IGF 2021

Best Practice Forum Cybersecurity

on the use of norms to foster trust and security

Testing Norms Concepts against Cybersecurity Events

BPF WORKSTREAM 2 DRAFT REPORT

NOVEMBER 2021

Testing norms concepts against cybersecurity events

How would specific norms have been effective at mitigating adverse cybersecurity events? The following is a discussion paper that interrogates which are the core ideas behind prominent cybersecurity normative agreements that had the most continuity through various incidents. Since 2018, the Internet Governance Forum (IGF) Best Practice Forum on Cybersecurity (BPF) has focused its efforts on the evolution, implementation, and impact of international cybersecurity norms. In 2021, by writing background briefs for historical cybersecurity events, the authors' review, evaluation and analysis take into consideration the Best Practice Forum on Cybersecurity's prior reports, as well as other published research and reports, to conclude whether and how cyber norms have been successful at mitigating the adverse effects of these events. In some cases we conclude that important cybersecurity events may have supported norms implementation, or expanded the scope of an existing norm.

Editor:
Mallory Knodel <mknodel@cdt.org>;

Authors:
Anastasiya Kazakova, Niamh Healy, Allison Wylde, Barbara Marchiori de Assis, Fred Hansen, Evan Summers, Louise Marie Hurel, Ying Chu Chen, Mallory Knodel, Apratim Vidyarthi.

IGF Secretariat consultant:
Wim Degezelle.

Disclaimer:
The views and opinions expressed herein do not necessarily reflect those of the United Nations Secretariat. The designations and terminology employed may not conform to United Nations practice and do not imply the expression of any opinion whatsoever on the part of the Organization.

Table of contents

Introduction

The Best Practice Forum on Cybersecurity of the Internet Governance Forum has set out to test cybersecurity norms concepts against significant historical internet events in order to answer the central question: How would specific norms have been effective at mitigating adverse cybersecurity events?

In a discussion paper, expert contributors bring forward past analyses from the BPF Cybersecurity that connect the core ideas behind cybersecurity normative agreements, and present details of the actual risks, told through the voices of those most affected, to cybersecurity and human rights from incidents around the world of data leaks, vulnerability disclosures, malware and others.

First we identified criteria to select major historical cybersecurity events (including adverse events such as incidents) that are representative of cybersecurity issues, and that in some cases may have informed cyber norms development. Second we analysed a subset of those significant events, especially those that were or might have been impacted by or influenced the creation of global cybersecurity norms. Lastly we conducted qualitative research to include the voices of those affected by cybersecurity events through expert contributor-led interviews with incident responders and victims of historical cybersecurity events to determine first-hand perception of the research question, “how would specific norms have been effective at mitigating adverse cybersecurity events?”

Building on the past work of the BPF Cybersecurity, a group of expert contributors sought to answer our central research question through desk research and analysis of nine significant cybersecurity events.

For four of those events, researchers additionally identified both victims of the attacks and those who helped mitigate them, and interviewed them for an additional deep dive into the research question through qualitative methods. In describing the events, and in four cases those most affected by the events, researchers analysed through summative evaluation of present-day proposed norms that would have had influence or impact, and identify any proposed cyber norms that have resulted from the incidents. Our findings, where possible, are supported through qualitative interviews with those most affected.

The nine chosen cyber incidents had the minimum elements of: coverage by secondary sources (media, academia) and at least three primary sources; demonstrable harm at scale (number affected, impacted community); successful mitigation (was it attributed? fixed?); relationship to cybernorms. We ensured that our analysis was complete by mapping events that were distributed over time; from a variety of stakeholder groups; demonstrating the gamut of incident types, and with geography diversity.

For interviews, we ensured baseline consistency in interrogating our research question with the following loose script:

- Describe the incident and your role.
- What do cyber norms mean to you?
- What cyber norms do you think apply in this case?
- What cyber norms do you think have been, or would have been, helpful in this case?
- What cyber norms did you, or might you hope to, see arising from this case?

Analysing cybersecurity events

The following is a table that captures and highlights the main qualities of each of the events that our group of expert contributors analysed against mitigations that included or impacted cybersecurity norms.

