includes technical aspects of cyber protection, systems (and people) resilience, risk mitigation, as well as nurturing talent within a viable cyber ecosystem. Three case studies (Estonia, Singapore, and the US) are given where these and other relevant issues are examined.

Keywords: advanced persistent threat, cyber, cyberattacks, critical information infrastructure, cyberterrorism, hacking, malware, phishing, Supervisory Control and Data Acquisition, industrial control systems

Part I - Introduction

Meaning of "Cyberterrorism:" Past, Present, and Future

What is cyberterrorism? Is cyberterrorism simply terrorist acts (causing death, serious disruption, fear in the target population, attempting to change the ideology of a people) carried out using digital or cyber electronic means, or does it involve cyberattacks carried out by terrorists and terrorist groups? Does the actor actually matter? Can cyberterrorism technically speaking be done by a state?

In 1997 Mark Pollitt, special agent for the FBI, offered an early working definition of cyberterrorism: "Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub national groups or clandestine agents."[1]

It is tempting, following Pollitt's influential - and early - attempt at definition, to simply suggest that cyberterrorism can only be committed by what are considered terrorist organizations (that is, non-state actors or the clandestine agents highlighted by Pollitt). But consider another relatively early, and still useful definition from James Lewis, who in 2002 defined cyberterrorism as "the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population."[2] Lewis' definition is similar in some respects to Pollitt's, but Lewis leaves open the possibility that state action might be caught within his definition as well.

Finally, consider a widely-cited definition by Dorothy Denning:

> "Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not."[3]

Denning is precise when it comes to what types of acts constitute cyberattacks, and, like Lewis, is *actor-agnostic*: her definition leaves open the possibility that actors apart from conventional non-state terrorist groups and organizations might be caught.

[1] Pollitt, Mark 'Cyberterrorism: Fact or Fancy', *Computer Fraud & Security*, 2 1998, p. 9.
[2] Lewis, James A., 'Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats' Center for Strategic and International Studies , December 2002. Available: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf
[3] Denning, D. Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives, Committee on Armed Services, 23 May 2000. Available at: https://www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf

DOI: 10.19165/2020.6.0129

Past surveys of experts aimed at either arriving at definitions of cyberterrorism (or indeed aimed at eliciting views on whether a definition is necessary) tend to have shown more than anything else that there is no single accepted definition; nor is there likely to be one in the near future.[4] This chapter avoids tendentious discussions on contested definitions of cyberterrorism; nor for that matter has this author chosen to dwell on the vexed question as to whether or not all cyberattacks are cyberterrorism attacks.[5] The first part of this chapter is a discussion of cyberattacks by what are conventionally understood as terrorist organizations. Following this, in the second part of the chapter the discussion is broadened to study cyberattacks by malevolent actors. These could be state and non-state actors; necessarily, the instruments could be used by terrorist groups or individuals. Preparedness against, and prevention of, cyberattacks are then discussed with three case studies (the US, Estonia, and Singapore) in the third and final part of this chapter.

Cyber Attacks by Terrorist Organizations

Cyber-attack plotting by terrorist organizations has a long history. This section discusses two periods: the late 1990s to early 2000s where cyber-attacks were largely aspired to, to early 2000s to 2015 when intent became more visible.

1990s –2000s: Aspiration

Terrorist groups such as Al-Qaeda have had a presence on online platforms since the late 1990s.[6] Using the internet was (and is) cheap and (relatively) anonymous; it also bypassed mainstream or traditional news sources with the websites and forums, certainly in the earlier phase, largely free from any meaningful censorship. This route also provided the means to quickly reach a growing audience.[7]

Al-Qaeda's leadership had, from early on, a vision of attacking Western critical infrastructures, and it does seem that this vision could have encompassed remote attacks by computer or digital means.[8] This aspirational goal devolved in time to the wider Al-Qaeda-sympathetic diaspora, members of which would, from time to time in the 2000s, make claims on various online

[4] Jarvis, Lee, and Stuart Macdonald, *What Is Cyberterrorism? Findings From a Survey of Researchers*, *Terrorism and Political Violence*, 27:4, 2015, pp. 657-678, and also Lee Jarvis & Stuart Macdonald , *Locating Cyberterrorism: How Terrorism Researchers Use and View the Cyber Lexicon*, *Perspectives on Terrorism* 8(2), 2014, pp. 52-65.

[5] See the still useful introductory remarks in John Rollins and Clay Wilson, 'Terrorist Capabilities for Cyberattack: Overview and Policy Issues', Washington D.C.: Congressional Research Service, 20 Oct. 2005, updated 22 January 2007, pp. 1-2.

[6] For background, see Weimann, Gabriel, *Terror on the Internet* (Washington, DC: United States Institute of Peace, 2006), and Weimann, Gabriel, *Terrorism in Cyberspace: The Next Generation* (New York: Columbia University Press, 2015).

[7] For observations on the advantages that social media platforms and networking sites give terrorist groups, over and above online fora and websites, see Gabriel Weimann, 'Terrorist Migration to Social Media' *Georgetown Journal of International Affairs*, Vol. 16, No. 1 (Winter/Spring 2015), pp.181-183.

[8] See Davis, Anthony, 'The Afghan files: Al-Qaeda Documents from Kabul', *Jane's Intelligence Review*, 1 February 2002. Shortly after the 11 September 2001 attacks, Osama bin Laden gave a statement to Hamid Mir (editor of the Urdu-language *Ausaf* newspaper) indicating that "hundreds of Muslim scientists were with him and who would use their knowledge in chemistry, biology and (sic) ranging from computers to electronics against the infidels". 'Usamah Bin-Ladin denies involvement in, but backs US attacks', *BBC Monitoring South Asia*, 12 September 2001 (original report – Hamid Mir, 'I have no hand in blasts in US and attack on Masud: Usamah', *Ausaf* , 12 September 2001). I am grateful to Hamid Mir for a personal communication on the subject.

DOI: 10.19165/2020.6.0129

platforms concerning the development of cyber/hacking capabilities and impending cyber-attacks (such as DDoS attacks). In general, these either never materialized or were markedly unsuccessful.[9]

From time to time, individuals who claimed some sort of affiliation or link to Al-Qaeda would gain something of a reputation for hacking prowess. An example was Younis Tsouli, who became infamous as "Irhabi 007" ("Terrorist 007") from 2003 until his arrest a few years later. Starting out in various extremist forums where he uploaded instruction manuals on computer hacking, he began to support online operations linked to Al-Qaeda, and in 2005 became the administrator of the extremist internet forum al-Ansar. Tsouli's actual hacking ability appears to have been moderate at best, but by the time of his arrest by October 2005 he had gained a wide reputation as a hacker of some prowess, as well as having the ability to securely distribute across the internet Al-Qaeda's messages.[10]

2000s – 2015: Intent

From the early to mid-2000s, governments, analysts, and observers began to have a heightened appreciation of how terrorist organizations (such as Al-Qaeda and Hezbollah) were becoming more adept in their understanding of the possibilities that the internet and digital technologies afforded them, and how this could in turn lead to a mastery of the tools needed for a successful cyberattack.[11]

In 2011, an Al-Qaeda video called on followers and sympathizers to launch cyberattacks against Western targets. The video, which came to public attention the following year, apparently observed that the US was vulnerable to cyberattacks, just as airline security was vulnerable in 2001 in the period leading up to the 9/11 attacks. The video called on Muslims "with expertise in this domain to target the websites and information systems of big companies and government agencies."[12] However, no cyberattack from Al-Qaeda Central ever seems to have materialized.

There was an uptick in interest, and in the number of groups themselves, after the declaration of the Caliphate in 2014.[13] ISIS, as well as various pro-ISIS influencers and cheerleaders were keen in disseminating key texts online, or dispense advice to jihadi aspirants, through various online means, including (besides mainstream online platforms) encrypted messaging apps such as Telegram, which have become increasingly popular, notwithstanding recent crackdowns by Telegram itself and by national governments. Needless to say, these platforms and apps were instrumental for many individuals on various points of their radicalization journey to meet each other virtually, exchanging views and information, and, through this discourse, further

[9] *Cyber Terrorism: Assessment of the Threat to Insurance*, Cambridge: Centre for Risk Studies, November 2017. Available at: https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/pool-re-cyber-terrorism.pdf

[10] On Irhabi 007, see Corera, Gordon, 'Al-Qaeda's 007', *The Times*, 16 January 2008. See also Gabriel Weimann, 'Terror on Facebook, Twitter, and Youtube', *The Brown Journal of World Affairs*, Vol. 16, No. 2 (Spring / Summer 2010), pp. 47-48.

[11] Verton, Dan, *Black Ice: The Invisible Threat of Cyber-Terrorism* (Emeryville, CA: McGraw-Hill, 2003), p.87.

[12] Cf Catherine Herridge, Catherine 'Al Qaeda video calling for cyberattacks on Western targets raises alarm in Congress' *Fox News*, 22 May 2012. Available at: https://www.foxnews.com/politics/al-qaeda-video-calling-for-cyberattacks-on-western-targets-raises-alarm-in-congress

[13] Alkhouri, Leith, Alex Kassirer and Allison Nixon, 'Hacking for ISIS: The Emergent Cyber Threat Landscape.' *Flashpoint*, April 2016, p. 23.

DOI: 10.19165/2020.6.0129

influencing or reinforcing each other's beliefs. Further, there is evidence that *plotting* of terrorist attacks has increasingly taken place on social media, encrypted messaging apps, or the "Dark Web." In some cases, the perpetrator can be guided "remote-controlled," as it were, by an overseas mastermind, sometimes in near real-time.[14] These areas have become an increasing focus of concern for security agencies.

While various ISIS media units have been successful in disseminating messages and slickly-produced propaganda online, the lack of genuine cyber disruptive capability could be said to have continued on into the ISIS era. *Threats* of hacking were not altogether infrequent. On 11 May 2015, Rabitat Al-Ansar, a pro-ISIS collective, released a video titled, "Message to America: from the Earth to the Digital World," threatening hacking attacks against American and European targets. The following year, it tweeted plans to hack US targets, including government websites on 11 September 2015; these appear not to have materialized.

At an individual level, ISIS members or individuals with pronounced pro-ISIS sympathies did have some technical knowledge of the type to create basic attacks, and, in some cases, were able to co-opt cadres of like-minded individuals to attempt attacks. A prime example is Junaid Hussain Abu Hussain al-Britani, a UK national who went to Syria in 2013. Prior to his move, he appears to have been a hacktivist with allegiance to various causes (including the Palestinian cause, and against far-right groups in the UK; an illustration of the point that the line between hacktivism and cyberterrorism may sometimes be not all that clear-cut),[15] as well as associating with well-known hacking collectives such as Anonymous. He also founded "Team Poison," responsible for hacking NATO, and the British Ministry of Defense. He was jailed in 2012, with his incarcerations playing some part in hardening his views. After his release, he resurfaced in Syria, becoming not simply a key ISIS influencer on Twitter, but, it appears, an important member of ISIS' cyber offensive operations team. During this time Junaid attempted attacks against various websites linked either directly or indirectly with the anti-ISIS coalition (or against countries that supported anti-ISIS efforts).[16]

Other pro-ISIS elements have had basic hacking and data exfiltration ability. In 2016, Ardit Ferizi, originally from Kosovo, became the first person ever prosecuted in the US on cyberterrorism charges, in a case that, according to US officials, represented "the nexus of the terror and the cyber threats."[17] Ferizi (who was sentenced to 20 years imprisonment), went online by the moniker Th3Dir3ctorY, was arrested in Malaysia (where he had been studying computer science) in October 2015. According to the US federal criminal complaint filed against him, Ferizi and his associates stole the personal information of more than 1,300 US military and government personnel through hacking an unnamed US company. This personal information was then passed to Junaid Hussain, who, in the name of the Islamic State Hacking

[14] See Callimachi, Rukmini, 'Not 'Lone Wolves' After All: How ISIS Guides World's Terror Plots From Afar', *New York Times*, 4 February 2017.
[15] Weimann, Gabriel, 'Cyberterrorism: The Sum of All Fears?' *Studies in Conflict & Terrorism*, 28:129–149, 2005, p. 137.
[16] For Junaid Hussain, see Nafees Hamid, 'The British Hacker Who Became the Islamic State's Chief Terror Cybercoach: A Profile of Junaid Hussain', *CTC Sentinel*, April 2018, pp. 30-37; see also John P. Carlin, 'Inside the Hunt for the World's Most Dangerous Terrorist', *Politico*, 21 November 2018. Available at: https://www.politico.com/magazine/story/2018/11/21/junaid-hussain-most-dangerous-terrorist-cyber-hacking-222643
[17] 'ISIL-Linked Hacker Pleads Guilty to Providing Material Support', U.S. Department of Justice Press release, 15 June 2016. Available at: https://www.justice.gov/opa/pr/isil-linked-hacker-pleads-guilty-providing-material-support.

DOI: 10.19165/2020.6.0129

Division (ISHD), released details of these individuals in August 2015 - the same month that saw him killed in a drone strike.

The publication of the "kill list" was something of a minor propaganda coup.[18] But some of Hussain's "kill list" releases were actually not hacks nor the exfiltration of data, but detailed open source research.[19] Indeed, in the recent history of doxing and the release of kill lists, the sense is that these were not highly sophisticated attacks, with some of these releases involving (essentially) repackaged information available elsewhere.[20] A case in point was the January 2015 hack of the CENTCOM (US Central Command) Twitter and YouTube pages. Besides posting threatening messages against the US on the pages, what appeared to be US military documents (although not classified) were released.[21] This was not a hack into a sensitive military network, and was characterized (although something of a propaganda coup by the perpetrators, who may have included Junaid Hussain) as "cyber-vandalism." by US authorities.[22]

Pro-ISIS online groups such as the United Cyber Caliphate have continued what could be best described as low-level hacks, attempting DDoS attacks in 2016 and 2017.[23] The attacks were mainly focused on targets in the Middle East, and although some of the targeted sites appear to have been briefly knocked offline, the action points more towards a kind of resourcefulness rather than a high level of technical mastery.[24] Separately, hackers sympathetic to some degree

[18] Ibid. On Ardit Ferizi, see also Murphy, L. 'The Curious Case of the Jihadist who started out as a Hactivist', *Vanity Fair*, 15 December 2015. Available at: https://www.vanityfair.com/news/2015/12/isis-hacker-junaid-hussain; Hamid, 'The British Hacker Who Became the Islamic State's Chief Terror Cybercoach: A Profile of Junaid Hussain', p.35; Audrey Alexander and Bennett Clifford, 'Doxing and Defacements: Examining the Islamic State's Hacking Capabilities', *CTC Sentinel*, April 2019, pp. 23-24.

[19] Alexander, Audrey and Bennett Clifford, 'Doxing and Defacements: Examining the Islamic State's Hacking Capabilities', *CTC Sentinel*, April 2019, p. 25. Available at: https://ctc.usma.edu/doxing-defacements-examining-islamic-states-hacking-capabilities/

[20] Ibid. For other examples of releases of large Kill lists by ISIS -linked groups, see 'Pro-ISIS Hacking Group Releases Kill List Targeting Canadians, Containing Over 12,000 Entries', *MEMRI Cyber & Jihad Lab*, 29 June 2016. Available at: http://cjlab.memri.org/lab-projects/monitoring-jihadi-and-hacktivist-activity/pro-isis-hacking-group-releases-kill-list-targeting-canadians-containing-over-12000-entries/ .

[21] Lamothe, Dan, 'U.S. military social media accounts apparently hacked by Islamic State sympathizers', *Washington Post*, 12 January 2015. Available at: https://www.washingtonpost.com/news/checkpoint/wp/2015/01/12/centcom-twitter-account-apparently-hacked-by-islamic-state-sympathizers/?noredirect=on&utm_term=.e1ca1a751c71

[22] Murphy 2015; Lamothe 2015.

[23] It is important to note that many of these pro-ISIS collectives, including the UCC and the Cyber Caliphate Army, never appear to have had a formal association with ISIS "Central". The history, nomenclature and evolutions of the cyber/hacking groups said to be part of, or linked to ISIS's central arm is by no means straightforward. Many with grand names may be devolved individuals, having no formal link with the terror organization; further complicating the picture is that the recent history of groups claiming some sort of affiliation with ISIS is littered with unproven claims of mergers and associations of groups which have gone by various names, including the Caliphate Cyber-Army, Sons Caliphate Army and Kalashnikov Team, and the United Cyber Caliphate (said, in some accounts, to be the organization formed by fusing the aforementioned disparate groups). For a discussion, see Rose Bernard, 'These are not the terrorist groups you're looking for: an assessment of the cyber capabilities of Islamic State', *Journal of Cyber Policy*, Vol. 2, No. 2,2017, pp. 258-260. See also the comments of Laith Alkhouri, Alex Kassirer and Allison Nixon, in 'Hacking for ISIS: the Emergent Cyber Threat Landscape', *Flashpoint*, April 2016, p.19.

[24] Wolf, K., 'Cyber Jihadists Dabble in DDoS: Assessing the Threat', *Flashpoint*, 13 July 2017. Available at: https://www.flashpoint-intel.com/blog/cyber-jihadists-ddos/. For a detailed study of the UCC (which appears to have coalesced in 2016 as the result of the merger of previously distinct groups) and its capabilities, see Nadine Liv, *United Cyber Caliphate*, International Institute for Counter-Terrorism, 20/3/2019. Available at: https://www.ict.org.il/Article/2361/United_Cyber_Caliphate#gsc.tab=0. The UCC in some of its cyber operations also appears to have managed to compile "kill lists" by accessing servers that held data of Saudi soldiers. In yet

DOI: 10.19165/2020.6.0129

to ISIS – in this case the group known as the Tunisian Fallaga Team – carried out a series of attacks against the UK's National Health Service (NHS) – involving defacing websites to show gruesome images of the Syrian Civil War.[25]

Overall, the cyber offensive ability of groups conventionally thought of as terrorist organizations (such as Al-Qaeda or ISIS) should be considered to be of a fairly basic order, with no compelling evidence that these groups have been able to launch a full-scale cyber-attack of the type that causes harm, death, or destruction, or which has instilled fear in the population of a country.[26] While concern over potential cyberattacks has grown in recent years, commensurate with the growth in digital and cyber infrastructure, the vast majority of serious attacks that have caused either serious damage or disruption (or monetary loss) can be traced to criminal organizations, or states, but not to terrorist organizations. It is states, for the most part, who up till this point of time have a serious capability in the cyber sphere to cause destruction through cyber/digital means.[27]

The remainder of this chapter does not confine itself to what governments and the private sector have done to protect against attacks by terrorist groups or subnational groups. Good prevention and preparedness does not by its very nature attempt to distinguish who the malicious actor is, and national preparedness has to be premised facing major threats first, whatever their origin. As Gen. John Gordon, Assistant Secretary for Intelligence at DHS (also at the time serving as chairman of the Homeland Security Council), observed at the RSA Conference in 2004, "The damage will be the same whether the attacker was a bored teenager, an organized criminal or

another operation, the UCC released on its Telegram channel another kill list containing over 8,000 names and identifiers, mainly from the US and UK. Nadine Liv, *United Cyber Caliphate*, pp. 12-13; Chris Summers, 'ISIS orders American lone wolf jihadis to slaughter 8,000 citizens by releasing 'kill list' which includes the names of several Hollywood celebs', *The Daily Mail Online*, 9 June 2016.

[25] Sengupta, Kim 'Isis-linked hackers attack NHS websites to show gruesome Syrian civil war images.' *Independent, 7* February 2017. For more on the Tunisian Fallaga Team and its members, see 'Fallaga Team – Tunisian Hacker Group Engages in Jihadi Activism, Active on Twitter, Facebook, Youtube', *Middle East Media Research Institute* (MEMRI), 5 February 2015. Available at: http://cjlab.memri.org/lab-projects/monitoring-jihadi-and-hacktivist-activity/fallaga-team-tunisian-hacker-group-engages-in-jihadi-hacktivism-active-on-twitter-facebook-youtube/, and Ian Moore and Henrik Saltzstein, 'We Skyped with a 19-Year-Old Islamist Hacker from Tunisia', *VICE*, 26 Jun 2013. Available at: https://www.vice.com/sv/article/xdpeyq/we-skyped-with-a-19-year-old-islamist-hacker-from-tunisia

[26] There is some evidence that Hamas has a hacking wing. This came to light in May 2019, when the Israeli Defence Forces (IDF) announced the destruction of a building in Gaza where Hamas hackers were located. Details were scant on what the target of the Hamas cyber activity was (it appears to have been stopped online) and how advanced this capability was, but clearly it was of a nature that necessitated an immediate, real-world retaliation. The Israeli response was noteworthy as it may mark one of the first occasions that a kinetic action was made in response to hacking activity. Kate O'Flaherty, 'Israel Retaliates To A Cyber-Attack With Immediate Physical Action In A World First', *Forbes.com*, 6 May 2019. Available at: https://www.forbes.com/sites/kateoflahertyuk/2019/05/06/israel-retaliates-to-a-cyber-attack-with-immediate-physical-action-in-a-world-first/#ea907b3f8953. See also the IDF tweet at: https://twitter.com/IDF/status/1125066395010699264

[27] It is of course worth asking (but outside the scope of this chapter) why terrorists (as they are conventionally understood) have not managed to pull off a cyberattack of serious magnitude. "I'm as puzzled as you are," said Michael Hayden, who served as NSA director from 1999-2005 and CIA director from 2004 to 2008. "These folks are not cyberdumb (…) They use the web and show a great deal of sophistication in how they use it, for many purposes (…) But they have not yet used it to create either digital or physical destruction. Others have". Kathy Gilsinan, 'Will We see a Terrorist Cyberattack before Midterms?' *The Atlantic*, 1 November 2018. Available at: https://www.theatlantic.com/international/archive/2018/11/terrorist-cyberattack-midterm-elections/574504/

DOI: 10.19165/2020.6.0129

a [hostile] nation or state. We need to focus on the vulnerabilities—and not get too hung up on who the attacker will be."[28]

Cyber Attacks by Malevolent Actors

While terrorist groups lack the ability to severely impair the operations of state machinery, technologically advanced states with resources and developed cyber offensive capabilities can (given time and planning) severely impact terrorist organizations through cyberattacks (for a sense of what the various actors are capable of, see Figure 1). In 2016, the US Cyber Command and the National Security Agency commenced a major cyber operation, Glowing Symphony, which severely impacted ISIS' media operations.[29] In a separate operation from the same year, cyber operatives from the Australian Signals Directorate hacked into ISIS communications thousands of miles away, interdicting ISIS communications, directly assisting anti-ISIS coalition forces about to launch a major operation.[30]

In the pursuit of national objectives, states – and for the time being states alone - can deploy cyber weapons capable of *physical* damage. In the earlier era, assumptions on hacking and computer network attacks tended to take into account compromises of computers or networks ("disruptive" activity), assuming that critical infrastructures were less vulnerable as they were far more difficult to penetrate.[31] These assessments for the 1990s and most of the early 2000s were correct at that time, but events in recent years have shown that this assessment can no longer be regarded as tenable. As computer networks have become increasingly enmeshed with critical infrastructure, corresponding vulnerabilities have multiplied. This means that the attack surface has grown dramatically in recent years. One of the earliest cyberattacks that caused physical damage is Stuxnet, a malware which was responsible for causing damage at the Iranian uranium enrichment facility in Natanz between 2009 and 2010.[32] Stuxnet is commonly agreed by experts to have been the joint creation of the security services of the US and Israel (although both countries have not officially accepted responsibility).