Date	**Type**	**Countries**	**Event**	**Target**	**Attribution**
Jun 1998	Malware	Taiwan	**CIH virus**	Indistinct (all vulnerable systems online)	Unclear
Apr 2007	DDoS	Estonia	**Estonian DDoS attacks**	Estonia	Public policy protest
Mar 2009	APT	Tibet	**Ghostnet***	Tibetan institutions	Undetermined. Attack servers predominantly based in China
Jun 2010	APT, malware, Control systems breach	Iran	**Stuxnet**	Iran's nuclear program	Israel
Jun 2013	Technique disclosure	Global	**Snowden disclosures**	Global mass surveillance	US, Canada, UK, Australia, New Zealand
Apr 2014	Vulnerability	Global	**Heartbleed***	None	None
Jan 2018	APT	Mexico, Canada, Saudi Arabia, Palestine, Bahrain, Kazakhstan, Morocco, UAE	**NSO Group's Pegasus***	Human rights defenders, journalists	Governments using NSO Group commercial software
Jan 2018	Breach	India	**Aadhar data breach**	Indian citizens	[Sale of data]
Dec 2020	Supply chain	US/ global	**Solarwinds***	Compromise of government agencies and private companies (18,000+) followed by targeted espionage	APT29 / Organised cyber criminals

For each of these events we present the basic narrative of who, what, where, when and why supported with secondary source citations. What happened after the incident, or its mitigation, is then analysed to present how it was responded to and if cybersecurity norms played a role or were influenced as a result of the event. Lastly we present known information about the victims of the attack and their direct views on how norms did or could have shaped the incident and its outcomes.

For events marked with a * researchers conducted qualitative analysis to understand directly from those most affected by the incident their views on the relationship to mitigating the incident and cyber norms.

CIH virus (1999)

CIH malware, also known as Chernobyl or Spacefiller, is a very dangerous malware which targeted Microsoft Windows and specifically infected Windows 95, 98 and ME[1]. The name for the malware came from the alleged author, Chen Ing-hau[2], a Taiwanese computer engineering student. The malware is also sometimes referred to as Spacefiller, highlighting its ability to take up file space on computers and prevent anti-virus software from running. It is believed to be the first malware known to have the power to damage computer hardware. First detected as early as 1998, some sources state that its payload was triggered in April 16, 1999 which was the 13th anniversary of the disaster at the Chernobyl nuclear reactor[3].

Chen claimed to have written the malware as a challenge against bold claims of antivirus software developers about their products' efficiency. So he created the original virus to challenge those products. The spread of the malware began in Taiwan, and then spread globally quickly. The CIH-infected file is executed on a system and the virus becomes resident, infecting every executable accessed within empty, unused spaces in the file. Next, it breaks itself up into smaller pieces and inserts its code into these unused spaces. The virus only works on Windows 9X and ME OS. It cannot work on Windows NT or later Windows versions. Because the virus broke the BIOS, many producers made hardware modifications to prevent the damage.

It should also be noted that a virus seldom causes hardware failure, but the CIH virus disrupted the work of any infected system by deleting the data in the Flash BIOS[4], thus making it impossible to even boot the computer and in most cases the cost of the repair exceeded the cost of a new laptop (the drive, video card and other hardware are also affected as a consequence), resulting in damaged computers being simply thrown away.

[1] https://www.f-secure.com/v-descs/cih.shtml
[2] https://www.linkedin.com/in/cih-taiwan-2093224b/
[3] http://virus.wikidot.com/cih
[4] https://encyclopedia.kaspersky.com/knowledge/damage-caused-by-malware/

Interestingly, the first victims of the malware were Chen's classmates at Tatung University, however prosecutors in Taiwan could not charge Chen at the time because no victims came forward with a testimony, so Chen was detained and investigated in 2000, but he was never convicted of any crime. This case has further led to the adoption of a **specialized computer crime legislation in Taiwan**[5].

What Cyber Norms Could Have Been Helpful?

- Secure software development and trustworthy computing: In 2002 following the incident, the **CEO of Microsoft Bill Gates sent**[6] **the internal memo informing the colleagues about this nascent normative framework**[7] perhaps in part because the CIH virus has been among the most devastating malware targeting Windows machines, but its spread has increased the industry's awareness of a necessity to invest more into secure software development and trustworthy computing practices.

Estonian DDoS attacks (2007)

In April of 2007, there were a series of cyberattacks which targeted websites of Estonian organizations, including Estonian parliament, banks, ministries, newspapers and broadcasters. The series of cyberattacks lasted almost for 22 days[8]. The internet services from the government nearly collapsed, at a time when Estonia depended fully on internet connectivity to deliver critical government services. The email services, online banking, web-based government services have been largely hit, impacting many citizens in Estonia (a population of about 1.3 million people).

In the chain of those attacks, there were in particular three DDoS attacks and a few more complex attempts to hack into systems, for example using SQL injection. Some of these attacks were successful at non-critical sites[9]. At the same time it was reported that the 2007 attacks did not damage much[10] of the Estonian IT infrastructure because they were not sophisticated, and also because the limited size of the country allowed it to quickly respond to incidents and mitigate the impact for national networks. However, these attacks were a wake-up call for the country and other NATO members, highlighting a new attack vector and vulnerability.

The Estonia government thought the attacks were from Russia because of political issues at that time. But the Russian government denied the accusation. As a member of NATO, Estonia requested emergency

[5] https://www.parenting.com.tw/article/5020407
[6] https://www.wired.com/2002/01/bill-gates-trustworthy-computing/
[7] https://docs.microsoft.com/en-us/previous-versions/ms995349(v=msdn.10)?redirectedfrom=MSDN
[8] https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf
[9] https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf
[10] https://www.files.ethz.ch/isn/143191/rp_76.pdf

assistance, however, the lack of timely response revealed that NATO did not have a 'coherent cyber doctrine and a comprehensive cyber strategy'[11].

What Cyber Norms Could Have Been Helpful?

- Requesting for assistance: the norm H in the 2015 UN GGE report[12] which says that '*states should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts*.'
- The majority of norms, including on the protection of critical infrastructure, which emerged together with the 2015 UN GGE report could have been helpful at the event of these cyberattacks. Their possible existence in 2007 could have already greatly systematized possible options which Estonia as a victim state might have to defend itself as well as how it could have cooperated better with its allies for investigation, remediation and attribution.
- Together with these norms, **greater clarity on the application of international law to cyberspace** could have also served Estonia as a victim state with a better understanding on how to qualify and react to these cyberattacks. Some countries, including Estonia, have since pushed for such clarity.

What Cyber Norms Have Arisen As a Result?

- The direct result of the cyberattacks was the launch by NATO of internal assessment of its cybersecurity and infrastructure defenses, and further greater awareness and work on a coherent cybersecurity strategy within NATO. The internal assessment led to the report issued to the allied defense ministers in October 2017 and helped to create **an intergovernmental cyber defense policy** as well as the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia.[13]
- The Tallinn Manual,[14] as a consequence after these attacks, has become an influential resource for legal advisers and policy experts dealing with cyber issues. This report outlined international laws which are considered applicable to the cyber realm. The manual provided a total of ninety-five rules addressing cyber conflicts and most likely informed the work of governmental experts at the UN which later in 2013 and 2015 agreed on the set of eleven non-binding cyber norms.

[11] R. Hughes, NATO and Cyberdefence, Mission Accomplished?, April 2009, No 1/4.

[12] https://undocs.org/A/70/174

[13] https://ccdcoe.org

[14] https://ccdcoe.org/research/tallinn-manual/

GhostNet (2009)

GhostNet was a large-scale cyber espionage campaign discovered in March 2009, following a ten-month investigation by the Information Warfare Monitor (IWM).[15] In this campaign, attackers used social engineering to distribute malware to targeted machines. The investigation of the attack began at the request of the Office of His Holiness the Dalai Lama, and Tibetan government and civil society organisations were extensively affected. The investigation by the IWM however revealed a much larger network of high-value, compromised computers, consisting of 1,295 computers in 103 countries.[16] Particularly notable about this attack was the public documentation of the campaign through the published report by IWM and the method of attack that used highly personalised social engineering to infect the campaign's targets

This case study was completed using analysis of publicly available written documents, including newspaper reporting and technical publications about the campaign, and interviews with individuals directly involved in responding to the campaign: Dr Shishir Nagaraja (University of Strathclyde) and Lobsang Gyatso Sither (Tibet Action Institute).

There had been historical allegations of cyber attacks against the Tibetan community in the years prior to the discovery of GhostNet.[17] Investigation of GhostNet by IWM began following a specific request by the Office of His Holiness the Dalai Lama (OHHDL).[18] The IWM team consisted of researchers from the SecDev Group, a think-tank based in Ottawa, Canada, and the Munk Centre for International Studies, University of Toronto.[19] An initial investigation by the research team discovered malware on computers within the OHHDL, other Tibetan government institutions, and Tibetan non-governmental organisations (NGOs).[20] Through an analysis of this malware, the researchers identified servers associated with the attack and mapped out a wider network of control servers and compromised computers. The attack was investigated in 2008 and 2009, with the report by IWM published in March 2009.