Computer malware can cause physical damage and potentially loss of life (even though the latter has not yet happened). In recent years, analysts therefore have been forced to treat malware-based attacks against critical infrastructure (including ICS (Industrial Control

[28] Gen. John Gordon, 25 February 2004. See E. Montalbano, 'Homeland Security Chair likens 'Cyber Terrorists' to Al Qaeda'. *CRN News* 25 February 2004. Available at: https://www.crn.com/news/security/18825553/homeland-security-chair-likens-cyber-terrorists-to-al-qaeda.htm

[29] Temple-Raston, Dina, 'How the U.S. Hacked ISIS', *NPR*, 26 Sep 2019. Available at: https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis?utm_source=facebook.com&utm_term=nprnews&utm_campaign=npr&utm_medium=social&fbclid=IwAR2mxns6EoDAZbmR0qsV4uitkZhvwNsziYimZYmJsrl-GX3eJcoWcoBIXuM

[30] Grigg, Angus, 'Australia claims world first in cyber war', *The Australian Financial Review*, 27 March 2019. Available at: https://www.afr.com/technology/australia-claims-world-first-in-cyber-war-20190326-p517q6

[31] Lewis, James A., 'Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats' Center for Strategic and International Studies, December 2002. Available at: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf

[32] Or by some accounts as early as 2007. For Stuxnet, see David E.Sanger, 'Obama Order Sped up Wave of Cyberattacks Against Iran', *New York Times*, 1 June 2012. Available at: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html; see also: Zetter, Kim, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*,New York, NY: Broadway Books, 2014.

DOI: 10.19165/2020.6.0129

Figure 1: Cyber Attacks from Actor to Aim

	Actor	Target	Attack mode	(Primary) Aim/ Motivation
Cyber Warfare	• States	• Military and civilian infrastructure, CII (critical information infrastructure) • Private sector • Private Sector (ICS, SCADA systems) • Civilians • Government institutions • Terrorist groups and non-state actors	• APTs (Advanced Persistent Threat) and other malware (including implanting malware/APT reconnaissance prior to open hostilities) • Social engineering • Phishing attacks • Watering hole attacks • IOT attacks • Botnet Attacks • Disinformation campaigns/ • influence operations/ attacks against election system	• Force surrender; • Negotiated settlement on favorable terms • Degrade opposing side's ability in peacetime/ prior to commencement of declared hostilities • Subversion/ undermine resilience of target
Cyber Espionage	• States	• State infrastructure/ military-industrial complex • Private sector • ICS, SCADA systems	• APTs • Data exfiltration • Social engineering	• Theft of intellectual property / commercially sensitive or valuable information
Cyber Crime	• Criminal groups (including criminal groups acting on behest of states); • States	• State infrastructure • Private sector	• Malware (including ransomware) • APT • Social engineering • Phishing attacks • Watering hole attacks • IOT attacks • Botnet attacks	• Financial gain
Ideological/ Cause-based attacks/ Hacktivism	• Extremist /anti-establishment groups; • Black Hat hackers	• States • Private sector	• DDoS • Phishing • Basic malware • Defacing websites • Doxing	• Force political or social change • Sow fear in target population

DOI: 10.19165/2020.6.0129

Systems) and SCADA (Supervisory Control and Data Acquisition)) systems as a serious cyber threat. Another case in point is an attack against an unnamed steel mill in Germany that occurred, it appears, sometime in or just before 2014. The malware affected the operations of a blast furnace, causing a great deal of (unspecified) damage.[33] The malicious actor, not formally named, deployed tolls and showed skills of a high level. These included a combination of spear phishing, social engineering methods aimed at particular individuals, as well as familiarity with the not just conventional IT security systems but also mill's specialized control systems.[34]

Many cyberattacks fall just short of those described above in terms of severity (or immediacy) but still have a serious fallout. Saudi Aramco, the state petroleum and natural gas company of Saudi Arabia, was hit by a major cyberattack in August 2012 that affected 30,000 workstations. Critical files were overwritten with an image of a burning American flag. A group "Cutting Sword of Justice" claimed the attack was in retaliation for the Saudi regime's "crimes and atrocities taking place in various countries around the world."[35] The malware had a data wiping capability, and could thus be considered destructive to some degree as opposed to simple DDoS style attacks.[36] The attack was seen by some as a hacktivist attack, but state responsibility (possibly Iran) cannot be ruled out.[37]

Some cyberattacks exhibit more aspects of reconnaissance, probing vulnerabilities, or deployment of assets in advance of (or in preparation for) the outbreak of hostilities. From around 2016, for example, there began to be reports of Russian attempts to probe the US power grid. No physical damage was caused, and the probing appears to have been more of a sniff out vulnerabilities operation.[38] The US appears to have returned the favor, with evidence

[33] *Die Lage der IT-Sicherheit in Deutschland 2014*, Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security), p. 31. Available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile%20. For a discussion (and relevant excerpt of the BSI report in translation), see Lee, Robert M., Michael J Assante and Tim Conway, 'German Steel Mill Cyber Attack', *ICS Defense Use Case (DUC)*, Dec 30, 2014. Available at: https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf

[34] 'Hack caused 'massive damage' at steelworks', *BBC*, 22 December 2014. Available at: https://www.bbc.com/news/technology-30575104

[35] Perlroth, Nicole, 'Among Digital Crumbs from Saudi Aramco Cyberattack, Image of Burning U.S. Flag', *New York Times*, 24 August 2012.

[36] Leyden, John 'Hack on Saudi Aramco hit 30,000 workstations, oil firm admits', *The Register*, 29 August 2012. Available at: https://www.theregister.co.uk/2012/08/29/saudi_aramco_malware_attack_analysis/

[37] Perlroth, Nicole, 'In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back', *New York Times*, 23 Oct 2012. Triton, the malware involved in a subsequent 2017 attack against a Saudi Aramco petrochemical facility, which was said to be the first attack to directly target the safety systems of a critical infrastructure facility, was, according to experts, likely created by one or more states, with some suggesting Iran and/or Russia as the possible authors of the virus. Perlroth, Nicole and Clifford Krauss, 'A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try', *The New York Times*, 15 March 18; Elias Groll, 'Cyberattack Targets Safety System at Saudi Aramco', *Foreign Policy*, 21 December 17. Available at: https://foreignpolicy.com/2017/12/21/cyber-attack-targets-safety-system-at-saudi-aramco/

[38] Smith, Rebecca and Rob Barry, 'America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It', *The Wall Street Journal*, 10 January 2019. Available at: https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112; Greenberg, Andy, 'The Highly Dangerous 'Triton' Hackers Have Probed the US Grid', *WIRED*, 14 June 2019. Available at: https://www.wired.com/story/triton-hackers-scan-us-power-grid/, Nicole Perlroth and David E. Sanger, 'Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says', *The New York Times*, 15 March 2018. Available at: https://www.nytimes.com/2018/03/15/us/politics/russia-cyberattacks.html?module=inline

DOI: 10.19165/2020.6.0129

suggesting that relevant agencies have begun in recent years to aggressively intensify existing efforts to probe and implant malware in the Russian power grid.[39]

Government control over their cyberweapon creations is not fool proof: malware that is kept for use at a later date (or else meant for a specific use) can escape "into the wild" and be used by others. An example is the EternalBlue exploit, allegedly stolen from the National Security Agency (NSA) in 2016 and leaked online in April 2017 by a group known as Shadow Brokers. This, in turn, enabled high profile cyberattacks, including the infamous WannaCry attacks, used by states as well as cybercriminals, as well as the 2017 NotPetya malware campaign, which crippled parts of the Ukrainian government (an attack thought to have been executed by the Russian military) before spreading to multinational corporations such as FedEx and Maersk, causing billions in damage.[40]

Certain states that might be considered "rogue" nations might attempt cyber offensive methods that are more commonly associated with criminal enterprises. North Korea, for example, is thought to have been responsible for a string of attacks against various state and non-state targets. Its activities in recent years have included cyber theft and attacks against the international banking system. These attacks, which included hacks against cryptocurrency exchanges, generated income to fund, inter alia, North Korea's nuclear program.[41] These hacks also included attacks against the international banking system through the exploitation of weaknesses of the SWIFT payments system, most notably a February 2016 heist which saw the theft of $81 million from the account of the Bangladesh Central Bank at the Federal Reserve Bank of New York.[42] APT 38, a group linked to the North Korean regime, is thought to be responsible, and has also been linked to cyber heists targeting numerous other financial institutions.[43]

When states undertake a course of offensive cyber action, there are often "guardrails" that might prevent collateral damage. The malware might, for instance, have an expiration date, or else it might be precisely tailored and only usable in certain locations and contexts.[44] But states that occasionally exhibit "rogue" cyber behavior do not exhibit such guardrails, with the

[39] Sanger, David E. and Nicole Perlroth, 'U.S. Escalates Online Attacks on Russia's Power Grid', *New York Times*, 15 June 2019. Available at: https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html

[40] 'When Cyberweapons Escape', The Soufan Center. Available at: https://www.thecipherbrief.com/column/soufan-center/when-cyberweapons-escape; Andy Greenburg, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History', *WIRED*, 22 August 2018. Available at: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/) and Lee Matthews, "Not Petya ransomware attack cost Shipping Giant Maersk Over $200 Million', *Forbes*, 16 August 2017. Available at: https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-costshipping-giant-maersk-over-200-million/#7e0f16a34f9a

[41] Goodin, Dan, 'Meet the three North Korean hacking groups funding the country's weapons programs', *Ars Technica*, 14 September 2019. Available at: https://arstechnica.com/tech-policy/2019/09/us-sanctions-north-korean-hackers-for-wannacry-and-dozens-of-other-attacks/; Perez, Evan and David Shortell, 'North Korean-backed bank hacking on the rise, US officials say', *CNN*, 1 March 2019. Available at: https://edition.cnn.com/2019/03/01/politics/north-korea-cyberattacks-cash-bank-heists/index.html

[42] Hammer, Joshua 'The Billion Dollar Bank Job', *The New York Times Magazine*, 3 May 2018. Available at: https://www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html

[43] For discussion, see 'APT 38: Un-usual Suspects', *FireEye*, 3 October 2018. Available at: https://content.fireeye.com/apt/rpt-apt38. See also Shannon Vavra, 'Cyber Command flags North Korean-linked hackers behind ongoing financial heists', *Cyberscoop*, 11 November 2019. Available at: https://www.cyberscoop.com/north-korea-malware-cyber-command-virus-total-apt38/

[44] Stilgherrian, 'North Korea is the most destructive cyber threat right now: FireEye', *ZDnet*, 5 October 2018. Available at: https://www.zdnet.com/article/north-korea-is-the-most-destructive-cyber-threat-right-now-fireeye/

DOI: 10.19165/2020.6.0129

malware either capable of causing indiscriminate damage, or the attack itself designed to be visible and to embarrass or draw attention to the attack or the target. The well-known cyber hack against Sony Pictures, allegedly carried out by North Korea in 2014, is a case in point, with confidential Sony documents posted online by the hackers.[45]

Cyber strikes may be carried out by states in retaliation for certain actions. In the wake of the drone and missile attacks against Saudi oil processing facilities in Abqaiq and Khurais on 14 September 2019, for example, reports suggested that the US carried out a retaliatory cyber strike against Iran, the country which was widely thought to have been behind the attack on Saudi Arabia. This cyber strike was severe enough to affect physical hardware.[46] The US also appears to have carried out a cyberattack in June 2019 against Iranian maritime installations, partly as retaliation for attacks in May and June 2019 against shipping in the Gulf of Oman and the Persian Gulf, and the destruction of a US drone by an Iranian missile on 20 June 2019.[47]

States with advanced capabilities routinely engage in cyber espionage and theft of intellectual property as well. An example of an APT group linked to a series of hacks attempting to steal intellectual property and industrial secrets is APT 10/Cloudhopper, which has been linked to the Chinese Ministry of State Security (MSS).[48] The cyberattack against the Norwegian software firm Visma in 2018 which saw client information stolen also appears to have been carried out by hackers working on behalf of the Chinese state security apparatus (part of a wider, organized campaign.)[49] In the US in particular, there has, in recent years, been considerable discussion and public debate about the scale of intellectual property theft conducted by China, with then-National Security Agency Director and Commander of Cyber Command Keith Alexander calling this in 2012 "the greatest transfer of wealth in history."[50]

As events of recent years have shown, some states are willing and able to attack other states using cyber means (hacking) combined with social media manipulation, information warfare, troll farms, hackers, and cyber espionage operating in a mesh. The aim can be to undermine the resilience of a country, to humiliate it, or to influence the course of the democratic process.

---

[45] Peterson, Andrea, 'The Sony Pictures hack, explained', *Washington Post*, 19 December 2014. Available at: https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/. The hack was thought by officials to be in retaliation for a film financed by Sony which depicts an assassination plot against North Korean leader Kim Jong-un.

[46] Ali, Idrees, and Phil Stewart, 'Exclusive: U.S. carried out secret cyber strike on Iran in wake of Saudi oil attack: officials', *Reuters*, 16 October 2019. Available at: https://www.reuters.com/article/us-usa-iran-military-cyber-exclusive/exclusive-u-s-carried-out-secret-cyber-strike-on-iran-in-wake-of-saudi-oil-attack-officials-say-idUSKBN1WV0EK

[47] Halpern, Sue, 'How Cyberweapons are Changing the Landscape of Modern Warfare', *The New Yorker*, 18 July 2019. Available at: https://www.newyorker.com/tech/annals-of-technology/how-cyber-weapons-are-changing-the-landscape-of-modern-warfare

[48] Christopher Bing, Jack Stubbs and Joseph Menn, 'Exclusive: China hacked HPE, IBM and then attacked clients – sources', *Reuters*, 21 December 2018. Available at: https://www.reuters.com/article/us-china-cyber-hpe-ibm-exclusive/exclusive-china-hacked-hpe-ibm-and-then-attacked-clients-sources-idUSKCN1OJ2OY. For a detailed study on APT 10/Cloudhopper, see *Operation Cloud Hopper: Exposing a systematic hacking operation with an unprecedented web of global victims*. PricewaterhouseCoopers and BAE Systems, April 2017. Available at: https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf

[49] Jack Stubbs, 'China hacked Norway's Visma to steal client secrets: investigators', *Reuters*, 6 February 2019. Available at: https://www.reuters.com/article/us-china-cyber-norway-visma/china-hacked-norways-visma-to-steal-client-secrets-investigators-idUSKCN1PV141

[50] Josh Rogin, 'NSA Chief: Cybercrime constitutes the "greatest transfer of wealth in history"', *Foreign Policy*, 9 July 2012. Available at: https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/

DOI: 10.19165/2020.6.0129

Although a full treatment would be beyond the scope of this chapter, it is worth at this point to consider briefly Russian interference in the 2016 presidential election in the US. One prong of this interference involved subversion and the creation of fake groups on social media to sow dissension in society. Another prong involved hacks and subsequent publishing of stolen material from the Democratic National Committee's servers in 2015 and 2016, by (it appears) more than one group linked to Russian intelligence services.[51] One of the groups involved, Fancy Bear (or APT 28), which has been linked to GRU, Russia's military intelligence agency, is thought to be responsible for the 2015 hack of the German Bundestag.[52] German officials were clear that the Russian state could, if it wished, release the exfiltrated messages in the form of doxed material or for disinformation purposes, or to damage the integrity of the German elections.[53] The same group has been identified as being behind the attempted interference (through the exfiltration and publication of emails) in the 2017 election campaign of presidential candidate Emmanuel Macron.[54]

Finally, activity by criminal or hacktivist elements not linked to states also needs to be considered. In recent years, cybercriminals have in recent years been capable of causing a type of severe impairment which - while not amounting to physical damage - can still hinder certain types of operations. In March 2018, for example, Atlanta's municipal administration (including government departments and the police records system) was severely affected by ransomware attacks using the SamSam virus which saw the administration of this American city spend over $2.5 million to regain control.[55] In addition to the financial sector, in recent years the healthcare sector has also increasingly come into the crosshairs of criminal enterprises. Theft of data (including research data) and personal information can be very lucrative, as the data can be used for identity theft and can be resold on the Dark Web. Increasingly, a particular risk area for healthcare has been the use of Internet-of-Things (IOT) -enabled devices (such as pacemakers) which can be compromised.[56] More generally, it appears to be just a matter of time before the nascent IOT is compromised in other sectors as well. While some of the

[51] Poulsen, Kevin 'Russian Cyber Unit That Went Dark After Hacking DNC Is Still Spying', *The Daily Beast*, 17 October 2019. Available at: https://www.thedailybeast.com/the-dukes-russian-intels-cyber-unit-that-went-dark-after-dnc-hack-is-still-spying .

[52] For a riveting blow by blow account, see Beuth, Patrick Kai Biermann, Martin Klingst and Holger Stark, 'Merkel and the Fancy Bear', *Die Zeit*, 12 May 2017. Available at: https://www.zeit.de/digital/2017-05/cyberattack-bundestag-angela-merkel-fancy-bear-hacker-russia/komplettansicht.

[53] Tyson Barker, 'German Strengthens its Cyber Defense', *Foreign Affairs*, 26 May 2017.

[54] 'Macron hackers linked to Russian-affiliated group behind US attack', *The Guardian*, 8 May 2017. Available at: https://www.theguardian.com/world/2017/may/08/macron-hackers-linked-to-russian-affiliated-group-behind-us-attack

[55] For the Atlanta attacks, see Lily Hay Newman, 'Atlanta Spent $2.6M to Recover from a $52,000 Ransomware Scare', *WIRED*, 23 April 2018. Available at: https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/; and Benjamin Freed, 'One year after Atlanta's ransomware attack, the city says it's transforming its technology', *Statescoop*, 22 March 2019. Available at: https://statescoop.com/one-year-after-atlantas-ransomware-attack-the-city-says-its-transforming-its-technology/. The attacker demanded a Bitcoin payment roughly equal to $51,000, but it is unclear whether this sum was paid. For a similar ransomware attack against Baltimore in May 2019 that caused approximately $18 million in damage, see Christine Fisher, 'A ransomware attack is holding Baltimore's networks hostage', 8 May 2019. Available at: https://www.engadget.com/2019/05/08/baltimore-city-government-ransomware-attack/#comments

[56] For an introduction to the issues in the healthcare industry, see *Beyond Compliance: Cyber Threats and Healthcare*, *FireEye*, 23 Augustus 2019. Available at: https://content.fireeye.com/cyber-security-for-healthcare/rpt-beyond-compliance-cyber-threats-and-healthcare. See also Kate O'Flaherty, 'Why Cyber-Criminals Are Attacking Healthcare - And How To Stop Them', *Forbes*, 5 October 2018. Available at: https://www.forbes.com/sites/kateoflahertyuk/2018/10/05/why-cyber-criminals-are-attacking-healthcare-and-how-to-stop-them/#4e19e6847f69

DOI: 10.19165/2020.6.0129

methods themselves are not yet firmly in place, there is evidence that the criminal underground is on the lookout for ways to refine its approaches in this respect.[57]

Individual hackers or small hacker collectives have not yet reached a level capable of causing serious disruption or major monetary loss, but their activities have on occasion garnered attention from media and law enforcement. A case in point is LulzSec, a loose hacker collective with a small group of members which was behind various hacks in 2011. LulzSec's activities included attacks against Fox Broadcasting, Britain's National Health Service (NHS), and Sony Pictures (attacks included gaining access to administrator passwords, causing website outages, and accessing customer details). Law enforcement in the UK and the US took action and some of the members were arrested and charged.[58]

There have been occasions where the actions of individual actors or small groups have had an outsized effect on ICT infrastructure. One example is the Mirai botnet, created in 2016 by three college-age students in the US, for no greater purpose than trying to gain an advantage in the online game Minecraft. Mirai eventually escaped into the wider online world, taking control of a huge number of other computers and IOT-enabled devices. Together with the various variants it spawned, it was from October 2016 to early 2017 responsible for over 15,000 individual DDoS attacks, and for a time affected the internet in the Eastern US.[59]

[57] Stephen Hilt, Vladimir Kropotov, Fernando Mercês, Mayra Rosario, and David Sancho, 'The Internet of Things in the Cybercrime Underground', *Trend Micro Research*, 10 September 2019. Available at: https://documents.trendmicro.com/assets/white_papers/wp-the-internet-of-things-in-the-cybercrime-underground.pdf

[58] Jana Winter, 'EXCLUSIVE: Infamous international hacking group LulzSec brought down by own leader', *FOX News*, 6 March 2012. Available at: https://www.foxnews.com/tech/exclusive-infamous-international-hacking-group-lulzsec-brought-down-by-own-leader

[59] Garrett M.Graff, 'How a Dorm Room *Minecraft* Scam Brought Down the Internet', *WIRED*, 13 December 2017. Available at: https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/#

DOI: 10.19165/2020.6.0129

Part II: Four Tiers of Preparedness and Prevention

"We will be in a world of ceaseless and pervasive cyber insecurity and cyber-conflict against nation-states, businesses and individuals."

- Glenn S. Gerstell, General Counsel, National Security Agency, September 2019[60]

This section will discuss the four tiers of preparedness and prevention: international cooperation; government; private sector; and the public.

1. International Level

In the past, there have been global (or regional) efforts to strengthen cooperation on cyber issues through treaties and international agreements. An example is the Convention on Cybercrime, commonly known as the Budapest Convention, which entered into force in 2004.[61] The Convention covers (inter alia) information sharing and mutual assistance, as well as developing a common framework for tackling cybercrime, including interference into computer and ICT systems.

Efforts like the Budapest Convention might be considered useful beginnings, but the critical issues within the global cyber debate continue to be argued over, with key protagonists unable to reach agreement on what exactly constitutes cyber conflict (and what level of cyber operations qualify as "use of force" or "attack"), whether the law of armed conflict applies in cyberspace, and what constitutes acceptable state behavior in cyberspace both in times of conflict and peace, and what constitutes acceptable and proportional response to a cyber-attack.[62] Academics and experts have from time to time made efforts to come up with (necessarily non-binding) manuals on these issues.[63] While some of these efforts have been well-received, they have had limited real-world effect. The same may be said of efforts by

[60] Gerstell, Glenn S., 'I Work for N.S.A. We Cannot Afford to Lose the Digital Revolution', *New York Times*, 10 September 2019. Available at: https://www.nytimes.com/2019/09/10/opinion/nsa-privacy.html

[61] *The Convention on Cybercrime of the Council of Europe (CETS No.185).* Available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800815 61

[62] For a useful introduction to some of the issues through the prism of the thinking of a country that has given considerable thought to crucial critical issues, see the Dutch Minister of Foreign Affairs' *Letter to the parliament on the international legal order in cyberspace*, 26 September 2019, and *Appendix: International law in cyberspace.* Available at: https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace. For commentary, see Michael Schmitt, 'The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis', *Just Security*, 14 October 2019. Available at: https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/

[63] Schmitt, M (Ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), and M. Schmitt (Ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017).

DOI: 10.19165/2020.6.0129

individual governments – even well-regarded ones which have done considerable thinking on these issues – to set out national positions on some of these very problem-fraught issues.[64]

It is no accident that some of the key norm-shaping mechanisms have been conceived under the ambit of the UN. The UN Secretary-General António Guterres himself has on several occasions expressed concern over the use of cyber means for malicious purposes, noting that cyberattacks had contributed to diminishing trust among states.[65] Cyber features prominently in the UN' Agenda for Disarmament, especially when it comes to promoting responsible behavior and ensuring peace and stability in cyberspace.[66] There are, at the time of the writing of this chapter, within the UN two separate ongoing deliberative processes that are ongoing – the UN Group of Governmental Experts (GGE) and the UN Open-Ended Working Group (OEWG). Both seek to address the issue of promoting responsible state behavior in cyberspace.[67]

A full discussion on global debates on international norms, rules of the road, and acceptable state behavior falls beyond the scope of this chapter. However, it can be observed here that amidst ambiguity and lack of settled consensus on norms, some powers could be said to have already entered into a state of *undeclared* cyber warfare – activity that is usually deniable (or denied) and calibrated to stop just short of the level that might invite an armed response or a declaration of hostilities in the physical world.[68] Given this reality, and given the absence of any likelihood of global agreement on acceptable behavior in cyberspace, governments themselves, depending on national contexts, often have had to take the overall lead in securing sovereign cyber defenses. The private sector (given the risks of damaging hacks, ransomware and IP theft) has also begun to pay considerably more attention to cybersecurity than in the past. Finally, good cyber hygiene and preparedness at the level of the individual has also been increasingly emphasized by experts and governments as the cornerstone of cyber resilience.

2. Government/National Level – The Cyber Ecosystem

[64] For an example, see Schmitt, M. 'The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis'.

[65] *Securing Our Common Future: An Agenda for Disarmament*. United Nations Office for Disarmament Affairs (New York, 2018), p. 56. Available at: https://s3.amazonaws.com/unoda-web/wp-content/uploads/2018/06/sg-disarmament-agenda-pubs-page.pdf#view=Fit.

[66] *Securing Our Common Future: An Agenda for Disarmament*, pp. 56-57. Cyber also features in the implementation plan in the Agenda, in terms of prevention of malicious cyber activity and fostering an adherence to accountability and adherence to international cyber norms. Available at: https://www.un.org/disarmament/sg-agenda/en/

[67] For a basic introduction to the two processes and some issues under discussion, see Nele Achten, 'New U.N. Debate on Cybersecurity in the Context of International Security', *Lawfare*, 30 September 2019. Available at: https://www.lawfareblog.com/new-un-debate-cybersecurity-context-international-security; Gillian Goh, 'Overview of the Group of Governmental Experts and Open-ended Working Group Processes'. Available at: https://www.unidir.org/sites/default/files/conferences/pdfs/overview-of-the-group-of-governmental-experts-and-open-ended-working-group-processes-eng-0-786.pdf, 'UN GGE and OEWG', *Geneva Internet Platform Digital Watch Observatory*. Available at:
https://dig.watch/processes/un-gge

[68] As one observer has put it, "In many ways, nation-state cyber-wars are already well underway. The lack of established international norms means that many cyber-attacks fall into a grey area below the threshold of total war." Isaac R Porsche III, 'Fighting and Winning the Undeclared Cyber War', 24 June 2019. *The Rand Blog*. Available at:
https://www.rand.org/blog/2019/06/fighting-and-winning-the-undeclared-cyber-war.html

DOI: 10.19165/2020.6.0129

As we increasingly become networked at a personal level, and as the economic foundations of states are increasingly tied to digital infrastructure and the digital economy, governments, corporations, individuals and national (as well as international) ICT infrastructures face an enormous range of threats. These span from state actions almost amounting to cyberwarfare to hacking, espionage (which can involve the theft of secrets and IP), to botnets created for various purposes.

That is just the present. With an unavoidable future of information technology ever more embedded in our everyday lives, plus the promise – and peril – of the Internet of Things (IOT), cyber threats that did not exist in a not-so distant past are now moving from the realms of the conceptual into concrete emergent threats. The intensification of the threat should not therefore be measured solely in terms of numbers of malware attacks; the diversification of the malware itself and evolution of hackers' methods bear watching.[69]

The use of Artificial Intelligence (AI) in cyberattacks is a case in point. Experts note that conceptual models for AI-powered attacks (for example, to evade anti-virus mechanisms, or to crack passwords) exist and can be used to strengthen existing malware.[70] There have already been cases of voice "deepfakes" used to trick unsuspecting company employees to make payments to fraudulent accounts (by using AI to convincingly spoof the voice of the CEO or senior company official).[71]

The cyber environment is therefore by default a compromised one. Cybersecurity has had to become much more than simply the state or its constituent parts repelling attacks. Governments and corporations alike have increasingly come to acknowledge that cybersecurity paradigms envisaging complete protection, and all attacks repelled, is chimerical. Rather than focusing on absolute prevention, or trying to achieve a "good" level of cybersecurity, some of the most practical – not to mention sensible - approaches emphasize overall risk mitigation, minimizing the impact of cyber intrusions, and defense-in-depth to enable systems continuity.[72] In practice, this means a shift in focus toward cyber resilience, which the US National Institute of Standards and Technology, has usefully defined as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources."[73]

---

[69] For some observations, see Sam Cook, 'Malware Statistics and Facts for 2019', *Comparitech*, 15 August 2019. Available at: https://www.comparitech.com/antivirus/malware-statistics-facts/

[70]For a sense of the possibilities, see Adam Jonofsky, 'AI Could Make Cyberattacks More Dangerous, Harder to Detect', *The Wall Street Journal*, 13 November 2018. Available at: https://www.wsj.com/articles/ai-could-make-cyberattacks-more-dangerous-harder-to-detect-1542128667?mod=article_inline, and Dan Patterson, 'How weaponized AI creates a new breed of cyber-attacks', *TechRepublic*, 16 Augustus 2018. Available at: https://www.techrepublic.com/article/how-weaponized-ai-creates-a-new-breed-of-cyber-attacks/

[71] 'Fake Voices 'help cyber-crooks steal cash'', *BBC*, 8 July 2019. Available at: https://www.bbc.com/news/technology-48908736

[72] See, for example, Australian Signals Directorate/Australian Cyber Security Centre, *Strategies to Mitigate Cyber Security Incidents – Mitigation Details*, February 2017. Available at: https://www.cyber.gov.au/sites/default/files/2019-03/Mitigation_Strategies_2017_Details_0.pdf and National Security Agency, 'NSA'S Top Ten Cybersecurity Mitigation Strategies', March 2018. Available at: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf

[73] Ross, Ron, Victoria Pillitteri, Richard Graubart, Deborah Bodeau and Rosalie McQuaid, *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*, NIST Special Publication 800-160, Vol. 2, November 2019, p. xiv. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf. As the authors observe, "Cyber resilient systems operate more like the human body than a finite-state computer. The human body has a powerful

DOI: 10.19165/2020.6.0129

One aspect of resilience and overall risk management has to do with technical approaches and systems engineering. This might involve regular systems upgrades and building in of specific redundancies and back-ups with the system. These should not be treated as an afterthought: the systems that are genuinely cyber resilient are those which have these security features and redundancies built into the architecture from the design stage. If done correctly, the mission-critical functions of an enterprise will be better able to withstand cyberattacks, respond adaptively, and also operate even when compromised to some degree.[74]

States that have considered the issue deeply, however, assess that cyber resilience is not simply a technical or engineering competence. High-level direction and decision, as well as a comprehensive vision, is necessary in order to communicate national objectives in the cyber domain.[75] Increasingly, this has come in the guise of holistic cyber security strategies or masterplans. These might encompass (for example) robustness (containing threats and repelling them), resilience (which either at the government or private sector level might involve mitigation, sharing information, public education), and other aspects of defense (early warning, deterrence), with these three factors being interdependent.[76] By the end of 2018, over 90 countries had such a strategy.[77] The actual content however varies from country to country: Finland's Cyber Security Strategy has three main prongs: the development of international cooperation, better coordination of cybersecurity management, planning and preparedness of cyber security and the development of cyber security competence and skills, while the four pillars of Singapore's Cybersecurity Strategy pertain to resilient infrastructure(s), a safer cyberspace, a vibrant cybersecurity ecosystem, and strong international partnerships.[78]

Government has a critical role in instilling a mindset and culture of cybersecurity throughout all levels of society. It also sets standards (e.g. through regulation), and ensures accountability. Transparency at all levels (government, the private sector, and the public at large) is critical in

immune system that absorbs a constant barrage of environmental hazards and provides the necessary defense mechanisms to maintain a healthy state. The human body also has self-repair systems to recover from illness and injury when defenses are breached. But cyber resilient systems, like the human body, cannot defend against all hazards at all times." (Op. cit., p.xvi).

[74] Ross, Ron Developing Cyber Resilient Systems: A Systems Security Engineering Approach. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf pp. 1-2 & pp.10-11 (for a detailed discussion on techniques for cyber resilience from an engineering/systems perspective).

[75] This can involve discussion and thinking at the very fundamental level: who deals with cyber threats? One authority? Or is an interagency model to be preferred? For some sense of the thinking in Israel which has pondered these questions deeply, and which has gone through various evolutions (and now has a single agency responsible for cyber in the civilian domain, the National Cyber Directorate), see Eviatar Matania, Lior Yoffe and Tal Goldstein, 'Structuring the national cyber defence: in evolution towards a Central Cyber Authority', *Journal of Cyber Policy*, Vol.2 (Issue 1), 2017, pp. 16-25.

[76] Many such national frameworks exist – either fully formed or implemented as official strategy, or put forward as conceptual proposals. This author has found particularly useful the framework contained in Eviatar Matania, Lior Yoffe, and Michael Mashkautsan, 'A Three-Layer Framework for a Comprehensive National Cyber-security Strategy', *Georgetown Journal of International Affairs*, Volume 17, Number 3, Fall/Winter 2016, pp. 77-78.

[77] 'National Cyber Security Strategies Reveal States' Thinking about Rules in the Cyberspace', NATO Cooperative Cyber Defense Center of Excellence. Available at: https://ccdcoe.org/news/2019/national-cyber-security-strategies-reveal-states-thinking-about-rules-in-the-cyberspace/. All countries within the EU have a cyberstrategy. Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies

[78] *Finland's Cyber Security Strategy 2019, Turvallisuuskomitea* (The Security Committee). Available at: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf;
Singapore's Cybersecurity Strategy. Available at:
https://www.csa.gov.sg/news/publications/~/media/0ecd8f671af2447890ec046409a62bc7.ashx

DOI: 10.19165/2020.6.0129

order for relevant agencies to obtain a holistic threat picture. Several nations have thus introduced within their cyber legislation or frameworks mandatory reporting of cyber breaches – especially breaches that cross a certain threshold of severity. Australia, for example, made it a legal requirement through its Notifiable Data Breaches Scheme in 2017 for organizations to notify individuals as soon as practicable when their personal information is involved in a data breach that is likely to result in "serious harm."[79] Typically, overarching cyber legislation extends to cover the private sector, with governments assessing that cybersecurity is a public good that cannot be provided by the market. A further calculation is that it is unsatisfactory to allow cybersecurity standards to be left to the private sector (which might see cybersecurity primarily as a cost item, or which might lack incentives to invest in cybersecurity) to decide.[80]

At the heart of national cyber defenses, in terms of operational readiness, ought to be a Computer Emergency Response Team (CERT). Ideally, this should be much more than a team of technical experts attempting to defeat malware attacks. Although the core work of CERTs involves minimizing the risks and effects of cyberattacks, effective CERTs look holistically at the cyber threat surface and mitigation efforts: these might involve data security, endpoint security, testing and national (or sector-specific) cyber drills.

Near the top of state/CERT priorities for cyber defense has to be the protection of critical information infrastructures (CII) – computer systems directly involved in the provision of essential services. Examples might be the power grid, telecommunications services or the banking system. CII are complex and often interdependent, and the prospect of a sophisticated cyberattack crippling CII (potentially with knock on effects cascading through the economy and through other sectors) has now become a tangible threat.[81] It is on account of this that national cybersecurity exercises for key CII are a regular occurrence for states which prioritize cybersecurity. Besides multi agency involvement from the government, the best of these exercises bring in the private sector (which would have an operational involvement, or sometimes ownership in whole or in part) over the sector in question. One such exercise (held in November 2019) was GridEx V, which tested responses in real-time to cyber/physical threats against the North American energy grid. Over 6,500 participants from 425 government and energy sector organizations (from the, Canada, and Mexico) participated in the biennial event. Given the interdependencies and potential learning points, it is unsurprising that there was representation from other CII sectors (including telecommunications and natural gas.[82]

Governments are often in receipt of the most up to date cyber threat intelligence. Mechanisms need to be devised to share information on specific threats, or provide guidance of a more general variety from time to time to the private sector. The Australian Cyber Security Centre (ACSC) for example shares detailed strategies with organizations to manage or mitigate cyber

[79] Asha Barbaschow, 'Australia's Notifiable Data Breaches scheme is now in effect', *ZDNet*, 22 February 2018. Available at: https://www.zdnet.com/article/australias-notifiable-data-breaches-scheme-is-now-in-effect/

[80] Even where the private sector recognizes the need for effective cybersecurity measures and mitigation and is willing to allocate resources to this end, it may still see cybersecurity primarily as an issue of technical protection. A government's law enforcement arm, however, may have priorities such as the identification of the threat actor. See the trenchant remarks of Myriam Dunn Cavelty and Victor Mauer, 'Introduction', in Myriam Dunn Cavelty and Victor Mauer (Eds.), *International CIIP Handbook Vol.II: Analysing Issues, Challenges, and Prospects.* Center for Security Studies, ETH Zurich, 2006, p. 11. Available at: https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP-HB-2006-2.pdf

[81] See Cavelty, Myriam Dunn, 'Understanding Critical Informational Infrastructures: An Elusive Quest', in Myriam Dunn Cavelty and Victor Mauer (Eds.), *International CIIP Handbook Vol.II*, pp. 36-37.

[82] Kovacs, Eduard 'Security of North American Energy Grid Tested in GridEx Exercise', *Security Week*, 18 November 2019. Available at: https://www.securityweek.com/security-north-american-energy-grid-tested-gridex-exercise

DOI: 10.19165/2020.6.0129

threats, with its 'Essential Eight Maturity Model' coming from three tiers of maturity that enables organizations to see how fully aligned they are with the mitigation strategy.[83]

Public-private partnerships can be useful in several respects. Chief among them is the creation of mechanisms that enable information sharing on cyber threats. One example is the US Information Sharing and Analysis Centers (ISAC) in the US, created in 1998, as a public/private sector partnership that serves to share information on cyber threats at the industry level with the aim of protecting critical infrastructure.[84] These efforts were supplemented in 2015 by the addition of more devolved (and in theory sector-agnostic) Information Sharing and Analysis Organizations (ISAO), with President Obama tellingly observing at their creation that "Government cannot do this alone. The fact is, the private sector cannot do this alone either, as the government has the latest information on threats".[85]

Other nations have developed their own models for sharing information and bringing both public and private sectors up to speed on cyber threats. The UK's National Cyber Security Centre (NCSC) is an example. The NCSC has access to government intelligence on cyber threats, but also pools together experts from both government and private sector, disseminating its threat analyses and assessment to critical infrastructure providers in and out of government.[86]

3. The Private Sector

As organizations transform their businesses, the threat surfaced has vastly enlarged, particularly with IOT devices increasingly embedded in processes.[87] It has become commonplace that "there are only two types of companies – those that know they've been compromised, and those that don't know. If you have anything that may be valuable to a competitor, you will be targeted, and almost certainly compromised."[88] Private sector enterprises have to consider risk mitigation and cyber resilience as seriously as the government, which itself often has limited ability or leverage to be able to enforce some of the best practices discussed above.

---

[83] Australian Signals Directorate (Australian Cyber Security Centre), *Essential Eight Maturity Model* (July 2019). Available at: https://www.cyber.gov.au/publications/essential-eight-maturity-model

[84] Vijayan, Jaikumar, 'What is an ISAC or ISAO? How these cyber threat information sharing organizations improve security', *CSO Online*, 9 July 2019. Available at: https://www.csoonline.com/article/3406505/what-is-an-isac-or-isao-how-these-cyber-threat-information-sharing-organizations-improve-security.html

[85] Statt, Nick, 'Obama signs information-sharing order as privacy question looms', *CNET*, 13 February 2015. Available at: https://www.cnet.com/news/obama-signs-information-sharing-order-as-privacy-question-looms/

[86] See Calam, Mary David Chinn, Jonathan Fantini Porter, and John Noble, 'Asking the right questions to define government's role in cybersecurity', *McKinsey*, September 2018. Available at: https://www.mckinsey.com/industries/public-sector/our-insights/asking-the-right-questions-to-define-governments-role-in-cybersecurity, National Security Cyber Centre, *Cyber Essentials. Available at*: https://www.cyberessentials.ncsc.gov.uk/

[87] See the observations in Harald Bauer, Gundbert Scherf, and Valerie von der Tann, 'Six ways CEOs can promote cybersecurity in the IoT age', *McKinsey*, August 2017. Available at: https://www.mckinsey.com/featured-insights/internet-of-things/our-insights/six-ways-ceos-can-promote-cybersecurity-in-the-iot-age

[88] Gross, Michael Joseph, 'Enter the Cyber-Dragon', *Vanity Fair*, 2 August 11 (giving the original source for the oft-repeated quote, cybersecurity expert Dmitri Alperovitch.). Available at: https://www.vanityfair.com/news/2011/09/chinese-hacking-201109

DOI: 10.19165/2020.6.0129

Certain sectors have a holistic appreciation of cyber threats, and have a strong incentive to put in place measures to protect their systems and client data. Notwithstanding several well-known successful attacks against them, financial institutions (to take one example) do regular penetration testing, and share information on threats with national cyber authorities or with the financial regulator. But in practice, this level of vigilance and mitigation is not consistently replicated throughout the private sector. One all-too-common error is treating cyber-security as an issue solely in the domain of IT specialists; another is that executives at the C-Suite level may simply treat cybersecurity as another cost item. Even where managements might be willing to allocate resources to cybersecurity, the assumption often is that the issue can be dealt with by allocating funds in the budget cycle. Many companies fail to appreciate that this is far from sufficient. Given that cyber-threats represent in fact a global enterprise risk, mindset shifts are required from top management down, with cyber taking center stage rather than being tacked on as an afterthought.

The actual best practices for cybersecurity are well-known, and, if the right mindset exists at the management and employee level, relatively simple to implement. Some examples:

- Providing appropriate training of employees to understand the vulnerabilities (both cyber and behavioral); embedding data security in every aspect of daily operations.
- Downloading the latest security software and patches; protecting resources through regular maintenance (including remote maintenance).
- Use of two-factor authentication, or other means (for example, physical tokens) identify verification; other forms of access management.
- Use of encryption; secure connections to websites (https as opposed to http) at scale.[89]
- Other systems safeguards (segmentation; privilege restriction; Enterprise Digital Rights Management; creating redundancies).
- Use of automated scanning and testing; endpoint detection and response.[90]

What has been presented above should (in theory at least) operate in a situationally-aware mesh. While there are no failsafe solutions either individually or in combination, observing these tenets does afford a degree of mitigation and preparedness.[91] Several high-profile cyberattacks have been shown through subsequent investigation to have been avoidable if such measures of a basic nature had been in place. For example, the breach of the credit reporting agency Equifax in 2017, which resulted in the compromise of data pertaining to just under 150 million individuals, could have been prevented by installing basic patches for a vulnerability that had been known for months.[92]

---

[89] See Sulmeyer, Michael, 'How the U.S. can play Cyber Offense'. *Foreign Affairs*, 22 March 2018. Available at: https://www.foreignaffairs.com/articles/world/2018-03-22/how-us-can-play-cyber-offense.

[90] What has been presented above is necessarily a brief treatment of various preparedness, mitigation, and cyber resilience measures. For detailed discussion, see further Ron Ross, Victoria Pillitteri, Richard Graubart, Deborah Bodeau and Rosalie McQuaid, *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*, NIST Special Publication 800-160, Vol. 2, November 2019, pp. 10-11.

[91] The use of two factor or multi-factor authentication is (for example) not perfect, and there have been an increasing number of sophisticated attempts (including those using social engineering) that attempt to defeat it. See Zak Doffman, 'FBI Issues Surprise New Cyber Attack Warning: Multi-Factor Authentication is Being Defeated', *Forbes*, 7 October 2019. Available at:
https://www.forbes.com/sites/zakdoffman/2019/10/07/fbi-issues-surprise-cyber-attack-warningurges-new-precautions/#3ac359b27efb

[92] Newman,Lily Hay, 'Equifax officially has no Excuse', *WIRED*, 14 September 2017. Available at: https://www.wired.com/story/equifax-breach-no-excuse/. The US Justice Department in February 2020 charged officers from the Chinese People's Liberation Army (PLA) for being behind the cyberattack. 'Chinese Military

DOI: 10.19165/2020.6.0129

One further observation: some of the most commonplace threats stem from attacks committed by "insiders."[93] The insider threat has been described by the DHS' National Cybersecurity and Communications Integration Center as "…a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally misused that access to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems."[94] In practice, the insider threat can extend beyond malicious employees to those who were negligent or careless (or who were co-opted in some way) in a manner that allows malicious actors to exploit, or do damage to the ICT systems and data of the company, enterprise or government agency in question. While some of the measures described further above might mitigate aspects of the insider threat, there are also other solutions that can be deployed. These include user-behavior monitoring software, or predictive analytics (incorporating tools such as machine-learning applications) that can identify behaviors that fall outside of accustomed patterns.

Corporations in the private sector as well as governments that take cyber security seriously have one thing in common – they recognize the need to develop multidisciplinary teams examining (and tasked with maintaining) cyber security from all angles – not just the technical. Experts who understand behavioral sciences are needed to complement computer and software engineers.[95] In addition, innovative thinking should be encouraged when it comes to rooting out potential weaknesses. Bug bounty programs (where "ethical" hackers are tasked with finding weaknesses in code and applications) have been useful in both the private and public sector, and governments with a holistic view on these matters have tended to encourage a culture of ethical hacking.[96] Separately, enterprises (as well as government agencies) sometimes employ "red cells" or "red teams" to test the level of cyber security both at the systems and employee level. At a basic level, these teams may (just like CERTS) send out spoof phishing emails to test the levels of employee alertness. But true red teams, typically employed by agencies with a mature security posture, are capable of far more advanced activities if given the remit, and go beyond simple penetration testing. They may be allowed (for example) to try almost any measure to hack into the systems of the enterprise or agency, testing the responses of the in-house CERT.[97]

Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax', United States Department of Justice, 10 February 2020. Available at: https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking

[93] See Tucker Bailey, Brian Kolo, Karthik Rajagopalan, and David Ware, 'Insider threat: The human element of cyberrisk', *McKinsey*, September 2018. Available at: https://www.mckinsey.com/business-functions/risk/our-insights/insider-threat-the-human-element-of-cyberrisk

[94] 'Combating the Insider Threat', National Cybersecurity and Communications Integration Center, 2 May 2014. Available at: https://www.us-cert.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat_0.pdf

[95] Multidisciplinary teams can also be useful for modelling cyber risk scenarios. See 'Cyber risk research impeded by disciplinary barriers' (various authors), *Science*, Vol .366, Issue 6469, pp.1066-1069 (29 November 19).

[96] For an example of its uses in India, see 'Ethical Hacking: The Challenges Facing India', *BBC*, 4 December 2019. Available at: https://www.bbc.com/news/world-asia-india-50583733

[97] Kelly Sheridan, 'Think Like an Attacker: How a Red Team Operates', *Dark Reading*, 20 Sept. 2018. Available at: https://www.darkreading.com/threat-intelligence/think-like-an-attacker-how-a-red-team-operates/d/d-id/1332861

DOI: 10.19165/2020.6.0129

One final comment: the "offensive" side in cyber always seems to be one step ahead of a defense frantically playing catch-up.[98] This is often not on account of technical failures such as deficiency in malware detection, but it is often tied to a lack of awareness of cyber security; indeed, many high-profile hacks have had at their root human weakness. These might span an entire spectrum, ranging from weak (and easily exploited) passwords, failure to secure Wi-Fi connections, the opening of phishing emails that contain malicious code, being lured to an online "watering hole," or thoughtlessly inserting a compromised USB thumb-drive into an open port. It has thus become a commonplace that humans are the weakest link in cybersecurity. Several national cyber centers, including some of those mentioned above, give to the general public also guidance on cybersecurity.)[99] But the cyber threat is not as visible as (say) terrorism, and, unlike kinetic attacks by terrorists, the attack may have been ongoing long before the target is aware. Good cyber hygiene at the personal level is often a key component of national plans for shoring up cyber defenses. While it cannot be said that any country has achieved complete competence of cybersecurity over the government, private sector and people pillars, some have advanced further in the journey than others. The defense efforts of three countries which have gone about this are the US, Estonia, and Singapore. These will be discussed in the following case studies.

[98] An observation made (to give one example) by Katherine Hutton, LTC Ernest Wong, and Ryan Gagnon, 'Thinking Outside-the-Box for Cyber Defense: Introducing an Innovation Framework for the 21st Century', *The Cyber Defence Review*, 18 July 2018. Available at: https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1577721/thinking-outside-the-box-for-cyber-defense-introducing-an-innovation-framework/

[99] The Canadian Centre for Cybersecurity also does similar outreach and provision of guidance to the public on cyber threats and cyber hygiene. '5 Practical Ways to make Yourself Cybersafe'. Available at: https://www.cyber.gc.ca/sites/default/files/publications/five-practical-ways-yourself-ef.pdf

DOI: 10.19165/2020.6.0129

Part III: Case Studies: Estonia, Singapore, and US

Estonia: What Doesn't Kill You…

"The Estonian cyberspace can be defended if the state and society as a whole participate in the defence, the necessary experts have been trained, and society is aware of the dangers of the virtual world and knows how to avoid them and acts correctly if problems occur."

- Estonian National Security Concept, 2017[100]

"For Estonia, cybersecurity does not mean protecting technological solutions; it means protecting digital society and the way of life as a whole."

- Estonian Cybersecurity Strategy, 2019-2022[101]

The internet, and the connectivity it brings, constitute the *sine qua non* to the functioning of the modern Estonian state. It is the backbone of utilities (such as the electrical grid), government communications, and services. Unsurprisingly, 99 percent of public services are dispensed online given the internet penetration was almost 90 percent in 2018.[102] In 2005, Estonia became the first country in the world to hold elections over the internet, partly facilitated through the e-ID, the Estonian national digital identity system, which can be held by every Estonian (regardless of location).[103] As the 2017 Estonian National Security Concept observes, the state would be unable to function without digital services that are integrated into society – but "this increases the impact that potential attacks have on [the Nation's] security. Due to the connectivity between communications and information systems, an interruption in one vital service may influence the availability of many others, thereby endangering the functioning of the state as a whole."[104]

Reaching the current level of awareness and preparedness has been a learning journey, to say the least. In April 2007, Denial-on-Service (DDoS) attacks of severe magnitude severely disrupted online services of government, media, and banking (this at a time when 97 percent of all bank transactions were conducted online, and where 60 percent of the population used the internet daily). Other targets included the Estonian Parliament.[105] The magnitude of the

[100] *Estonian National Security Concept*, 2017, p.17. Available at: http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_2017pdf. The author is very grateful to Eneken Tikk-Ringas for reading this section and making numerous suggestions concerning Estonian cyber preparedness, which improved the draft immeasurably. Remaining errors are the author's own.

[101] *Cybersecurity Strategy 2019-2022*, Republic of Estonia. Available at: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

[102] For the figures, see the initial pages of *E-Estonia Guide*. Available at: https://e-estonia.com/wp-content/uploads/eestonia-guide-2018.pdf

[103] The digital ID system covers every Estonian, but not everyone holds the ID-card or other artefact allowing use of the system. I am grateful to Eneken Tikk-Ringas for enlightenment on this point.

[104] Estonian National Security Concept, 2017, p.5.

[105] For accounts of the attacks, see Eneken Tikk, Kadri Kaska, and Liis Vihul, *International Cyber Incidents : Legal Considerations*, Cooperative Cyber Defence Centre of Excellence (CCDCOE, 2010), pp.15-34. Available at: https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf; Cyrus Farivar, 'Cyberwar I : What the attacks on Estonia have taught us about online combat', *Slate*, 22 May 2007. Available at:

DOI: 10.19165/2020.6.0129

attacks was such that White House cybersecurity advisor Howard Schmidt observed, "Estonia has built their future on having a high-tech government and economy, and they've basically been brought to their knees because of these attacks."[106]

Estonian officials initially pointed the finger at Russia, but subsequently, partly it appears on account of the technical difficulty in pinning down attribution, there was some backtracking.[107] There was, however, compelling evidence of Russian links, with at least some of the hackers identifying as Russian, and with some of the attacks originating from Russian IP addresses.[108]

The attacks were severe enough for the Estonian CERT (which had been set up in 2006) to request for international and NATO assistance.[109] But this does not mean it was caught completely unprepared. Estonia already had a high level of technical cyber expertise, some of which had been used earlier, in 2005, to secure Estonia's online election. This expertise, and the networks that Estonian cyber defenders (who were drawn from both the private and public sectors) had built over the years, proved useful during the 2007 attacks.[110] International contacts were also leveraged on for assistance to block suspicious IP addresses.[111]

Important lessons were learnt and conclusions drawn during the post-mortem, with Estonia since 2007 undergoing a complete transformation in terms of preparedness, mitigation, and response to cyberattacks. This has also encompassed a turn towards securitization of ICTs and digital technologies critical infrastructure. The latter point concerned the technical question of the architecture of ICT systems and building in redundancy. As one informed observer noted

---

https://slate.com/technology/2007/05/what-the-attacks-on-estonia-have-taught-us-about-online-combat.html; Ruus, Kertu, "Cyber War I: Estonia Attacked from Russia," *European Affairs* 9:1 (Winter/Spring 2008): Columbia International Affairs Online. Available at: (https://www.europeaninstitute.org/index.php/42-european-affairs/winterspring-2008/67-cyber-war-i-estonia-attacked-from-russia) and Ian Traynor, 'Russia accused of unleashing cyberwar to disable Estonia', *The Guardian*, 17 May 2007. The initial trigger was the relocation of a statue of a Russian soldier from a prominent place in central Tallinn. The statue represented the Russian state (which had unveiled the statue in 1947) and to the ethnic Russians living in Estonia the Soviet victory over Fascism, but to many Estonians this was seen as a symbol of occupation. The two nights of rioting over the issue (between ethnic Russians and Estonians) on 26 and 27 April 2007 coincided with the beginning of the cyberattacks (on 27 April). The attacks spiked on 9 May (Victory Day, the Russian holiday marking the defeat of Fascism) and 10 May. See Mark Landler and John Markoff, 'Digital Fears Emerge After Data Siege in Estonia', *The New York Times*, 29 May 2007. Available at: https://www.nytimes.com/2007/05/29/technology/29estonia.html; and Damien McGuinness, 'How a Cyber Attack Transformed Estonia', *BBC*, 27 April 2017. Available at: https://www.bbc.com/news/39655415.

[106]Quoted in Stephen Herzog, 'Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses', *Journal of Strategic Security* 4, no. 2 (2011), p.52.

[107] Jose Nazario, 'Politically Motivated Denial of Service Attacks', 2009. Available at: https://ccdcoe.org/uploads/2018/10/12_NAZARIO-Politically-Motivated-DDoS.pdf; Cyrus Farivar, 'Cyberwar I: What the attacks on Estonia have taught us about online combat', *Slate*, 22 May 2007. Available at: https://slate.com/technology/2007/05/what-the-attacks-on-estonia-have-taught-us-about-online-combat.html

[108] For the evidence, see Marco Roscini, 'Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations'; in: Jens David Ohlin, Kevin Govern, and Claire Oakes Finkelstein (Eds.) *Cyberwar: Law and Ethics for Virtual Conflicts*, (Oxford: Oxford University Press, 2015), p. 216. The possibility that hacktivists in Russia sympathetic to the Kremlin also had a hand cannot be completely ruled out: Estonian officials speaking on the condition of anonymity suggested as much. See Damien McGuinness, 'How a Cyber Attack Transformed Estonia', *BBC*, 27 April 17, and also Shaun Waterman, 'Analysis: Who cyber smacked Estonia?',*United Press International*, 11 June 2007. Available at: https://www.upi.com/Defense-News/2007/06/11/Analysis-Who-cyber-smacked-Estonia/26831181580439

[109] Kertu 2008.

[110] Ibid.

[111] Landler, Mark, and John Markoff, 'Digital Fears Emerge After Data Siege in Estonia', *New York Times*, 29 May 2007.

DOI: 10.19165/2020.6.0129

in this connection, "a distributed architecture where there is no single point of failure is way more resilient."[112] So seriously is "distribution" taken that some critical backup servers are now located in a data center in Luxembourg – in theory, if a cyberattack in Estonia wiped out data or if Estonian ICT and servers were to be physically destroyed or taken over through invasion or annexation, "data continuity" would be ensured and the core aspects (included land and business registries, which are among the several databases transferred) could "reboot."[113] Separately, the Estonian government also subsequently decided to locate critical servers and databases in different locations throughout the country – minimizing the risk of total data failure should there be physical destruction of one site. E-health and e-ID records are for example stored in separate data centers.

Organization

Lessons were also learnt organizationally. In 2009, an inter-agency body, the Cyber Security Council, was established within the Security Committee of the government. The Council, chaired by the Secretary General of the Ministry of Economic Affairs and Communications, supports strategic level inter-agency cooperation and oversees the implementation of the Estonian Cybersecurity Strategy (on which more details are provided below). Also in 2009, pursuant to the first National Cyber Security Strategy issued the year before, the Department of Critical Information Infrastructure Protection (CIIP) was added to the structure of Estonian Informatics Centre (EIC), the state agency tasked with cyber security for essential information and communication systems. The intention was to give a strategic layer of oversight (and the ability to give holistic recommendations) to the operational work already done by the Estonian CERT.[114] The EIC was itself in 2011 re-organized into the Estonian Information Systems Authority (EISA), becoming Estonia's central cyber security coordination center under the Ministry of Economic Affairs and Communications. EISA is responsible for the development and administration of state information systems, and drafting cyber policies; it has in addition the overarching responsibility for cyber incidents Estonian networks.[115]

Estonia has also become known as a country capable of articulating its cyber vision in a clear-eyed manner. The first Estonian cybersecurity strategy, issued in 2008, was one of the first of

---

[112] 'Estonia's Cyber Lessons for Singapore', *The Straits Times*, 9 August 2018. Available at: https://www.straitstimes.com/opinion/estonias-cyber-lessons-for-singapore

[113] 'Data security meets diplomacy: Why Estonia is storing its data in Luxembourg', Yuliya Talmazan, *NBC News*, 26 June 2019. Available at: https://www.nbcnews.com/news/world/data-security-meets-diplomacy-why-estonia-storing-its-data-luxembourg-n1018171

[114] 'EIC creates unit for defense of critical information systems'. Available at: https://www.ria.ee/en/news/eic-creates-unit-defense-critical-information-systems.html; see also Christian Czosseck, Rain Ottis and Anna-Maria Talihärm, 'Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organizational Changes in Cyber Security', *International Journal of Cyber Warfare and Terrorism*, pp. 24-34 (2011). For the responsibilities of the Estonian CERT, See Anna-Maria Osula, *National Cyber Security Organization: Estonia, 2015*, p. 8. Available at: https://ccdcoe.org/uploads/2018/10/CS_organisation_ESTONIA_032015_1.pdf

[115] Idem, pp. 7-8. - For a schematic overview on policy evolution and the various evolutions concerning agencies responsible for cyber, see Pernik, Piret, 'National Cyber Security Strategies: The Estonian Approach', 22 June 2017. Available at: https://www.cncs.gov.pt/content/files/estonian_cyber_security_strategy_-_piret_pernik.pdf. Also useful to understand the precise delineation of responsibilities for cyber amongst various agencies is Piret Pernik and Emmet Tuohy, 'Interagency Cooperation on Cyber Security: The Estonian Model', NATO Science & Technology Organization, STO-MP-HFM-236. pp. 9-5 to 9-6. Available at: https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-HFM-236/MP-HFM-236-09.pdf

DOI: 10.19165/2020.6.0129

its kind in the world. The third edition, the Cybersecurity Strategy 2019–2022, expands and amplifies on the earlier strategies. Its fundamental principles:

- Protection and promotion of fundamental rights and freedoms as important in cyberspace as in the physical environment.
- Seeing cybersecurity as an enabler and amplifier of Estonia's rapid digital development, which is the basis for Estonia's socioeconomic growth. Security must support innovation and innovation must support security.
- Recognition of the security assurance of cryptographic solutions to be of unique importance for Estonia as it is the foundation of the Estonian digital ecosystem.
- Transparency and public trust are considered fundamental for digital society.

Therefore, Estonia commits to adhere to the principle of open communication.[116] The strategic objectives of the Strategy include the following:

- A sustainable digital society: Estonia as a sustainable digital society relying on strong technological resilience and emergency preparedness.
- Cybersecurity industry, research and development: Estonian cybersecurity industry as a strong, innovative, research-oriented and globally competitive, covering all key competences for Estonia.
- A leading international contributor: Estonia as a credible and capable partner in the international arena.
- A cyber-literate society: Estonia as a cyber-literate society ensuring sufficient and forward-looking talent supply.[117]

The holistic approach through the emphasis on fundamental principles and strategic objectives is especially noteworthy: what can be seen is not just recognition of the need for cyber protection, but for awareness and cyber literacy and the building up of a capacity and talent pipeline. Cybersecurity is not something that protects systems and CII; it is a fundamental part of the future growth, which is why Estonia seeks to be at the forefront of the field.

People

The active involvement of the Estonian public in cyber defense is notable and has been matched by few other nations. The Ministry of Defense, the overall authority for military aspects of cyber defense, works closely with the Estonian Defense League, a voluntary national defense organization. The League formed a Cyber Unit in 2010 with the aim of protecting Estonian cyberspace and digital society (essentially, the ability of ordinary Estonians to function and interact with each other, as well as with the government, online).[118] Members of the unit, who

[116] *Cybersecurity Strategy 2019-2022*, Republic of Estonia. Available at: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf
For a summary, see: https://www.mkm.ee/sites/default/files/contacts/files/onepager_eng_web.pdf. The previous strategies were issued in 2008 (covering 2008-2013) and 2014 (covering 2014-2017).

[117] *Cybersecurity Strategy 2019-2022*. For a summary, see: https://www.mkm.ee/sites/default/files/contacts/files/onepager_eng_web.pdf. The previous strategies were issued in 2008 (covering 2008-2013) and 2014 (covering 2014-2017).

[118] Available at: http://www.kaitseliit.ee/en/cyber-unit. For still useful overview of the Unit, see Sharon L. Cardash, Frank J. Cilluffo, and Rain Ottis, 'Estonia's Cyber Defense League: A Model for the United States?', Studies *in Conflict and Terrorism*, (Vol.36, Issue 9), 2013, pp. 778-780. This author prefers the use of the official

DOI: 10.19165/2020.6.0129

as League members are volunteers, are either IT professionals or have specific IT skills. They are mobilized when circumstances require (for example, crisis management in the event of an attack on CII, or boosting the capability of in-house CERTS when a specific sector comes under attack). The unit maintains readiness through regular training and exercises, and also has a role when it comes to boosting cyber awareness in the public domain.[119] Those involved in the Cyber Unit have, in addition to the requisite skills, a sense of duty to the country, with work in the Cyber Unit also being a useful avenue for those who for various reasons are unable to serve in the armed forces. Another attraction of the unit is that (given the nucleus of highly skilled professionals) there are good networking opportunities within, and the connections made and skills learnt in turn lead to a diffusion of competence and expertise back into the private sector.[120]

Estonian cyber preparedness now ranks as one of the highest in the world.[121] It has helped other nations further afield build their cyber capacity,[122] and is also a key player in the EU's cyber agenda. But just as important in terms of the wider multinational response that arose from the 2007 attacks is NATO's own analysis and reaction. These are worth highlighting.

Before the attacks, NATO's focus was less on cyber threats and more on countering real-world aggression by Russia.[123] The 2007 attacks (followed by the Russian-Georgian conflict, which took place one year after, also marked by information operations and cyber warfare) were a wake-up call – it forced an internal assessment on NATO's cyber posture. The realization that cyber defense should now be a NATO priority in the wake of the 2007 attacks played a part in the creation of the Tallinn-based, and NATO-accredited, Cooperative Cyber Defense Center of Excellence (CCDCOE) in May 2008.[124] The CCDCOE functions as a multidisciplinary center bringing together cyber experts, researchers, analysts from various sectors (the military, government, academia and industry) from over two dozen nations (and funded voluntarily by them). The focus is on research, development, training and education on all aspects of cyber

name of the Estonian Defense League Cyber Unit, rather than its unofficial moniker "the nerd reserves". See Christa Case Bryant, 'Cybersecurity 2020: What Estonia knows about thwarting Russians', *The Christian Science Monitor*, 4 February 2020. Available at: https://www.csmonitor.com/World/Europe/2020/0204/Cybersecurity-2020-What-Estonia-knows-about-thwarting-Russians

[119] Monica M. Ruiz, 'Is Estonia's Approach to Cyber Defense Feasible in the United States', *War on the Rocks*, 9 Jan 2018. Available at: https://warontherocks.com/2018/01/estonias-approach-cyber-defense-feasible-united-states/

[120] Bruce Sterling, 'Estonian Cyber Security', *WIRED*, 9 January 2018. Available at: https://www.wired.com/beyond-the-beyond/2018/01/estonian-cyber-security/. For a detailed analysis of the Cyber Unit, its mission, membership and objectives, see Kadri Kaska, Anna-Maria Osula, LTC Jan Stinissen, *The Cyber Defense Unit of the Estonian Defense League: Legal, Policy and Organizational Analysis*, Tallinn 2013. Available at: https://ccdcoe.org/uploads/2018/10/CDU_Analysis.pdf

[121] Perez, Roi 'Estonian cyber-security ranks best in Europe, fifth in the world', *SCMagazine.co.uk*, 20 June 2017. Available at: https://www.scmagazineuk.com/estonian-cyber-security-ranks-best-europe-fifth-world/article/1474485

[122] 'Estonia's RIA concludes agreement on enhancement of cyber-security with India' *The Baltic Times*, 22 Augustus 2019. Available at: https://www.baltictimes.com/estonia_s_ria_concludes_agreement_on_enhancement_of_cyber-security_with_india/

[123] Tamkin, Emily, '10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?', *Foreign Policy*, 27 April 2017. Available at;: https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/

[124] The center had already been offered to NATO in 2003, but the events of 2007 hastened the process and gave the CCDCOE a great deal more visibility. (Personal communication, Eneken Tikk-Ringas, February 2020).

DOI: 10.19165/2020.6.0129

defense.[125] Over time, the CCDCOE has drawn in collaborations and partnerships with technology companies from the Nordic world; in addition, countries much further afield have found it useful to either maintain links with CCDCOE or plan to join it as partners.[126]

The beginnings of the fundamental reassessment and reorganization of NATO cyber architecture can be traced to the years immediately following 2007. The year 2008 saw the formation of what was at the time NATO's primary executive body for cyber, the Cyber Defense Management Authority (CDMA). The CDMA, headquartered in Brussels, had as its chief role the direction, coordination and assessment of the various member states' cyber capabilities. This role, since taken over by Cyber Defense Management Board (CDMB), includes coordinating response to any cyberattack against NATO or its member states.[127]

At the operational level, there was also fresh emphasis on the importance of the NATO Communications and Information (NCI) Agency's NATO Computer Incident Response Capability (NCIRC TC), which has originally been set up in the aftermath of the 1999 Kosovo conflict.[128] Following further reorganizations, centralized cyber defense for NATO came under the NATO Communications and Information Agency (NCIA), with the NCIRC becoming part of NCIA.[129] A key part of the NCIRC was the Rapid Reaction Team (RRT), which became operational in 2012. The core of RRT is constituted of a group of experts who can be supported by further NATO professionals if the given case requires it. By the end of 2012, the RRT capability became operational.[130]

In 2014, NATO Member States made cyber defense a core part of collective defense, declaring that a cyberattack could lead to invoking the critical NATO collective defense clause, Article 5 of the NATO Treaty.[131] Moreover, in 2016, NATO members recognized cyberspace as a domain of military operations, (adding it to the conventional domains of air, land and sea), and further pledging to make cyber defense a priority.[132] This was followed in 2018 by the

[125] Available at: https://ccdcoe.org/about-us

[126] O'Dwyer, Gerard, 'Nordic countries deepen collaboration with Estonia-based cyber security operation', *Computer Weekly*, 11 September 2019. Available at: https://www.computerweekly.com/news/252470489/Nordic-countries-deepen-collaboration-with-Estonia-based-cyber-security-operation

[127] For the various evolutions, see Jason Healey and Klara Tothova Jordan, 'NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow', Atlantic Council Brent Scowcroft Center on International Security Issue Brief, September 2014. Available at: https://www.atlanticcouncil.org/wp-content/uploads/2014/08/NATOs_Cyber_Capabilities.pdf

[128] Dunn Cavelty, Maryam, 'Cyber-Allies: Strengths and Weaknesses of NATO's Cyberdefense Posture' IP Global Edition, Vol. 12/3, 2011, pp. 11-158. Available at: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID1997153_code1782288.pdf?abstractid=1997153&mirid=1

[129] See Herzog, Stephen 'Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses', *Journal of Strategic Security* 4, no. 2, 2011, p.55, and also: CDR Wiesław Goździewicz, 'From Riga to Wales. NATO's Road to Collective Cyberdefence' in Joanna Świątkowska (Ed.), *NATO Road to Cybersecurity*, (The Kosciuszko Institute, 2016), p.12. Available at: https://ik.org.pl/wp-content/uploads/nato_road_to_cybersecurity_the_kosciuszko_institute_2016.pdf .

[130] 'NATO Rapid Reaction Team to fight Cyber Attack', 13 March 2012. Available at: https://www.nato.int/cps/en/natolive/news_85161.htm

[131] The actual threshold for triggering Article 5 has not (yet) been clearly spelt out, with this lack of certainty owing (at least partly) to difficulties with attribution, and to determining what exactly constitutes a cyberattack of a magnitude that would make an Article 5 invocation an appropriate response. See 'Nato: Cyber-attack on one nation is an attack on all', *BBC*, 27 August 2019. Available at: (https://www.bbc.com/news/technology-49488614) and Jason Healey and Klara Tothova Jordan, 'NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow', p.7 (and Box 7). It should be borne in mind that Estonia during the 2007 cyberattacks did not consider itself to be under armed attack and refrained from requesting NATO support under Article 5.

[132] Brent, Laura 'NATO's role in Cyberspace', 12 February 2019. Available at:

DOI: 10.19165/2020.6.0129

establishment of the NATO Cyberspace Operations Centre (CyOC), which comes under the NATO military command structure.[133] In the same year, Estonia created its own cyber command, whose mission besides cooperating with NATO allies is, inter alia, to defend the country's information systems, and to conduct "active cyber defense" operations where appropriate.[134]

Given the importance attached to cyber defense by the Estonian government and also given Estonia's geographical location, it is unsurprising that some of the largest NATO cyber defense exercises are held there. An example is the NATO flagship cyber exercise (organized with the cooperation of Estonia's Cyber Command), held in Estonia in 2019 (an earlier edition in 2016 had also been held in Estonia). Amongst the participants, besides cyber experts (including members of the Estonian Defense League cyber unit), were government officials, academic experts and individuals from the private sector.[135]
Another major exercise is Locked Shields, organized by the NATO CCDCOE since 2010. Locked Shields is a real-time exercise that sees red team/blue teams under pressure to defend (or find a way to undermine) the cyber defenses of an unnamed country. New technological challenges are regularly injected into the exercise. The 2019 edition (which involved more than 1,200 experts from nearly 30 nations taking part) saw as the key scenario a fictional country under hostile attack, with the attacks including a cyber-component, severely disrupting (inter alia) power generation and distribution, 4G communication systems, maritime surveillance, and other critical infrastructure components. Blue teams were tasked with maintaining operations while at the same time understanding the higher strategic level calculations.[136]

Estonia has also been an early, and innovative mover in public-private partnerships for cybersecurity and artificial intelligence (AI), with official support being given to startups in these fields. Initiatives include inviting start-ups to join its defense artificial intelligence and cybersecurity accelerator, the first of its kind in Europe. One accelerator, CyberNorth, was launched in 2019 by the business-to-business accelerator Startup Wise Guys, in collaboration with the Estonian Defence Industry Association, and supported by the Ministry of Defense. Participants benefit from intensive mentorship by industry, cybersecurity and defense sector mentors, as well as benefiting from seed money (and the possibility of further investment if successful).[137]

---

https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html

[133] "The CyOC serves as NATO's theatre component for cyberspace and is responsible for providing cyberspace situational awareness, centralized planning for the cyberspace aspects of Alliance operations and missions, and coordination for cyberspace operational concerns". Available at: https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html.
For analysis, see Sydney J.Freedberg Jr., 'NATO To 'Integrate' Offensive Cyber By Members', *Breaking Defence*, 16 November 2018. Available at: https://breakingdefense.com/2018/11/nato-will-integrate-offensive-cyber-by-member-states/

[134] *Estonian Cyber Command: What is it For?* 26 November 2018. Available at: https://icds.ee/estonian-cyber-command-what-is-it-for/

[135] Available at: https://shape.nato.int/news-archive/2019/exercise-cyber-coalition-2019-concludes-in-estonia; 'Estonia's Cyber Command helps to organize NATO's Cyber Coalition exercise', *The Baltic Times*, 6 December 2019. Available at: https://www.baltictimes.com/estonia_s_cyber_command_helps_to_organize_nato_s_cyber_coalition_exercise/

[136] Cf. Available at: https://ccdcoe.org/exercises/locked-shields/

[137] 'Start-ups invited to beef up Estonian cyber security', *Emerging Europe*, 19 November 2018. Available at: https://emerging-europe.com/news/start-ups-invited-to-beef-up-estonian-cyber-security/; Jaroslaw Adamowski, 'Estonia supports start-up accelerator to develop defence AI, cyber-security solutions', *SC Magazine UK*, 3 December 2018. Available at: https://www.scmagazineuk.com/estonia-supports-start-up-accelerator-develop-defence-ai-cyber-security-solutions/article/1520109

DOI: 10.19165/2020.6.0129

Efforts are also being made to impart good cyber hygiene, and teach cyber skills, at an early stage. The Ministry of Defense (together with private sector and educational institutions) supports a program known as CyberOlympics, which aims to identify (and train) future cyber talent, and to educate the wider public (especially the young) about cybersecurity and opportunities in the cybersecurity field. One aspect is a cyber-defense competition, which sees the winners having the opportunity to represent Estonia at higher level (including international) competitions.[138] Another aspect, CyberNuts, aimed at younger students, sees students test themselves in a survey on digital safety and cyber security, which was organized as part of the CyberOlympics project. The 2018 edition involved over 9,000 student participants.[139]

Beneath the seemingly rosy picture of the state of Estonian cyber preparedness, it is worth noting that the 2019-2022 cyber strategy lists significant challenges, including some related to problems with strategic leadership, lack of ICT specialists, and insufficient volume of R&D.[140] Some observers have also pointed to the fact that Estonia's digital infrastructure suffers from a lack of investment.[141]

The need to stay up to date has been thrown into relief through incidents in recent years involving the Estonian e-ID card. The discovery of vulnerabilities in the cards has in some cases necessitated software updates (or the revocation of security certificates). Although these do not appear to have been exploited by malicious actors, the discovery of these vulnerabilities (with the attendant potential for ID theft) does raise the issue of the security of access to -government services.[142]

Having become a model for the world, Estonia sees its cyber preparedness closely observed by other nations seeking to prepare themselves for a new generation of threats. The likelihood of its continued position as exemplar depends not just on the strides other nations make, but also on the degree to which Estonia builds on progress made since 2007 and addresses its own existing areas in need of improvement.

---

[138] Cf. Available at: http://itacademy.ee/en/cyberolympics-2017-european-cyber-security-challenge-2017-estonian-preliminary-round ; https://sites.google.com/view/kyberolympia/eng/about-the-project; http://studyitin.ee/students-to-battle-it-out-during-estonian-cyberolympics

[139] Cf. Available at: https://www.internet.ee/eif/news/cybernuts-crushed-by-over-9-500-students-across-estonia. - Separately, there have also been pilot programs ongoing to develop courses in basic cybersecurity that have been conducted in schools. See Kalev Aasmae, 'Cybersecurity for kids: 'The earlier we teach this, the better specialists we'll have', *ZDnet*, 24 February 2016. Available at: https://www.zdnet.com/article/cyber-security-for-kids-the-earlier-we-teach-this-the-better-specialists-well-have/

[140] *Cybersecurity Strategy 2019-2022*, pp. 26-28.

[141] Tomas Jermalavičius, 'Small State Power in the Digital Era: Insights from the Estonian Experience'. Available at: https://www.americanacademy.de/small-state-power-in-the-digital-era/;
see also "Estonia's e-service maintenance underfunded, needs extra €60 million yearly," *ERR News / BNS, 13* April 2018. Available at: https://news.err.ee/747826/estonia-s-e-service-maintenance-underfunded-needs-extra-60-million-yearly

[142] 'ID-kaardi kiibis peitub teoreetiline turvarisk' ('There is a theoretical security risk in the ID card chip'), *ERR.ee. Available at*: https://www.err.ee/616719/id-kaardi-kiibis-peitub-teoreetiline-turvarisk
4 September 2017; Hans Lõugas, 'Riik palub: ID-kaarti saab küll uuendada, aga ärge tehke seda' ('The state asks: ID cards can be updated, but don't do it'), *Digigeenius*, 26 October 2017. Available at: https://digi.geenius.ee/rubriik/uudis/riik-palub-id-kaarti-saab-kull-uuendada-aga-arge-tehke-seda/; 'Uuendamata jäi 300 000 turvariskiga ID-kaarti', ('300,000 ID cards with security risks were not renewed'), *Pealinn*, 2 April 2018. Available at: http://www.pealinn.ee/tagid/koik/uuendamata-jai-300-000-turvariskiga-id-kaarti-n218022

DOI: 10.19165/2020.6.0129

Singapore's SMART Nation: "Baking" in Security

"Cyber security is a key enabler for Smart Nation. We can't be a Smart Nation that is trusted and resilient if our systems are open and vulnerable."

- David Koh, Chief Executive, Cyber Security Agency, 9 June 2016.[143]

"We have to bake [data] security into the design [of the SMART Nation]."

- Dr Vivian Balakrishnan, Minister in charge of the SMART Nation initiative, 27 November 2019.[144]

The Smart Nation: Opportunity and Risk

Singapore is firmly on the path to becoming a SMART Nation – a vision launched by its Prime Minister, Lee Hsien Loong in 2014.[145] This is, in the words of the government agency tasked with implementing the vision,

> "…an ongoing digital revolution, and advancements in digital technologies are transforming the way we live, work and play. We envision a Smart Nation that is a leading economy powered by digital innovation, and a world-class city with a Government that gives our citizens the best home possible and responds to their different and changing needs.
>
> At the broadest level, the economy is the biggest domain driving Singapore's growth and competitiveness. It is supported by the Government, which is leaning forward to catalyse growth and innovation across all domains, including the public sector. Crucially, these efforts are underpinned by efforts to ensure that all segments of society are able to harness digital technologies and benefit from them."[146]

The nascent vision brings with it seemingly immense possibilities in terms of economic development, societal advancement, and interconnectedness (through, for example, the Internet of Things (IoT). But the vision also brings with it a vastly expanded threat surface. The SMART City generates a large amount of data which is of interest to criminal syndicates, as

[143] 'Internet Policy Part of Cyber Defence', *The Business Times*, 10 June 2016. Available at: https://www.asiaone.com/singapore/internet-policy-part-cyber-defence-ida-csa

[144] *Public Sector Data Review Committee Report*, November 2019. Available at: https://www-smartnation-sg-admin.cwp.sg/docs/default-source/press-release-materials/psdsrc-main-report.pdf
For a snapshot of the findings and recommendation, see https://www.smartnation.sg/whats-new/press-releases/completion-of-public-sector-data-security-review--to-secure-and-protect-citizens-data, and also 'Government accepts 5 measures to improve data security, to set up single contact for public to report breaches', *TODAY*, 27 November 2019. Available at: https://www.channelnewsasia.com/news/singapore/government-improve-data-security-contact-public-report-breaches-12130700

[145] For the various milestones in Singapore's SMART Nation journey, see 'SMART Nation Progress'. Available at: https://www.smartnation.sg/why-Smart-Nation/smart-nation-progress

[146] Cf. 'Transforming Singapore'. Available at: https://www.smartnation.sg/why-Smart-Nation

DOI: 10.19165/2020.6.0129

well as states keen to learn more about the underlying resilience and vulnerabilities of the nation.[147]

A second issue is awareness at the people level. Here, it is worth making a comparison with Estonia. Both countries are technologically advanced and relatively small, and both have suffered serious cyberattacks in the past. But while Estonia has a large neighbor that might attempt to undermine it from time to time, including through the use of cyber means (particularly at times when the bilateral relationship is especially fraught), Singapore has no such adversaries – at least none located at its doorstep. Singapore has, by almost all measures, been shielded for decades from major security incidents of the type that others, including near neighbors, have seen – not least terrorist attacks. This can partly be put down to an exceptionally competent security apparatus that works largely out of the limelight. But the sheer fact of Singapore's "normalcy," somewhat counterintuitively, weighs against efforts to protect the people and systems from cyber threats. The latter type of threats, unlike kinetic terror threats (which are visible), cannot easily be measured (since there is often no visible damage, nor are there direct fatalities). The seemingly invisible nature of the threat therefore has bred a degree of complacency and poor security consciousness.[148] A major nationwide cybersecurity survey conducted by the Cyber Security Agency (CSA) in 2019 found seven out of ten respondents exhibiting high levels of concerns when it came to have their computers hacked, having personal information stolen, or falling victim to an online scam. But less than half of respondents felt like they themselves would fall victim to a cyberattack.[149]

Compounding complacency is the lack of awareness of the dangers that the much-heralded future brings. The reality of the SMART nation means innumerable IOT nodes at the individual, household or precinct level. These might include smart devices at home, personal SMART wearables, or smart CCTV systems – all might have interlinkages, and all can in theory be compromised, especially in a climate where individuals do not routinely change default passwords, and routinely log onto unsecured Wi-Fi networks.[150]

Another concern is the security of Singapore's Critical Information Infrastructure (CII). Singapore has eleven designated CII, which encompass sectors that are responsible for delivery of critical services. These are: government, InfoComm, energy, aviation, maritime, land transport, healthcare, banking and finance, water, security and emergency, and media. CII protection is a core part of Singapore's Cybersecurity Strategy, launched in October 2016.[151]

---

[147] For some considerations, see: Yu-Min Joo and Teck-Boon Tan, 'Smart Cities: A New Age of Digital Insecurity', *Survival*, 60:2, 2018, pp. 91-106; also Morta Vitunskaite, Ying He, Thomas Brandstetter and Helge Janicke, 'Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership', *Computers and Security*, 83, 2019, pp. 313–331.

[148] Of 2,035 respondents polled in the Cyber Security Agency's 2018 edition of its public awareness survey, approximately 34% had stored their passwords in their computers or wrote them down, or used the same password for work and personal accounts.
'The Big Read: As more cyberattacks loom, Singapore has a weak 'first line of defence'', *TODAY*, 23 Feb 2019. Available at: https://www.todayonline.com/big-read/big-read-more-cyber-attacks-loom-singapore-weak-first-line-defence

[149] 'While aware of cyber-security threats, many here still not adopting defensive practices: Survey', *The Straits Times*, 11 September 2019. Available at: https://www.straitstimes.com/tech/while-aware-of-cyber-security-threats-many-here-still-not-adopting-defensive-practices-survey

[150] For some reflections, see Benjamin Ang and Shashi Jayakumar, 'Smart Nation, but will we be Secure?', *The Straits Times*, 14 August 2016. Available at: https://www.straitstimes.com/opinion/smart-nation-but-will-we-be-secure

[151] The Strategy has one of its key tenets, strengthening the resilience CII. The others tenets are: (a) mobilizing businesses and the community to make cyberspace safer by countering cyber threats, combating cybercrime and

DOI: 10.19165/2020.6.0129

One concern, falling into the category of "Digital Pearl Harbour" scenarios, has to do with the ICS and SCADA systems that play a critical role in Singapore's utilities. The provision of some of these utilities and resources could almost be considered an existential issue - a large part of Singapore's water supply is imported from neighboring Malaysia. Although there has to date been no major ICA/SCADA attack against Singapore's utilities (not of the type that has caused massive disruption or physical damage), there has been a significant attack against one CII (healthcare – discussed below).[152] It unsurprising that CSA has in recent years organized large multi-sector cyber preparedness and crisis management exercises involving all CII operators.[153] Separately, a masterplan developed by CSA and industry partners, the Ops-Tech Masterplan, which has a core focus safeguarding CII through public-private partnerships, has also been unveiled in 2019.[154]

Awareness and Talent

Singapore has decided to make cyber security a national priority. Partly in recognition of cyber threats, and also of the threats posed by hybrid activity and disinformation, a new "digital defense" pillar was added to Singapore's Total Defense framework on 15 February 2019, the first addition of a new pillar (the others being military, civil, economic, psychological defense) since the introduction of the Total Defense concept in 1984.[155]

Beyond the symbolic, concrete moves aimed at raising ground awareness and instilling cyber hygiene from a young age have gathered pace in recent years. CSA regularly runs campaigns targeting ordinary citizens, aimed at getting them to understand the basics (such as strong passwords, how to recognize phishing emails). CSA's Cybersecurity Awareness Campaign began in 2017 and, into its third edition in 2019, involves roadshows for the general public, including in educational institutions. There is the recognition, like in Estonia, that the youth are a demographic segment that should be particularly drawn in early into the cybersecurity ecosystem. Besides working cooperation with the Ministry of Education to introduce cyber

protecting personal data; (b) developing a vibrant cybersecurity ecosystem comprising a skilled workforce, technologically-advanced companies and strong research collaborations, so that it can support Singapore's cybersecurity needs and be a source of new economic growth, and (c) stepping up efforts to forge strong international partnerships, given that cyber threats do not respect sovereign boundaries. Cf. Available at: https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy; for the full strategy see: https://www.csa.gov.sg/news/publications/~/media/0ecd8f671af2447890ec046409a62bc7.ashx).

[152] 2016 saw the first attack of any note against CII (in this case, telecommunications) - broadband outages caused by customers' own virus-infected machines that carried out DDoS attacks on the network of a key broadband provider. - 'Star hub: Cyber-attacks that caused broadband outages were from customers' own infected machines', *The Straits Times*, 26 October 2016. Available at: https://www.straitstimes.com/tech/starhub-cyber-attacks-that-caused-broadband-outages-came-from-customers-infected-machines . It is possible that the ultimate source of the attack could have been malware-infected devices (such as web cams or routers) that customers had purchased themselves.

[153] The 2017 edition of these drills, Exercise *Cyber Star* held in 2017, was the first such exercise to bring together all agencies responsible for the eleven CII. '11 critical information infrastructure sectors tested for the first time in national cybersecurity exercise', *ChannelNewsAsia*, 18 July 2017. Available at: https://www.channelnewsasia.com/news/singapore/11-critical-information-infrastructure-sectors-tested-for-first-9040914

[154] 'New cybersecurity masterplan to protect Singapore's critical systems', *ChannelNewsAsia*, 1 Oct. 2019. Available at: https://www.channelnewsasia.com/news/singapore/new-cybersecurity-measures-introduced-singapore-teo-chee-hean-11958326 .

For the masterplan, see *Singapore's Operational Technology Cybersecurity Masterplan 2019*. Available at: https://www.csa.gov.sg/news/publications/~/media/a9ba90ae668f4828af2a6bff60253a51.ashx

[155] 'Digital defense key to success of S'pore's Smart Nation drive: Iswaran', *TODAY*, 15 February 2019. Available at: https://www.todayonline.com/singapore/digital-defence-key-success-spores-smart-nation-drive-iswaran

DOI: 10.19165/2020.6.0129

wellness programme in schools,[156] CSA runs Singapore Cyber Youth Programme (SG Cyber Youth), which has multiple sub-initiatives within it. An example is the Youth Cyber Exploration Programme (YCEP) boot camp, which saw in 2019 all five polytechnics in Singapore hosting 400 students from over 30 secondary schools. The top students from these boot camps took part in the inaugural YCEP Central Capture-the-flag (CTF) Competition. CSA also plans to reach out to thousands of youths in the coming years through boot camps, competitions, learning journeys and career mentoring sessions.[157]

Bug bounty programs have also been used with increasing regularity by government agencies. A major such program is run by GovTech, which has the lead role in implementing Smart Nation vision and leading the government's own digital transformation. These programs thus far appear to have proved reasonably effective in unearthing vulnerabilities; added plusses include demonstrating a culture of openness and willingness on the part of officialdom to engage with the ethical hacking community, in addition to spotting talent that can potentially contribute to national cyber defense down the line in more tangible ways.[158]

Government/Government-linked Systems

Singapore consistently ranks highly in various regional and international surveys of cyber preparedness and readiness.[159] But these have not prevented Singapore, its government agencies, and other institutions within the country from being the victim of cyberattacks, with David Koh, Chief Executive of the Cyber Security Agency of Singapore, observing "Singapore is under constant attack on the cyber front. We are a prime target for cyber criminals, gangs, hacktivists and even state actors."[160]

Some of the best-known cyberattacks have targeted government agencies. The IT system of the Ministry of Foreign Affairs (MFA) was breached in 2014.[161] In another cyberattack in 2017 against a Ministry of Defense system providing system internet to personnel working in Singapore Armed Forces (SAF) premises, hackers stole national identity card numbers, telephone numbers and birth dates of approximately 850 personnel.[162] Other noteworthy

[156] See for example https://ictconnection.moe.edu.sg/cyber-wellness/cyber-wellness-101

[157] Available at: https://www.cyberyouth.sg/ and https://www.csa.gov.sg/programmes/sgcyberyouth

[158] '26 vulnerabilities detected from 2nd Singapore Govt bug bounty programme', *ChannelNewsAsia*, 4 March 2019. Available at: https://www.channelnewsasia.com/news/singapore/26-vulnerabilities-detected-from-2nd-singapore-govt-bug-bounty-11308946; ''Hackers' to test 12 systems in third Government Bug Bounty Programme', *The Straits Times*, 12 November 2019. Available at: https://www.straitstimes.com/tech/hackers-to-test-12-systems-in-third-government-bug-bounty-programme

[159] Singapore ranked for example at the top of the UN International Telecommunications Union (ITU) Global Cybersecurity Index (GCI) in 2017, and 6th in the 2018 edition. Global Cybersecurity Index 2017, p.17. Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf; Global Cybersecurity Index 2018, p. 62. Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

[160] 'Internet Policy Part of Cyber Defence', *The Business Times*, 10 June 2016. Available at: https://www.asiaone.com/singapore/internet-policy-part-cyber-defence-ida-csa

[161] 'MFA's IT system was breached last year, reveals Yaacob', *TODAY*, 11 May 2015. Available at: https://www.todayonline.com/singapore/immediate-steps-precautionary-measures-taken-against-govt-system-breaches-csa

[162] 'Hacking of Mindef system a 'covert' attack', *The Straits Times*, 4 April 2017. Available at: https://www.straitstimes.com/singapore/hacking-of-mindef-system-a-covert-attack. In 2019, in another attack involving the Ministry of Defense, systems of two vendors working with the ministry were compromised. The data potentially compromised included names, addresses and national identity card numbers of approximately 100,000 military personnel. 'Personal data of 2,400 Mindef, SAF staff may have been leaked', *The Straits Times*, 22 December 2019. Available at:

DOI: 10.19165/2020.6.0129

cyberattacks that did not directly target government ministries, but targeted data linked to government. In April 2017, in the first sophisticated cyberattack against Singapore universities, hackers infiltrated the networks of the National University of Singapore (NUS) and the Nanyang Technological University (NTU) in what appeared to have been an attempt to steal sensitive government and research data.[163]

Internet separation was implemented on government networks in 2017, affecting approximately 143,000 civil servants.[164] It was recognized, even at the time of implementation, that the measure was not a fool proof solution to protect government servers. But the aim was to afford some mitigation - to prevent malware finding its way into classified government systems, and to prevent classified emails from finding their way to unsecured computers and personal devices.[165]

The SingHealth/IHiS Breach

Internet separation has something of a bearing on Singapore's worst cyberattack in its history, which took place between June and July 2018, targeting Singapore's health records system. The agency targeted, Integrated Health Information Systems (IHiS), was the central IT agency responsible for Singapore's healthcare sector. IHiS was not a government ministry, but the data compromised (1.5 million SingHealth patients and the outpatient prescription records of 160,000 others, with the health data of Singapore's Prime Minister repeatedly targeted) came under SingHealth, Singapore's largest cluster of public healthcare institutions. The attacker was well-resourced and persistent, with the authorities suggesting that an unnamed state actor lay behind the APT responsible for the breach.[166] Malicious activity finally came to a complete

https://www.straitstimes.com/singapore/personal-data-of-2400-mindef-saf-staff-may-have-been-leaked

[163] 'Cyber-attacks on NUS, NTU in bid to steal sensitive data', *The Straits Times*, 13 May 2017. Available at: https://www.straitstimes.com/tech/cyber-attacks-on-nus-ntu-in-bid-to-steal-sensitive-data. It appears that an attack discovered in October 2017 against the National University of Singapore, which saw computers of at least two employees at NUS targeted, including a researcher involved in a security project funded by the Ministry of Defense, was distinct from the April attacks. 'NUS discovered global phishing attack to steal its academic research and data in October', *The Straits Times*, 31 October 2017. Available at: https://www.straitstimes.com/singapore/education/nus-targeted-in-global-phishing-attack-to-steal-academic-research

[164] 'Singapore to cut off public servants from the internet', *The Guardian*, 24 Augustus 2016. Available at: https://www.theguardian.com/technology/2016/aug/24/singapore-to-cut-off-public-servants-from-the-internet, and 'Some government agencies delink Net access ahead of deadline', *The Straits Times*, 15 March 2017. Available at: https://www.straitstimes.com/singapore/some-govt-agencies-delink-net-access-ahead-of-deadline. Government employees still have access to the internet through other computers, (or through personal devices) but these are air gapped from the government intranet.

[165] It is worth noting that email log-in information (and passwords) of employees of several government agencies featured within a tranche of data found on the Dark Web from 2017-2019. It appears that the leaks did not come directly from government systems, but from public servants' use of official government email addresses for non-official purposes. Also featuring in the tranche were details of over 19,000 compromised bank payment cards. 'E-mail log in details of govt staff put up for sale on Dark Web', *The Straits Times*, 22 March 2019. Available at: https://www.straitstimes.com/tech/e-mail-log-in-details-of-govt-staff-put-up-for-sale-on-dark-web

[166] 'Style of SingHealth cyber-attack, info targeted point to state-backed hackers, say experts', *The Straits Times*, 22 July 2018. Available at: https://www.straitstimes.com/singapore/style-of-attack-info-targeted-point-to-state-backed-hackers-say-experts. A cyber threat monitoring company, Symantec, subsequently laid the finger of blame on a APT actor, Whitefly, which is " is a highly adept group with a large arsenal of tools at its disposal, capable of penetrating targeted organizations and maintaining a long-term presence on their networks. 'Whitefly: Espionage Group has Singapore in Its Sights', Symantec, 6 March 2019. Available at: https://www.symantec.com/blogs/threat-intelligence/whitefly-espionage-singapore

DOI: 10.19165/2020.6.0129

halt after internet surfing separation was implemented on SingHealth systems on 20 July 2018.[167]

The high-level Committee of Inquiry (COI) examining the causes of the breach as well as the response to it found lapses in procedures and especially human weaknesses[168] While some individuals in the incident response team had attempted in the midst of the attack to remediate matters, there were also basic failures (on the part of a key incident response manager) when it came to recognizing the severity of the attack, and (somewhat startlingly) recognizing what in the first place constituted a security incident. These human failures, besides leading to delays in the ongoing attack being reported up the chain of command and to authorities such as CSA, also meant that opportunities to mitigate the effect of the cyberattack were missed.[169]

The inquiry made 16 main recommendations to improve processes and prevent a recurrence. One category of priority recommendations concerned improving competencies and staff awareness (including more effective incident response), as well as levels of cyber hygiene. The recommendations also included ensuring privileged administrator accounts would be subject to greater monitoring, and the use of two-factor authentication when engaged in administrative tasks. On the "technical" side, recommendations included real-time monitoring of databases, implementing a robust patch management to address security vulnerabilities, and putting into place controls to better protect against data theft.[170]

Beyond policy-related and technical aspects of the recommendations, more important was the overall philosophy the COI took, as these had implications for cyber preparedness in all other large organizations that might have data others covet. The COI in its report suggested the near-inevitability of sophisticated attackers being able to breach any network. Organizations therefore had to adopt an "assume breach" mindset and "defence in depth" strategy. This

---

[167] *Public Report of the Committee of Inquiry into the Cyber Attack on Singapore Health Services Private Limited's Patient Database on or around 27 June 2018* (10 Jan . 2019), p. 54, p.71 and p. 195. Available at: https://www.mci.gov.sg/-/media/mcicorp/doc/report-of-the-coi-into-the-cyber-attack-on-singhealth-10-jan-2019.ashx. In the wake of the IHiS/SingHealth attack, senior officials noted that internet separation should have been implemented at an earlier point in the public healthcare system (just as it had been done in the public sector). 'Internet separation 'could and should have' been implemented in public healthcare system: DPM Teo', *ChannelNewsAsia*, 24 July 2018. Available at: https://www.channelnewsasia.com/news/singapore/internet-separation-should-have-been-implemented-teo-chee-hean-10558584

[168] The inquiry reached no definitive finding as to how the malicious actor first gained entry into the IHiS system. But on the balance of possibilities, a spear phishing attempt that successfully infected a SingHealth front-ended workstation with malware seems to have been the most likely explanation. *Public Report of the Committee of Inquiry into the Cyber Attack on Singapore Health Services Private Limited's Patient Database on or around 27 June 2018* (10 January 2019), p.54. Despite the title of the report, the earliest signs of a system compromise in fact dated back to 23 August 2017, with the cyberattack spanning the period 23 August 2017 to 20 July 2018 (Idem, p.51).

[169] 'SingHealth cyberattack: IHiS sacks 2 employees, imposes financial penalty on CEO', *ChannelNewsAsia*, 14 January 2019. Available at: https://www.channelnewsasia.com/news/singapore/singhealth-cyberattack-ihis-fires-employees-ceo-fined-11120838. For a brief analysis of the cyberattack and some recommendations, see Shashi Jayakumar, 'SingHealth cyber-attack: Can parties involved learn from COI findings?', *TODAY*, 7 February 2009. Available at: https://www.todayonline.com/commentary/singhealth-cyber-attack-can-parties-involved-learn-coi-findings?fbclid=IwAR2RmyyUnM-X8JbbuYo2Cgl8lKM8SYO1i5zwnX7Uuh4N3gJpnpL5VWoxqNc

[170] What has been given above is a sampling of the recommendations. See 'COI on SingHealth cyber- attack: 16 recommendations', *The Straits Times*, 10 January 2019. Available at: https://www.straitstimes.com/singapore/16-recommendations; also *Public Report of the Committee of Inquiry into the Cyber Attack on Singapore Health Services Private Limited's Patient Database on or around 27 June 2018*, pp.221-425.

DOI: 10.19165/2020.6.0129

involves inter alia*:* arming themselves with sophisticated security systems and solutions which can facilitate early detection of malware, and by adopting emerging technologies, such as database activity monitoring endpoint detection and advanced behavior-based analytics.[171]

Breaches like the IHiS/SingHealth incident have the potential to affect public confidence in the government as custodian of public data.[172] As a result, the government in March 2019 convened a high-level Public Sector Data Security Review Committee, chaired by the minister in charge of Public Sector Data Governance. The five main recommendations of the Committee (which reviewed data management practices across all 94 public agencies to identify risk areas) will be mentioned here as they have a bearing on cyber preparedness:

- Improving data protection and preventing data compromise through measures like protecting data directly when stored to ensure it is unusable even if extracted.
- Improving detection and response to data incidents through measures like designating the Government Data Office to monitor and analyze data incidents that pose significant harm.
- Raising competencies and instilling a culture of excellence through measures such as training all public officers to attend improved data security training every year.
- Accounting for data protection at every level through measures like amending Singapore's Personal Data Protection Act to cover third-party vendors handling Government data.
- Ensuring a continuous approach to improving data security through measures like improving the Government's expertise in data security technology.

Lapses found by the committee (members of which were present in the majority of agencies reviewed) included failings in management of privileged user accounts, user access reviews, and encryption of emails with sensitive data.[173] These findings came on top of earlier government audit findings made public which had similarly pointed to weaknesses in government agencies' IT controls.[174]

---

[171] *Public Report of the Committee of Inquiry into the Cyber Attack on Singapore Health Services Private Limited's Patient Database on or around 27 June 2018*, p. 225. A great many of the "technical" recommendations from the COI were not new and were reminiscent of recommendations put forward in other contexts and locations. See for example the US CERT's 2019 recommendations for IT solutions providers and their customers. Recommendations (which find echoes in the SingHealth COI report) include applying the principle of least privilege to their environment, integrating log files and network monitoring data from IT service provider infrastructure and systems into customer intrusion detection and security monitoring systems for independent correlation, aggregation and detection, and working with customers to ensure hosted infrastructure is monitored and maintained, either by the service provider or the client. *Chinese Malicious Cyber Activity*. Available at: https://www.us-cert.gov/china

[172] For other incidents involving health data in Singapore, see 'HIV-positive status of 14,200 people leaked online', *ChannelNewsAsia*, 28 January 2019 (involving a deliberate leak online of the identities and identifiers of HIV-positive individuals by an individual linked to an "insider"), and 'Personal information of more than 800,000 blood donors exposed online by tech vendor: HAS', *ChannelNewsAsia*, 15 March 2019 (the leak of the personal information of approximately 800,000 blood donors in Singapore in January 2019 after mishandling by a vendor). Available at: https://www.channelnewsasia.com/news/singapore/hiv-positive-records-leaked-online-singapore-mikhy-brochez-11175718 and https://www.channelnewsasia.com/news/singapore/blood-donors-information-exposed-online-hsa-11349308

[173] 'Government accepts 5 measures to improve data security, to set up single contact for public to report breaches', *ChannelNewsAsia*, 27 November 2019. Available at: https://www.channelnewsasia.com/news/singapore/government-improve-data-security-contact-public-report-breaches-12130700

[174] The Auditor-General's Office in its 2019 annual report flagged several lapses in IT controls in government agencies, including weak controls and monitoring over privileged user accounts. *Report of the Auditor-General*

DOI: 10.19165/2020.6.0129

A concerted push to accelerate remediation could be discerned from late 2019 onwards, with the Smart Nation and Digital Government Group (SNDGG – which consists of the Smart Nation Office under the Prime Minister's Office and GovTech), working with public agencies to effect deep changes at the "technical, process and people levels to address the systemic causes" behind findings of vulnerabilities by earlier committees. Announced in early January 2020 were several measures to reduce vulnerability at the IT, systems, and people level. These pertained to areas of concern that had been flagged repeatedly by previous committees, such as the introduction of automated tools across government agencies that would enable review of the activity logs of privileged user accounts and flag any unexpected behavior, with a new system planned that would perform targeted checks using audit and incident data. Finally, in the works is a comprehensive revision of the government instruction manual dealing with IT security, with the new standards to be benchmarked against leading industry practices.[175]
These initiatives to protect government systems and data require adequate funding. February 2020 saw the announcement during the course of the annual Parliamentary budget debate of $1 billion over the next three years to build up the Government's cyber and data security capabilities. The funds will be used to safeguard citizens; data and critical information infrastructure systems, with the Deputy Prime Minister and Finance Minister Heng Swee Keat emphasizing in the course of his announcement how data security is a vital prerequisite and key enabler of Singapore's digital economy.[176]

The Private Sector

One of the SingHealth/IHiS COI recommendations was that partnerships be formed between government and industry to achieve a higher level of collective security.[177] There have been some positive developments. A case in point is the launch of a joint venture center of excellence (a partnership between an entity partly-owned by a government investment arm and IronNet, founded by former NSA Director Gen (retd.) Keith Alexander) to protect critical infrastructure against sophisticated cyberattacks.[178]

However, at the level of ordinary business, significant issues exist. Some of these have to do with factors cited further above which are common to companies around the world: key personnel at the management or C-suite level might still view cybersecurity as purely a IT issue (not a business risk), with investments in cybersecurity seen as a cost item on the balance

for the Financial Year 2018/19 (Republic of Singapore: Auditor-General's Office, July 2019), pp.4-6, pp.27-30, and pp. 32-33. Available at:
https://www.ago.gov.sg/docs/default-source/report/103c3319-e3df-4300-8ce0-e0b831e0c898.pdf

[175] 'Measures aimed at reducing ministries' IT lapses to be rolled out', *The Straits Times*, 17 January 2020. Available at: https://www.straitstimes.com/singapore/measures-aimed-at-reducing-ministries-it-lapses-to-be-rolled-out?xtor=CS3-18&utm_source=STiPhone&utm_medium=share&utm_term=2020-01-17%2019%3A01%3A38

[176] 'Budget 2020: S$1b to be spent on enhancing Government's cyber, data security capabilities', *ChannelNewsAsia*, 18 February 2020. Available at:
https://www.channelnewsasia.com/news/singapore/budget-2020-fund-enhancing-government-cybersecurity-12446336. Specifics programmes and initiatives leveraging on these funds have at the time of writing yet to be announced.

[177] *Public Report of the Committee of Inquiry into the Cyber Attack on Singapore Health Services Private Limited's Patient Database on or around 27 June 2018*, pp. 331-339.

[178] 'Temasek's Ensign, US partner launch centre for cyber defence of critical infrastructure', *The Straits Times*, 18 March 2019. Available at: https://www.straitstimes.com/business/companies-markets/temaseks-ensign-us-partner-launch-centre-for-cyber-defence-of-critical

DOI: 10.19165/2020.6.0129

sheet.[179] While major multinationals and institutions such as banks may have the resources and the perspective to recognize the need not just for investments in cybersecurity but also for the right mindset, a lack of knowledge and resources is preventing local small and medium enterprises (SMEs) from adopting robust cybersecurity measures." Many attacks that target SMEs come either from pre-identified risks or from insider threats.[180] CSA and other agencies such as the Infocomm and Media Development Authority (IMDA) have worked on this issue. On offer are tailored cybersecurity solutions and a one-stop portal to access grants to acquire and deploy these solutions.[181]

Observers of Singapore's SMART Nation drive will have been given considerable food for thought by events of recent years. Despite many positives, it is clear that all major constituents - government, private sector, and citizens and residents – still have areas for improvement. The private sector needs (especially below the level of MNCs and other well-resourced entities) to take cybersecurity more seriously and to see it as a continuing enterprise risk. The government needs to heed lessons of various lapses and breaches; lest the overall levels of public confidence reposed in the state to keep Singapore safe start to dip (of which there has been no sign yet). The people, for their part, can only progress to a certain level of maturity if the key drivers of awareness and education remain the slew of well-intended initiatives from relevant government agencies. If the people themselves are not seized with these issues, there may be further amplification of the sentiment, evinced already by some observers, that the weakest link in Singapore's cybersecurity efforts may well be the people.[182]

All this will in turn have a bearing on Singapore's future. It will certainly, given time, become a truly SMART Nation. But will it become a *secure* SMART Nation?

[179] The Singapore Board of Directors 2017 survey showed that while cybersecurity is a concern for 9 out of 10 boards in Singapore, it is still not part of strategic discussions at the board level. 'Cyber security critical concern of Singapore companies but not ranked high in board focus: Survey', *The Straits Times*, 7 November 2017. Available at: https://www.straitstimes.com/business/companies-markets/cyber-security-critical-concern-of-singapore-companies-but-not-ranked

[180] 'Report flags lack of cyber preparedness among SMEs in Singapore', *The Straits Times*, 17 October 2019. Available at: https://www.straitstimes.com/business/companies-markets/report-flags-lack-of-cyber-preparedness-among-smes-in-singapore

[181] Opening Remarks by Dr Janil Puthucheary, Senior Minister of State (SMS), Ministry of Communications and Information and SMS-in-Charge of Cybersecurity at the Launch of the Cyber Security Call for Innovation 2019, 2 October 2019. Available at: https://www.csa.gov.sg/news/speeches/cybersecurity-call-for-innovation-2019

[182] 'The Big Read in Short: Singapore's weakest link in cyber security', *TODAY*, 23 February 2019. Available at: https://www.todayonline.com/big-read/big-read-short-singapores-weakest-link-cyber-security

DOI: 10.19165/2020.6.0129

United States of America

The US was a pioneer in national approaches to securing cyberspace, with the national security and intelligence communities aware since the 1990s that various state and non-state actors could seek to undermine or cause outright damage to the country through cyber means.[183] This has been a continuing – and developing – threat perception. The 2019 Worldwide Threat Assessment given by Director of National Intelligence (DNI), Dan Coats, before the Senate Select Committee on Intelligence ranked cyber as the number one threat, above terrorism.[184] Every DNI Worldwide Threat Assessment (which represents the consolidated view of US intelligence agencies) from 2013 onwards had presented cyber threats above terrorism in its hierarchy of threats to the US Securing cyber national space poses enormous challenges to the many agencies concerned. The enormous attack surface includes the government at the federal and state levels, as well as the private sector, together with CII (mostly under the control of the private sector). Some of this is relatively well-defended, but in many cases, resources, manpower and expertise are lacking. Compounding the issue are interagency rivalries, and differing perspectives and threat perceptions between private sector and the federal government.

The sense of heightened vulnerability in the years immediately following the 9/11 attacks included something of a fixation with the possibility Islamist terrorists might acquire cyber capabilities.[185] This proved to be temporary, with Richard Clarke, the first White House Adviser for Cybersecurity, stating in 2002 that "there are terrorist groups that are interested in conducting cyberattacks. We now know that Al-Qaeda was interested. But the real major threat is from the information-warfare brigade or squadron of five or six countries."[186]

Some of the major US initiatives after 9/11 are worth remarking on here.

- The Office of Homeland Security (which was later in 2002 to become the Department of Homeland Security (DHS)) was given overall authority for the protection of critical infrastructure against threats (but not, as we shall see, made the overarching body responsible for cyber issues). In 2003, the National Cyber Security Division was created within the DHS, with the first US CERT coming under this division.[187]
- The establishing by Executive Order of the President's Critical Infrastructure Protection Board (CIPB) and the appointment of Richard Clarke, from the National Security Council, and former national coordinator for security, infrastructure protection and counterterrorism, as the first White House Special Adviser for Cyber Security and chair of the CIPB.[188]

[183] For a discussion of how US discourse on cyber from the national security perspective has evolved over the years, see Dunn Cavelty, Myriam, 'Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate', *Journal of Information Technology & Politics*, 2008, 4:1, pp. 19-36, pp. 24-30.

[184] Coats, Daniel, *Worldwide Threat Assessment of the US Intelligence Committee* (Statement for the Record before the Senate Select Committee on Intelligence), 29 January 2019. Available at: https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

[185] See Weimann, Gabriel 'Cyberterrorism: The Sum of All Fears?', *Studies in Conflict & Terrorism*, 28 (2), pp. 131-134.

[186] Ariana Eunjung Cha and Jonathan Krim, 'White House Officials Debating Rules for Cyberwarfare', *Washington Post*, 22 August 2002.

[187] The US CERT was also initially set up in partnership with Carnegie Mellon University. Available at: https://www.cmu.edu/cmnews/extra/030915_cyberpartner.html

[188] Dunn Cavelty, Myriam 'Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate', p. 26.

DOI: 10.19165/2020.6.0129

- The CIPB published under Clarke's leadership the National Strategy to Secure Cyberspace in February 2003. This, the first such official strategy, was a foundational document, identifying eight major planks for effective cyber preparedness and response:
    1. Establishing a public-private architecture for responding to national-level cyber incidents;
    2. Providing for the development of tactical and strategic analysis of cyberattacks and vulnerability assessments;
    3. Encouraging the development of a private sector capability to share a synoptic view of the health of cyberspace;
    4. Expanding the Cyber Warning and Information Network to support the role of DHS in coordinating crisis management for cyberspace security;
    5. Improving national incident management;
    6. Coordinating processes for voluntary participation in the development of national public-private continuity and contingency plans;
    7. Exercising cybersecurity continuity plans for federal systems; and
    8. Improving and enhancing public-private information sharing involving cyberattacks, threats, and vulnerabilities.[189]

Early exercises and penetration testing in the late 1990s and early 2000s did not give ground for a great deal of optimism when it came to the state of overall US preparedness. A well-known example is the 1997 exercise, code-named "Eligible Receiver" conducted by the National Security Agency (NSA). NSA hackers acting as a "red team" posing as North Korean hackers, penetrated various national security systems, including Pentagon computer systems (and in several cases, doing so with some ease, using brute force hacking, social engineering, and also through using off the shelf hacking tools that were relatively easily obtainable).[190] The results were alarming to the national security establishment, to say the least. The impression that the government was ill-prepared to defend itself against burgeoning cyber-threats was reinforced by several further exercises and studies in the years immediately following. Two cases in point: a 2003 study by the House Government Reform Subcommittee on Technology, which examined (and graded) cyber security in various federal agencies, awarded more than half the federal agencies surveyed a low or failing grade (D or F), including the DHS.[191] In 2006, Exercise Cyber Storm (itself overseen by the DHS), designed to test reactions of government agencies and the private sector to cyberattacks against key CII, found that participants across both government and the private sector had difficulty responding effectively to attacks (and indeed, in some cases, recognizing the attacks in the first place).[192]

The Obama Era

Particularly since the beginning of the Obama era, there was a move to enhance the sense of cybersecurity responsibility within the private sector, with, as one commentator observes, the White House "focused on helping the private sector protect itself, instead rather than trying to

[189] Cf. Available at: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf
[190] Weimann 2005, p. 138.
[191] Ibid., p. 140.
[192] 'DHS Releases Report on Cyber Storm Exercise'. *Security Focus*, 14 September 2006. Available at: https://www.securityfocus.com/brief/303; Myriam Dunn Cavelty, 'Cyber-Terror—Looming Threat or Phantom Menace?', p. 27.

DOI: 10.19165/2020.6.0129

make cybersecurity a government responsibility."[193] This was understandable: private industry owns and operates about 85 percent to 95 percent of the US critical infrastructures, and, in theory at least, has the resources and expertise for ensuring the security of these assets. The posture taken by relevant government agencies was to provide support in appropriate areas (for example, in law enforcement aspects and investigations, and, where appropriate, information sharing).[194]

The difficulty is that many companies prefer not to have an overly-close relationship with government agencies when it comes to cybersecurity. The better-resourced companies may have in-house CERTs, while others may prefer to use specialist providers (which may be able to respond more quickly than the government). Many private sector companies, once they have recovered from a breach, may be reluctant to work closely with government agencies when it comes to post-breach forensics, as (from their point of view) this might be exposing themselves to added scrutiny. Other weaknesses and vulnerabilities might be exposed, with government agencies possibly demanding additional mitigating measures for these while not seeming to have that much to offer in return.

Finally, the private sector is not necessarily hardwired to see the national security implications of a major breach. A case in point is the November 2014 hacking of Sony Pictures by a group calling itself the "Guardians of Peace." The attack was believed to be taken in response to *The Interview*, a middling Hollywood movie depicting the assassination of North Korean leader Kim Jong-un. Besides rendering many workstations inoperable, large amounts of data and emails were stolen, with some released to the public in a way that caused severe embarrassment to Sony.[195]

Weaknesses within Sony were partly to blame for the hack. Cybersecurity practices were extremely careless at best, and at worst, institutionally negligent. There was awareness at the management level of Sony's parent company of various failings, with internal IT assessments before the cyberattack showing that basic security protocols were ignored. The internal network had hundreds of unmonitored devices; in addition, passwords for Sony Pictures' internal computers were stored without even basic protection.[196]

The FBI moved quickly, attributing the hack to North Korea within weeks.[197] But it appears that outside of government, and particularly within the entertainment industry, many were skeptical on the attribution. In these circles, there also appeared to be an unwillingness to accept

[193] Knake, Rob, 'Obama's Cyberdoctrine: Digital Security and the Private Sector', *Foreign Affairs*, 6 May 2016. Available at:
https://www.foreignaffairs.com/articles/united-states/2016-05-06/obamas-cyberdoctrine
[194] Ibid.
[195] The story of the Sony hack and its ramifications has been told well by several knowledgeable commentators. See for example Richard Stengel, ''The Untold Story of the Sony Hack: How North Korea's Battle with Seth Rogen and George Clooney Foreshadowed Russian Election Meddling in 2016', *Vanity Fair*, 6 October 2019. Available at: https://www.vanityfair.com/news/2019/10/the-untold-story-of-the-sony-hack
[196] Feinberg, Ashley, 'Sony Execs Knew About Extensive IT Flaws Two Months Before Leaks', *Gizmodo*, 12 December 2014. Available at: https://gizmodo.com/sony-execs-knew-about-extensive-it-flaws-two-months-bef-1670203774
[197] Ellen Nakashima, 'U.S. Attributes cyberattack on Sony to North Korea', *Washington Post*, 19 December 2014. Available at: https://www.washingtonpost.com/world/national-security/us-attributes-sony-attack-to-north-korea/2014/12/19/fc3aec60-8790-11e4-a702-fa31ff4ae98e_story.html

DOI: 10.19165/2020.6.0129

the potential seriousness of the incident.[198] The Sony hack convinced influential figures within the administration that the US had to impose penalties for cyber misbehavior.[199]

The Sony hack was something of a turning point: senior figures within government realized that the private sector when faced by a cyber-threat of serious magnitude would not be able to deal with the threat on its own; nor would it be able to appreciate the wider implications of a state-linked attack. Both the public and private sectors have to be prepared to cooperate when it comes to incident response.[200] National Security Agency Director Michael Rogers called the attack a game-changer, and "a national-security issue that crosses almost every spectrum of our society." Emphasizing that government and private sector had to find ways work together to deter and respond to cyberattacks, Rogers also observed that there had to be clarity when it came to giving the private sector a sense of what they could expect from the authorities, and what they had to do, in the event of a major breach.[201]

Despite these initiatives, the legacy of the Obama presidency when it comes to the overall shoring up of the nation's cyber defenses was rather mixed. To be sure, there was a substantial amount of intellectual heavy lifting, as evidenced by the 2009 Cyberspace Policy Review, which aimed at producing a "coordinated cybersecurity plan" intended to, amongst other points, build capacity and pave the way to create effective information sharing mechanisms in the event of cyberattacks. The resulting cybersecurity strategy also meant, theoretically, something of centralization of cybersecurity efforts that saw an overarching cybersecurity coordinator appointed within the White House.[202]

There were other achievements. In 2013, the National Institute of Standards and Technology was directed by executive order to work with the private sector to develop the Cybersecurity Framework, a common set of (voluntary) cybersecurity best practices. This was finalized in December 2014.[203] The following year, President Obama signed the Cyber Information Sharing Act (CISA) designed to improve the sharing of threat information between federal government and the private sector.

CISA was a step in the right direction, but it did not represent a comprehensive (nor binding) instrument to get the private sector to work with the government. Notwithstanding the administration having a vision in terms of where the government and private sector had to go

---

[198] Marks, Joseph, 'The Cybersecurity 202: The Sony hack ushered in a dangerous era in cyberspace', *The Washington Post*, 27 November 2019. Available at: https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/11/27/the-cybersecurity-202-the-sony-hack-ushered-in-a-dangerous-era-in-cyberspace/5ddd716c602ff1181f264147/

[199] Ibid.

[200] Statement of Admiral Michael S. Rogers, Commander United States Cyber Command before the Senate Committee on Armed Services, 19 March 2015. Available at: https://fas.org/irp/congress/2015_hr/031915rogers.pdf

[201] Strohm, Chris, 'Sony hack prompts review of government help in private company security', *Seattle Times*, 11 January 2015. Available at: https://www.seattletimes.com/business/sony-hack-prompts-review-of-government-help-in-private-company-security/

[202] Cf. Available at: https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative; 'Text: Obama's remarks on Cyber-security', *New York Times*, 29 May 2009. Available at: https://www.nytimes.com/2009/05/29/us/politics/29obama.text.html; see also 'FACT SHEET: Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure', 29 May 2009. Available at: https://fas.org/irp/news/2009/05/cyber-fs.html

[203] Cf. Available at: https://www.nist.gov/cyberframework; Knake, Rob 'Obama's Cyber doctrine: Digital Security and the Private Sector'.

DOI: 10.19165/2020.6.0129

in improving cyber security, observers were by the end of the Obama presidency questioning how much all the measures enacted had actually improved the nation's overall state of cyber readiness. Criticisms included the government's use of outdated technology, as well as the failure to keep pace with the evolving nature of cyber threats.[204]

Inter/Intra-Agency Dynamics

On top of these criticisms was the issue of interagency turf squabbles. Which agency actually took overall responsibility for cybersecurity? CISA technically meant that DHS had become the node through which the private sector could share threat information (rather than companies going directly to agencies such as the FBI or NSA).[205] CISA built also on the National Cybersecurity Protection Act of 2014, which had officially authorized and codified the role of the DHS' cybersecurity information sharing hub, the National Cybersecurity and Communications Integration Center (NCCIC). The NCCIC would provide a platform for the government and private sector to share information about cybersecurity threats, incident response, and technical assistance. But CISA did not explicitly make DHS the lead cyber agency; other well-resourced agencies such as the NSA and the Pentagon all had major stakes and chafed at the notion that they should be subordinate to the DHS on cyber matters. They also did not believe that DHS could adequately protect the nation from cyber-threats.[206]

More clarity was, relatively speaking, reached in 2018 with the passing of the Cybersecurity and Infrastructure Security Agency Act (CISA; not to be confused with the Cyber Information Sharing Act above).[207] CISA was created out of the former National Protection and Programs Directorate (NPPD) within DHS. Its core responsibilities included protecting the nation's critical infrastructure from physical and cyber threats, safeguarding government systems, providing cybersecurity governance, and working to build the national capacity to defend against and cyberattacks.[208]

---

[204] A senior DHS official with responsibility for cybersecurity observed in 2015 that Einstein 3, the federal threat detection system introduced that year, "is really where we needed to be 15 years ago'. Armerding, Taylor, 'Obama's cybersecurity legacy: Good intentions, good efforts, limited results', *CSO*, 31 January 2017. Available at:https://www.csoonline.com/article/3162844/obamas-cybersecurity-legacy-good-intentions-good-efforts-limited-results.html. For other useful reviews of what the Obama administration did (and did not) do when it came to cybersecurity, see Joseph Marks, 'Obama's Cyber Legacy: He Did (Almost) Everything Right and It Still Turned Out Wrong', *NextGov*, 17 January 2017. Available at: https://www.nextgov.com/cybersecurity/2017/01/obamas-cyber-legacy-he-did-almost-everything-right-and-it-still-turned-out-wrong/134612/ , and Lauren Carroll, 'Obama makes progress on three-pronged cyber strategy', *PolitiFact*, 12 December 2016. Available at: https://www.politifact.com/truth-o-meter/promises/obameter/promise/203/develop-a-comprehensive-cyber-security-and-respons/

[205] See Rozenweig, Paul, 'The Cybersecurity Act of 2015', *Lawfare*, 16 December 2015. Available at: https://www.lawfareblog.com/cybersecurity-act-2015

[206] On the DHS' travails and interagency squabbles in the cyber arena, see Breanne Deppisch, 'DHS Was Finally Getting Serious About Cybersecurity. Then Came Trump.' *Politico*, 18 December 2019. Available at: https://www.politico.com/news/magazine/2019/12/18/america-cybersecurity-homeland-security-trump-nielsen-070149

[207] Available at: https://www.dhs.gov/news/2018/11/13/congress-passes-legislation-standing-cybersecurity-agency-dhs

[208] Engagement with CISA is voluntary, and some have argued that the collaboration between government and the private sector, and the ability to get the private sector to take up CISA's services designed to prevent and mitigate cyberattacks has been stymied by this lack of regulatory power. See Sam Bieler and Randy Milch,

DOI: 10.19165/2020.6.0129

Two other DHS-related developments that show its growing maturity are worth remarking on here. The first concerns the 2017 revamp of CISA's National Cybersecurity and Communications Integration Center (NCCIC), which is the DHS's node for cyber that sees to it that operational elements are coordinated and integrated. NCCIC provides daily operational cyber awareness, analysis, incident response and cyber defense capabilities to both the US federal government and to local authorities (as well as the private sector). The reorganization saw functions previously performed independently by the US Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) integrated into the NCCIC.[209] The second development was the release in 2017 of the DHS' National Cyber Incident Response Plan (NCIRP), an important doctrinal document that the delineates various lines of effort and clarified roles and responsibilities (for of the Federal Government, the private sector, and SLTT (State, Local, Tribal, and Territorial) government) in the aftermath of cyber incidents, showing also how the DHS would manage the effects of significant cyber incidents.[210]

CISA collaborates regularly with partners when it comes to instilling a culture of cyber preparedness nationwide. The Federal Emergency Management Agency (FEMA) facilitates its National Level Exercise (NLE) every two years, with the 2020 NLE event focusing on cybersecurity. NLE 2020, which draws participants from government as well as the private sector, will integrate CISA's cyber exercise CyberStorm (which is itself biennial).[211] In addition to the NLE, FEMA (again in partnership with CISA) regularly runs smaller table top exercises and roundtables, bringing together participants from federal, state and local agencies (and also including representatives from academia and the private sector) to test and run through response plans to cyber threats.[212]

Another key player in the interagency mix is the Department of Defense (DoD) Cyber Command (USCYBERCOM). Achieving fully operational status in 2010, USCYBERCOM Command was in 2017 elevated to the status of a Unified Combatant Command focusing on the planning and execution of cyberspace operations against adversaries of the US (another key role is ensuring the security of DoD networks). USCYBERCOM has in recent years refined the way it measures success. It now seeks to enable other government agencies, as well

'Cybersecurity in One Voice: Leveraging CISA Programming to Improve FTC Cybersecurity Enforcement', *Lawfare*, 5 December 2019. Available at: https://www.lawfareblog.com/cybersecurity-one-voice-leveraging-cisa-programming-improve-ftc-cybersecurity-enforcement

[209] Available at: https://www.us-cert.gov/nccic

[210] *National Cyber Incident Response Plan*, (Department of Homeland Security, December 2016). Available at: https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf.
The NCIRP was a follow up to the 2016 Obama administration Presidential Policy Directive 41 (PPD-41): *United States Cyber Incident Coordination*, which called for such a plan that would define a nationwide approach to cyber incidents and outlines the roles of both federal and non-federal entities. See 'National Cyber Incident Response Plan Now Available For Public Comment', 30 September 2016. Available at: https://www.dhs.gov/blog/2016/09/30/national-cyber-incident-response-plan-now-available-public-comment

[211] Daniel Kaniewski, *Building a culture of Cyber Preparedness.* Available at: https://www.fema.gov/blog/2019-10-28/building-culture-cyber-preparedness

[212] *Cyber Security Workshop Brings Together State, Federal and Private Sector Partners*, 26 June 2019. Available at:https://www.fema.gov/news-release/2019/06/26/cyber-security-workshop-brings-together-state-federal-and-private-sector

DOI: 10.19165/2020.6.0129

as industry, to defend against cyber threats.[213] In doing so, USCYBERCOM collaborates (and shares information with) with partners such as CISA and the FBI. [214]

Threats and Threat Actors

The vulnerability of critical infrastructure to cyberattacks has been recognized for a quarter of a century. July 1996 saw the formation of the President's Commission on Critical Infrastructure Protection (PCCIP) to study vulnerabilities of critical infrastructures and propose protection strategies.[215] In its final (and influential) report, issued in October 1997, the commission noted that the interdependences of various critical infrastructures were real and that, through mutual dependence and interconnectedness, attacks on vulnerabilities "could have severe consequences for our economy, security, and way of life."[216]

The rise of ISIS revived the question whether this jihadist organization could surpass Al-Qaeda and achieve a level of sophistication and capability to carry out destructive cyberattacks against American CII. In May 2015, FBI Director James Comey observed that ISIL was "waking up" to the idea of using sophisticated malware to cyberattack critical infrastructure in the US. But, although senior officials were at around this time observing that ISIS *seemed* to be attempting to target critical infrastructure, there was very little by way of hard evidence, and none concerning major attacks. While ISIL appears to have the intent, attempted attacks do not seem to have risen further than DDOS, defacement, and other, relatively minor, breaches.[217]

The real threat remains the same: state actors which have the technological capability and intent, with means to cause damage of a serious magnitude growing in parallel with the increasing sophistication and interdependence of CII. In 2012, General Keith Alexander, National Security Agency director and commander of the US Cyber Command, stated that cyberattacks against US information networks started as exploitative before becoming

[213] For example, USCYBERCOM is working with the energy sector and the Department of Energy as a way to bolster their relationship in case of a serious cyberattack. Mark Pomerleau, 'Cyber Command wants to work more closely with the energy sector', *Fifth Domain*, 16 October 2019. Available at: https://www.fifthdomain.com/show-reporter/ausa/2019/10/16/cyber-command-wants-to-work-more-closely-with-the-energy-sector/

[214] Statement of Admiral Michael S. Rogers, Commander United States Cyber Command before the Senate Committee on Armed Services, 27 February 2018. Available at: https://www.armed-services.senate.gov/imo/media/doc/Rogers_02-27-18.pdf; see also Shannon Vavra, 'U.S. Cyber Command has shifted its definition of success', *Cyberscoop*, 24 April 2019. Available at: https://www.cyberscoop.com/cyber-command-success-tim-haugh/

[215] The critical infrastructure identified: telecommunications, banking and finance, electrical power, oil and gas distribution and storage, water supply, transportation, emergency services, and government services.

[216] See Denning, Dorothy E., 'Activism, Hacktivism and Cybertorrism: The Internet as a Tool for Influencing Foreign Policy'; in: John Arquilla and David Ronfeldt, *Networks and Netwars The Future of Terror, Crime, and Militancy* (RAND, 2001), p. 285. Available at: https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf, and also: *Critical Foundations: Protecting America's Infrastructures*: The Report of the President's Commission on Critical Infrastructure Protection (October 1997). Available at: https://fas.org/sgp/library/pccip.pdf. For more on the PCCIP and the evolution at that time of the cyber security architecture, see Ralf Bendrath, The Cyberwar Debate: Perception and Politics in U.S. Critical Infrastructural Protection', *Information & Security*, Vol. 7, 2001. *The Internet and the Changing Face of International Relations and Security* (ed. by Andreas Wenger), pp. 80-103.

[217] Catherine Theohary, Kathleen McInnis, and John Rollins, "Information Warfare: DOD's Response to the Islamic State Hacking Activities," *CRS Insight*, Congressional Research Service, 10 May 2016.

DOI: 10.19165/2020.6.0129

disruptive, but now such attacks are moving into the realm of destructive.[218] Gen. Alexander's successor in both these positions, Admiral Mike Rogers suggested in 2014 that:

> "… the threat of a catastrophic and damaging cyberattack in the United States critical infrastructure like our power or financial networks is actually becoming less hypothetical every day…. Foreign cyberactors are probing Americans' critical infrastructure networks and in some cases have gained access to those control systems. Trojan horse malware that has been attributed to Russia has been detected on industrial control software for a wider range of American critical infrastructure systems throughout the country. This malware can be used to shut down vital infrastructure like oil and gas pipelines, power transmission grids and water distribution and filtration systems."[219]

Elsewhere, Admiral Rogers also pinpointed the key state actors – Russia and China – which posed the most serious cyber threats to the US, stating that they "count as peer or near-peer competitors in cyberspace."[220] It is, for example, Russia that has carried out reconnaissance against the US energy grid. DHS threat warnings to critical infrastructure operators have precisely highlighted this threat, providing details on how cyber actors linked to the Russian state targeted networks where they staged malware, conducted spear phishing, and gained remote access into energy sector networks. After obtaining access, the Russian government's cyber actors conducted network reconnaissance and collected information pertaining to Industrial Control Systems (ICS). Besides the energy sector, other targets have included nuclear, aviation, critical manufacturing and the water sector.[221]

Iran and North Korea were the other threat attacks singled out by Admiral Rogers. Despite having fewer technical tools, Rogers noted that they "employ aggressive methods to carry out malicious cyberspace activities," with Iran recruiting hackers for cyberespionage and cyberattacks, including attempts to penetrate US military systems.[222]

Iran appears to have ratcheted up attempts at cyberattacks against US targets following the assassination in January 2020 of Qassem Soleimani, the head of the Iranian Revolutionary Guard Corps' Quds Force.[223] Yet, attempted cyberattacks by Iran or its proxies have in fact

---

[218] John T. Bennett, 'NSA General on Cyberattacks: 'Probability for a Crisis Is Mounting,'' *U.S. News and World Report*, 9 July 2012.

[219] 'Cybersecurity Threats: The Way Forward'; Admiral Michael S. Rogers, commander, United States Cyber Command and director of the National Security Agency, before the House (Select) Intelligence Committee on 20 November 2014. Available at: https://www.nsa.gov/news-features/speeches-testimonies/Article/1620360/hearing-of-the-house-select-intelligence-committee-subject-cybersecurity-threat/

[220] Statement of Admiral Michael S. Rogers, Commander United States Cyber Command before the Senate Committee on Armed Services, 27 February 2018. Available at: https://www.armed-services.senate.gov/imo/media/doc/Rogers_02-27-18.pdf

[221] U.S. Cybersecurity and Infrastructure Security Agency Alert TA18-074A - *Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors*, 15 March 2018.Available at: https://www.us-cert.gov/ncas/alerts/TA18-074A.See also Rob Knake, 'The Next Cyber Battleground: Defending the U.S. Power Grid from Russian Hackers', *Foreign Affairs*, 19 July 2018. Available at: https://www.foreignaffairs.com/articles/north-america/2018-07-19/next-cyber-battleground

[222] Statement of Admiral Michael S. Rogers, Commander United States Cyber Command and director of the National Security Agency, before the Senate Committee on Armed Services, 27 February 2018. Available at: https://www.armed-services.senate.gov/imo/media/doc/Rogers_02-27-18.pdf

[223] For an assessment of the likelihood of Iranian retaliatory cyberattacks following Soleimani's assassination, as well as an excellent survey of recent cyberattacks by Iran or its proxies against the United States, see Annie Fixler, 'The Cyber Threat from Iran after the Death of Soleimani', *CTC Sentinel*, February 2020, Vol.13, Issue 2. Available at: https://ctc.usma.edu/app/uploads/2020/02/CTC-SENTINEL-022020.pdf

DOI: 10.19165/2020.6.0129

already been ongoing for some time – and not simply against military targets. Between 2011 and 2013, Iranian hackers (linked by the US to the Islamic Revolutionary Guard) carried out a series of attacks on the largest US financial institutions including J.P. Morgan Chase, Wells Fargo, Bank of America, and Citigroup.[224] These hackers for the most part employed relatively unsophisticated DDoS attacks in 2013.

It is not just the major players within CII that are vulnerable. Smaller, often regional, players often invest less resources in cybersecurity, assuming that they are somehow below the radar and immune from the threat. But one or more individuals from the Iranian group above attempted to penetrate the SCADA system of the Bowman dam in Rye, New York, in August and September of 2013. Although the dam was small, the access obtained would have permitted the hacker to remotely operate the dam's sluice gate, if it had not been for the fact that the gate had been disconnected for maintenance at that particular time.[225] Another case in point is the attacks in 2019 against small electricity providers (many in proximity to critical infrastructure) in 18 different states. These attacks (which attempted to use phishing techniques to implant malware) do not appear to have succeeded, and may have been more akin to preliminary reconnaissance operations than genuine attempts to cause serious disruption.[226] Separately, in December 2015, a group of hackers managed to infiltrate a water treatment plant (the exact location of which has not been made public) and change the levels of chemicals being used to treat tap water. The breach happened as the water company had been using operating systems which were more than a decade old to run its entire IT network. This server is also connected to the operational technology (OT) systems of the facility. Serious damage appears to have been averted as the hackers did not have detailed knowledge of the ICS/SCADA system.[227]

China's cyberattacks against US targets include espionage (both industrial theft and the theft of military or sensitive government data), with officials not ruling out the possibility that, like Russia, China might be attempting preposition cyberattacks against critical infrastructure. Attacks against utilities have also been attributed to hackers working on behalf of the Chinese state.[228]

---

[224] 'Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector', Department of Justice, 24 Mar 2016. Available at: https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged; Contessa Brewer and Katie Young, 'Cyberattacks are an 'immediate' challenge for businesses following Iran strike', *CNBC*, 7 January 2020. Available at: https://www.cnbc.com/2020/01/07/cyberattacks-are-an-immediate-challenge-for-business-after-iran-strike.html. Iranian hackers (this time apparently working for personal profit) also hacked into American hospitals, universities, government agencies and the city of Atlanta, attempting to extort money from their targets through the use of the SamSam ransomware. Nakashima, Ellen, and Devlin Barrett, 'Justice Department charges Iranians with hacking attacks on U.S. cities, companies', *The Washington Post*, 29 November 2018. Available at: https://www.washingtonpost.com/world/national-security/justice-dept-charges-iranian-hackers-with-attacks-on-us-cities-companies/2018/11/28/cad313d0-f29b-11e8-80d0-f7e1948d55f4_story.html

[225] Joseph Berger, 'A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case', *The New York Times*, 25 March 2016. Available at: https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html

[226] Rebecca Smith and Rob Barry, 'Utilities Targeted in Cyberattacks Identified', *The Wall Street Journal*, 29 November 2019. Available at: https://www.wsj.com/articles/utilities-targeted-in-cyberattacks-identified-11574611200

[227] Russon, Mary-Ann, 'Hackers hijacking water treatment plant controls shows how easily civilians could be poisoned', *International Business Times*, 23 March 2016. Available at : https://www.ibtimes.co.uk/hackers-hijacked-chemical-controls-water-treatment-plant-utility-company-was-using-1988-server-1551266

[228] For a flavor, see Lucas, Ryan, 'Charges Against Chinese Hackers Are Now Common. Why Don't They Deter Cyberattacks?', *NPR*, 5 February 2019. Available at:

DOI: 10.19165/2020.6.0129

Some cyberattacks attributed to China stand out in particular. The 2017 Equifax hack has already been discussed. Besides this, perhaps the best-known of all publicly-reported cyberattacks in the US attributed to China is the US Office of Personnel Management (OPM) hack. In 2013, hackers linked to China breached OPM networks, leading to an unprecedented leak of sensitive data of personnel (with personnel records and security-clearance files of approximately 22.1 million individuals, including federal employees and contractors compromised).[229] What came to light after the breach were revelations of internal neglect, and extremely poor IT security within OPM and its contractors. Earlier reports had flagged significant and "persistent deficiencies in OPM's information system security program," but there was a great deal of lethargy when it came to taking remedial action. Basic failings included the lack of multi-factor authentication for users remotely accessing OPM systems.[230]

The US government's CERT in CISA periodically issues warnings, and advice, on the persistent cyber threat emanating from certain quarters.[231] US CERT has observed that Chinese threat hackers are exploiting relationships between managed IT service providers and their customers. This space is a tempting target given that IT services have access to their customers' networks. Some of the suggestions aimed at protecting against Chinese threat actors are not altogether too different from recommendations issued in other countries. US CERT is encouraging clients to implement a defense-in-depth strategy to protect their infrastructure assets and increase the probability of successfully disrupting APT activity. This is similar to (and pre-dates) the recommendations issued by the Committee of Inquiry in Singapore examining the IHiS breach. Measures recommended by US CERT include:

- Applying the principle of least privilege to their environment, which means customer data sets are separated logically, and access to client networks is not shared.
- Implementing robust network and host-based monitoring solutions that looks for known malicious activity and anomalous behavior on the infrastructure and systems providing client services.
- Ensuring that log information is aggregated and correlated to enable maximum detection capabilities, with a focus on monitoring for account misuse; and

https://www.npr.org/2019/02/05/691403968/charges-against-chinese-hackers-are-now-common-why-dont-they-deter-cyberattacks; Doffman, Zac 'Chinese State Hackers Suspected Of Malicious Cyber Attack On U.S. Utilities', *Forbes*, 3 August 2019. Available at: https://www.forbes.com/sites/zakdoffman/2019/08/03/chinese-state-hackers-suspected-of-malicious-cyber-attack-on-u-s-utilities/#3854c7f56758, and Jim Finkle and Christopher Bing, 'China's hacking against U.S. on the rise: U.S. intelligence official', *Reuters*, 12 December 2018. Available at: https://www.reuters.com/article/us-usa-cyber-china/chinas-hacking-against-u-s-on-the-rise-u-s-intelligence-official-idUSKBN1OA1TB

[229] Nakashima, Ellen, 'Hacks of OPM databases compromised 22.1 million people, federal authorities say', *The Washington Post*, 10 July 2015. Available at: https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/; Michael Adams, 'Why the OPN Hack is Far Worse than you Imagine', *Lawfare*, 11 March 2016. Available at: https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine

[230] Gallagher, Sean, 'Why the "biggest government hack ever" got past the Feds', *ArsTechnica*, 8 June 2015. Available at: https://arstechnica.com/information-technology/2015/06/why-the-biggest-government-hack-ever-got-past-opm-dhs-and-nsa/; David Auerbach, 'The OPM Breach Is a Catastrophe', *Slate*, 16 June 2015. Available at:: https://slate.com/technology/2015/06/opm-hack-its-a-catastrophe-heres-how-the-government-can-stop-the-next-one.html

[231] Cf. Available at: https://www.us-cert.gov/china

DOI: 10.19165/2020.6.0129

- Working with customers to ensure hosted infrastructure is monitored and maintained, either by the service provider or the client. [232]

Talent Acquisition and Future Challenges

Finding the right cyber talent is a pressing issue in every nation, but especially problematic in a nation like the US that spreads cyber responsibilities across a multiplicity of agencies, and where both state and federal levels are competing with the lure of the private sector. In August 2017, the then-White House cybersecurity coordinator Rob Joyce warned that the US lacks 300,000 cyber-security experts needed to defend the country.[233] One comprehensive report in 2018 by Harvard's Kennedy School and Belfer Center has pointed to the "shortage in skilled cybersecurity-minded talent" at the federal level.[234] CISA Director Chris Krebs has himself weighed in, noting that talented cyber professionals would rather choose careers in big tech companies.[235] Efforts are underway to remediate, with the Cybersecurity Talent Management System announced in 2018 allowing the DHS to speed up hiring and offer higher salaries for cyber professionals. At least in theory, this should enable the federal government to compete with the private sector for cyber talent. One other facet of this plan involves the government paying for scholarships for cybersecurity professionals, who, under the plan, will have to spend three to five years in government before moving into the private sector. Originally slated for implementation in 2019, the Talent Management System has at the time of writing (February 2020) not yet been officially implemented.[236]

The American National Guard has in various states begun to develop cyber units. Some have already shown their value in remediating the effects of state-level ransomware attacks.[237] Separately, cyber personnel from the National Guard make up Task Force Echo (which

[232] For the full recommendations see: https://www.us-cert.gov/china and https://www.us-cert.gov/APTs-Targeting-IT-Service-Provider-Customers.

[233] 'W.H. cybersecurity coordinator warns against using Kaspersky Lab software', *CBSNews*, 22 Augustus 2017. Available at: https://www.cbsnews.com/news/kasperksy-lab-software-suspected-ties-russian-intelligence-rob-joyce/

[234] Charlet, Kate *Understanding Federal Cybersecurity* (Harvard Kennedy School/Belfer Center for Science and International Affairs), April 2018, p.41. Available at: https://www.belfercenter.org/sites/default/files/files/publication/Understanding%20Federal%20Cybersecurity%2004-2018_0.pdf. Reasons of space preclude a discussion of the various issues faced at the state level when it comes to cybersecurity. See 'Inside the Government Cybersecurity Landscape: Federal vs. State Level Challenges', *Tripwire*, 1 May 2019. Available at:https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/government-cybersecurity-federal-state/

[235] Corrigan, Jack, 'DHS Cyber Chief is Ready to Update Federal Tech Hiring', *NextGov*, 4 April 2019. Available at: https://www.nextgov.com/cybersecurity/2019/04/dhs-cyber-chief-ready-update-federal-tech-hiring/156086/

[236] Billy Mitchell, 'DHS preps launch of Cyber Talent Management System', *FedScoop*, 22 March 2019. Available at: https://www.fedscoop.com/cyber-talent-management-system-dhs-launch/; Jonathan Scheiber, 'Government will pay for scholarships for cybersecurity professionals who will spend three to five years in government before moving into the private sector', *TechCrunch*, 4 Oct. 2019. Available at: https://techcrunch.com/2019/10/03/lack-cybersecurity-professionals-threat-dhs/

[237] Ikeda, Scott 'The U.S. National Guard's Evolving Mission Includes Assisting Local Governments Experiencing Cyber Attacks', *CSO Magazine*, 18 November 2019. Available at: https://www.cpomagazine.com/cyber-security/u-s-national-guards-evolving-mission-includes-assisting-local-governments-experiencing-cyber-attacks/

DOI: 10.19165/2020.6.0129

currently has a strength of approximately 450 personnel drawn from the Army National Guard), which supports USCYBERCOM's mission.[238]

Task Force Echo, while filling a critical role for USCYBERCOM, has, however, been criticized as "lacking societal engagement and offering no way of integrating private-sector talent."[239] The US has long recognized the need for volunteers to help fill the gaps in its cyber defense efforts. Other, more innovative solutions to fill the talent vacuum have from time to time been floated. Some have suggested that the US needs its own cyber volunteers, akin to the Cyber Unit within the Estonian Defense League.[240] There are in fact already in existence a few examples of looser groupings, akin to cyber militia, coming together in the US in order to provide assistance in the wake of cyber incidents (and particularly in the event when federal assistance might not be immediately forthcoming). The Michigan Cyber Civilian Corps (MiC3) established in 2013, comprises approximately 100 volunteers from government, academia, and business and serves as a rapid response force against cyber incidents within Michigan.[241] Some commentators have suggested that it is imperative that this type of effort be scaled up into a US Cybersecurity Civilian Corps.[242]

Beyond simply protecting networks on a routine basis, it is likely that Task Force Echo and MiC3 will increasingly have roles assisting frontline agencies such as CISA in protecting critical processes such as elections. As has been well-documented, Russian hackers were extremely active in the run-up to the 2016 U.S. presidential election. Besides the manipulation of societal opinion through social-media-enabled subversion (via bots, troll factories), Russian hackers also broke into the Democratic National Committee's email servers. Russian hackers also attempt to seek out vulnerabilities in state election infrastructure. In certain states' voter databases, Russian hackers were in a position to delete or change voter data (although it appears they refrained from doing so).[243]

Interference in the democratic polity and the electoral process are best known from the Russia case study, but others have made attempts of their own too. In late 2019, a hacking group that appears linked to the Iranian government tried to infiltrate email accounts related to Trump's re-election campaign.[244] Suffice to say that the inference in 2016 will not be a one-off. Chris Krebs, Director of CISA (the federal agency with primary responsibility for assisting state and local officials in bolstering election security), observed in February 2020 that he spent "40 to 50 percent of my time on election security issues (…) A top priority for us right now is

[238] Pomerleau, Mark, 'Cyber National Guard Task force will focus on network defense', *Fifth Domain*, 28 February 2020. Available at: https://www.fifthdomain.com/dod/army/2020/02/27/cyber-national-guard-task-force-will-focus-on-network-defense/

[239] Monica M. Ruiz, 'Is Estonia's Approach to Cyber Defense Feasible in the United States?', *War on the Rocks*, 9 January 2018. Available at: https://warontherocks.com/2018/01/estonias-approach-cyber-defense-feasible-united-states/

[240] Ruiz, Monica, M., 'To Bolster Cybersecurity, the US Should Look to Estonia', *WIRED*, 14 February 2020. Available at: https://www.wired.com/story/opinion-to-bolster-cybersecurity-the-us-should-look-to-estonia/

[241] Cf. Available at: https://www.michigan.gov/som/0,4669,7-192-78403_78404_78419---,00.html

[242] Cohen, Natasha, and Peter Warren Singer, *The Need for C3: A Proposal for a United States Cybersecurity Civilian Corps*, New America, October 2019. Available at: https://d1y8sb8igg2f8e.cloudfront.net/documents/The_Need_for_C3_2018-10-22_151313.pdf

[243] Sanger, David E., and Katie Edmondson, 'Russia Targeted Election Systems in All 50 States, Report Finds', *The New York Times*, 25 July 2019. Available at: https://www.nytimes.com/2019/07/25/us/politics/russian-hacking-elections.html

[244] Perlroth, Nicole, and David E.Sanger, 'Iranian Hackers Target Trump Campaign as Threats to 2020 Mount', The New York Times, 4 October 2019. Available at: https://www.nytimes.com/2019/10/04/technology/iranian-campaign-hackers-microsoft.html

DOI: 10.19165/2020.6.0129

protecting 2020."[245] Besides election security, CISA's other operational priorities, outlined in its "strategic intent" plan from 2019, include defending against Chinese threats to 5G networks and reducing the risk of Chinese supply chain compromise.[246]

Protecting against a new generation of cyber and technology-enabled threats will be a critical concern for CISA, USCYBERCOM, and various state and local agencies in the years to come. In this battle against adversaries – many located thousands of miles away - metrics of success are vague and the successes themselves are often hidden under a cloak of operational secrecy. Achieving a better cybersecurity posture will lie not simply in technological prowess, but in strengthening a culture of awareness and responsibility, enhancing interagency cooperation, and in nurturing an ecosystem where cyber talent can flourish and can be directed to where it is needed the most.[247]

Shashi Jayakumar, Ph.D., is Head, Centre of Excellence for National Security (CENS) and Executive Coordinator, Future Issues and Technology at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore. Dr Jayakumar was a member of the Singapore Administrative Service from 2002-2017. During this time, he was posted to various Ministries, including the Ministries of Defense, Manpower, Information and the Arts, and Community Development, Youth and Sports. He was from August 2011-July 2014 a Senior Visiting Research Fellow at the Lee Kuan Yew School of Public Policy. His research interests include extremism, social resilience, cyber, and homeland defense.

[245] 'The 'accidental director' on the front line of the fight for election security', *The Hill*, 25 February 2020. Available at:
https://thehill.com/policy/cybersecurity/484430-the-accidental-director-on-the-front-line-of-the-fight-for-election

[246] *Cybersecurity and Infrastructure Security Authority Strategic Intent: "Defend Today, Secure Tomorrow"*. August 2019, p.8. Available at:
https://www.cisa.gov/sites/default/files/publications/cisa_strategic_intent_s508c.pdf

[247] The author would like to acknowledge the assistance of Beatrice Lee and Benjamin Low in the preparation of this article. All errors and omissions remain the author's own.

DOI: 10.19165/2020.6.0129

Bibliography

Armerding, Taylor, 'Obama's cybersecurity legacy: Good intentions, good efforts, limited results', *CSO*, 31 January 2017. Available at: https://www.csoonline.com/article/3162844/obamas-cybersecurity-legacy-good-intentions-good-efforts-limited-results.html.

Berger, Joseph, 'A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case', *The New York Times*, 25 March 2016. Available at: https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html

Beuth, Patrick, and Kai Biermann, Martin Klingst and Holger Stark, 'Merkel and the Fancy Bear', *Die Zeit*, 12 May 2017. Available at: https://www.zeit.de/digital/2017-05/cyberattack-bundestag-angela-merkel-fancy-bear-hacker-russia/komplettansicht

Cavelty, Myriam Dunn, 'Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate', *Journal of Information Technology & Politics*, (2008), 4:1, pp.19-36.

Czosseck, Christian, Rain Ottis and Anna-Maria Talihärm, 'Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security', International Journal of Cyber Warfare and Terrorism, pp. 24-34 (2011)

'Cyber attacks on NUS, NTU in bid to steal sensitive data', *The Straits Times*, 13 May 2017. Available at: https://www.straitstimes.com/tech/cyber-attacks-on-nus-ntu-in-bid-to-steal-sensitive-data

Cybersecurity and Infrastructure Security Authority Strategic Intent: "Defend Today, Secure Tomorrow". August 2019, p. 8. Available at: https://www.cisa.gov/sites/default/files/publications/cisa_strategic_intent_s508c.pdf

Cybersecurity Strategy 2019-2022, Republic of Estonia. Available at:; URL: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

Farivar, Cyrus, 'Cyberwar I: What the attacks on Estonia have taught us about online combat', *Slate*, 22 May 2007. Available at: https://slate.com/technology/2007/05/what-the-attacks-on-estonia-have-taught-us-about-online-combat.html

'Government accepts 5 measures to improve data security, to set up single contact for public to report breaches', *ChannelNewsAsia*, 27 November 2019. Available at: https://www.channelnewsasia.com/news/singapore/government-improve-data-security-contact-public-report-breaches-12130700

'Hacking of Mindef system a 'covert' attack', *The Straits Times*, 4 April 2017. Available at: https://www.straitstimes.com/singapore/hacking-of-mindef-system-a-covert-attack

Halpern, Sue, 'How Cyberweapons are Changing the Landscape of Modern Warfare', *The New Yorker*, 18 July 2019. Available at: https://www.newyorker.com/tech/annals-of-technology/how-cyber-weapons-are-changing-the-landscape-of-modern-warfare

Knake, Rob, 'Obama's Cyberdoctrine : Digital Security and the Private Sector', *Foreign Affairs*, 6 May 2016. Available at: https://www.foreignaffairs.com/articles/united-states/2016-05-06/obamas-cyberdoctrine

Landler, Mark, and John Markoff, 'Digital Fears Emerge After Data Siege in Estonia', *The New York Times*, 29 May 2007. Available at: https://www.nytimes.com/2007/05/29/technology/29estonia.html

Makridis, Christos Andreas, and Max Smeets, 'Determinants of cyber readiness', *Journal of Cyber Policy* 2019, 4:1, pp.72-89

DOI: 10.19165/2020.6.0129

Matania, Eviatar, Lior Yoffe and Tal Goldstein, 'Structuring the national cyber defence: in evolution towards a Central Cyber Authority', *Journal of Cyber Policy*, Vol.2 (Issue 1), 2017, pp. 16-25.

Matania, Eviatar, Lior Yoffe, and Michael Mashkautsan, 'A Three-Layer Framework for a Comprehensive National Cyber-security Strategy', *Georgetown Journal of International Affairs*, Volume 17, Number 3, Fall/Winter 2016, pp. 77-78

Nakashima, Ellen, 'Hacks of OPM databases compromised 22.1 million people, federal authorities say', *The Washington Post*, 10 July 2015. Available at: https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/

National Cyber Incident Response Plan, (Department of Homeland Security, December 2016). Available at: https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

Netherlands Ministry of Foreign Affairs, Letter to the parliament on the international legal order in cyberspace, 26 September 2019, *and Appendix: International law in cyberspace*. Available at: https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace

Pernik, Piret, 'National Cyber Security Strategies: The Estonian Approach', 22 June 2017. Available at: https://www.cncs.gov.pt/content/files/estonian_cyber_security_strategy_-_piret_pernik.pdf

Peterson, Andrea, 'The Sony Pictures hack, explained', *Washington Post*, 19 December. 2014. Available at: https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/

Public Report of the Committee of Inquiry into the Cyber Attack on Singapore Health Services Private Limited's Patient Database on or around 27 June 2018. Available at: https://www.mci.gov.sg/-/media/mcicorp/doc/report-of-the-coi-into-the-cyber-attack-on-singhealth-10-jan-2019.ashx

Ruiz, Monica M., 'Is Estonia's Approach to Cyber Defence Feasible in the United States', *War on the Rocks*, 9 January 2018. Available at: https://warontherocks.com/2018/01/estonias-approach-cyber-defense-feasible-united-states/

Ruiz, Monica M., 'To Bolster Cybersecurity, the US Should Look to Estonia', *WIRED*, 14 February 2020. Available at: https://www.wired.com/story/opinion-to-bolster-cybersecurity-the-us-should-look-to-estonia/

Sanger, David E., 'Obama Order Sped up Wave of Cyberattacks Against Iran', *The New York Times*, 1 Jun 2012. Available at: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

Sanger, David E., Sanger and Nicole Perlroth, 'U.S. Escalates Online Attacks on Russia's Power Grid', *The New York Times*, 15 June 2019. Available at: https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html

Schmitt, M. (Ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013)

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

'Singapore to cut off public servants from the internet', *The Guardian*, 24 August 2016. Available at: https://www.theguardian.com/technology/2016/aug/24/singapore-to-cut-off-public-servants-from-the-internet

DOI: 10.19165/2020.6.0129

Singapore's Cybersecurity Strategy. Available at: https://www.csa.gov.sg/news/publications/~/media/0ecd8f671af2447890ec046409a62bc7.ashx

Smith, Rebecca, and Rob Barry, 'America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It', *The Wall Street Journal*, 10 January 2019. Available at: https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112

Sulmeyer, Michael 'How the U.S. can play Cyber Offense'Foreign Affairs, 22 March 2012. Available at: https://www.foreignaffairs.com/articles/world/2018-03-22/how-us-can-play-cyber-offense.

Tamkin, Emily, '10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?', *Foreign Policy*, 27 April 2017. Available at: https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/

'The Big Read: As more cyberattacks loom, Singapore has a weak 'first line of defence'', *TODAY*, 23 February 2019. Available at: https://www.todayonline.com/big-read/big-read-more-cyber-attacks-loom-singapore-weak-first-line-defence

'The Big Read in Short: Singapore's weakest link in cyber security', *TODAY*, 23 February 2019. Available at: https://www.todayonline.com/big-read/big-read-short-singapores-weakest-link-cyber-security

U.S. Cybersecurity and Infrastructure Security Agency Alert TA18-074A - *Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors*, 15 March 2018. Available at: https://www.us-cert.gov/ncas/alerts/TA18-074A

Weimann, Gabriel, *Terror on the Internet* (Washington, DC: United States Institute of Peace, 2006)

Weimann, Gabriel, *Terrorism in Cyberspace: The Next Generation* (New York: Columbia University Press, 2015)

Weimann, Gabriel, 'Cyberterrorism: The Sum of All Fears?' *Studies in Conflict & Terrorism*, 28:129–149, 2005

DOI: 10.19165/2020.6.0129

Web-Based Resources

Alexander, Audrey, and Bennett Clifford, 'Doxing and Defacements: Examining the Islamic State's Hacking Capabilities', *CTC Sentinel*, April 2019, pp.23-24. Available at: https://ctc.usma.edu/doxing-defacements-examining-islamic-states-hacking-capabilities/

Australian Signals Directorate (Australian Cyber Security Centre), *Essential Eight Maturity Model* (July 2019). Available at: https://www.cyber.gov.au/publications/essential-eight-maturity-model

Australian Signals Directorate/Australian Cyber Security Centre, *Strategies to Mitigate Cyber Security Incidents – Mitigation Details*, February 2017. Available at:https://www.cyber.gov.au/sites/default/files/2019-03/Mitigation_Strategies_2017_Details_0.pdf

Canadian Centre for Cybersecurity, '5 Practical Ways to make Yourself Cybersafe'. Available at: https://www.cyber.gc.ca/sites/default/files/publications/five-practical-ways-yourself-ef.pdf

Carlin, John P., 'Inside the Hunt for the World's Most Dangerous Terrorist', *Politico*, 21 Nov 2018. Available at: https://www.politico.com/magazine/story/2018/11/21/junaid-hussain-most-dangerous-terrorist-cyber-hacking-222643

Cavelty, Myriam Dunn, and Victor Mauer (Eds.), *International CIIP Handbook Vol.II: Analysing Issues, Challenges, and Prospects*. Center for Security Studies, ETH Zurich (2006). Available at: https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP-HB-2006-2.pdf

Cyber Terrorism: Assessment of the Threat to Insurance, Cambridge: Centre for Risk Studies, November 2017. Available at:https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/pool-re-cyber-terrorism.pdf

Developing Cyber Resilient Systems: A Systems Security Engineering Approach, NIST Special Publication 800-160, Vol. 2, November 2019. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf

Finland's Cyber Security Strategy 2019, Turvallisuuskomitea (The Security Committee). Available at: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf

Greenberg, Andy, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History', *WIRED*, 22 August 2018. Available at: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Goh, Gillian, 'Overview of the Group of Governmental Experts and Open-ended Working Group Processes'. Available at: https://www.unidir.org/sites/default/files/conferences/pdfs/overview-of-the-group-of-governmental-experts-and-open-ended-working-group-processes-eng-0-786.pdf

Liv, Nadine, *United Cyber Caliphate*, International Institute for Counter-Terrorism, 20/3/2019. Available at: https://www.ict.org.il/Article/2361/United_Cyber_Caliphate#gsc.tab=0

National Security Agency, 'NSA'S Top Ten Cybersecurity Mitigation Strategies', March 2018. Available at:https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf

DOI: 10.19165/2020.6.0129

Ross, Ron, Victoria Pillitteri, Richard Graubart, Deborah Bodeau and Rosalie McQuaid, "Developing Cyber Resilient Systems: A Systems Security Engineering Approach," NIST, 27 November 2019. Available at: https://www.nist.gov/publications/developing-cyber-resilient-systems-systems-security-engineering-approach

Schmitt, Michael, 'The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis', *Just Security*, 14 October 2019. Available at: https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/

DOI: 10.19165/2020.6.0129