The malware was spread through a phishing attack where victims of the attack were targeted through fraudulent emails containing either a malicious link or file attachment.[21] The link or file would then direct infected computers to connect to a control server and await further instructions, while the user would be left unaware of the infection.[22] The attack was particularly innovative in how it was spread: specifically targeting the psychology and sociology of affected users.[23] For example, some malicious emails used

[15] http://news.bbc.co.uk/1/hi/world/americas/7970471.stm; https://www.nytimes.com/2009/03/29/technology/29spy.html; https://www.theguardian.com/world/2009/mar/30/china-dalai-lama-spying-computers
[16] https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf, p 5
[17] https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf, p 13
[18] https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf
[19] http://news.bbc.co.uk/1/hi/world/americas/7970471.stm
[20] https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf
[21] https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf, p 18
[22] https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf, p 18
[23] Author interview.

content stolen from previously-infected computers to imitate legitimate communications when targeting new users to enhance the apparent legitimacy of the communication.[24]

Infected computers were directed to download gh0st RAT or similar Trojan malware, which allowed the attackers to take full control of infected computers, search for and download files, and open attached devices such as microphones and webcams.[25]

Servers associated with the attack were mostly based in China,[26] but the researchers who discovered the attack did not conclusively attribute it to China or any other particular actor.[27] The Chinese government denied involvement in the attack.[28] The purpose of the attack appeared to be espionage.

The GhostNet campaign was one of the first publicly-reported targeted cyberattacks.[29] After the publication of the GhostNet report, more targeted cyberattacks began to be publicly reported and documented.

The investigation of the attack by the IWM was prompted by a request from the Tibetan government, and the investigation and subsequent report by IWM predominantly focused on the impact of the attack on the Tibetan government and Tibetan NGOs. However, during the course of the investigation, the IWM researchers identified the command and control servers used in the attacks, which in turn revealed a much larger network of affected computers.[30] The IWM researchers identified over 1,295 affected computers in 103 countries, including networks belonging to foreign ministries and regional organizations like ASEAN and NATO.

Interview participants observed that prior to the discovery of the attack, there was awareness of cyber-attacks and cybersecurity within the Tibetan community.[31] However, there was no concrete knowledge of the extent of targeted attacks against Tibetan groups or clear evidence of attacks.[32] The publication of the IWM report helped identify the extent of cybersecurity risks faced by the Tibetan community, how cyber-attacks were being carried out, and what the impact of cyber-attacks were, underscoring the importance of cybersecurity to the Tibetan community.[33] The discovery of GhostNet highlighted the significance of cybersecurity for both Tibetan organisations involved in advocacy and campaigns work, and for individuals working directly in Tibet.[34] Particularly notable about GhostNet was how *widespread* the attack was. Before the attack, there had been an assumption among some Tibetan organisations that

[24] https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf, p 18
[25] https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf, p 18
[26] https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf, p 22
[27] https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf, p 48 – 49
[28] http://news.bbc.co.uk/1/hi/world/americas/7970471.stm
[29] Author interview.
[30] https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf, p 30
[31] Author interview.
[32] Author interview.
[33] Author interview.
[34] Author interview.

attacks were limited, directed only towards high-level or high-profile individuals or organisations.[35] The discovery of GhostNet disrupted this assumption and suggested that cybersecurity was a **community-level concern**.[36]

The discovery of the GhostNet Campaign, along with mass protests in Tibet in 2008, led to the founding of the Tibet Action Institute in 2009.[37] In the years following GhostNet, particularly 2011 onwards, Tibet Action Institute began to offer information security training to the Tibetan community, focused on improving cyber-hygiene.[38] They adopted a **hyperlocal data-driven approach**, which explained best cybersecurity practices using Tibetan culture and humour.[39] Through work with partners like Citizen Lab, the Tibet Action Institute began to **monitor how threats evolved over time**.[40] **Cybersecurity training was adjusted as threats changed over time**: for example, material initially focused on being careful with email attachments changed to focus on the risks associated with Google Drive links, in response to changing attacker behaviour.[41] In 2018, the Tibetan Computer Emergency Readiness Team (TibCERT) was founded.[42] A key aim of the TibCERT is to enable information-sharing between Tibetan organizations using a shared Traffic Light Protocol (TLP), with the aim of enhancing Tibetan organizations' international collaboration.[43]

What Cyber Norms Could Have Been Helpful?

- Participants observed that norm J (report vulnerabilities and remedies) was well practiced in this case.[44] The Tibetan Central Administration's request for assistance from the IWM and their admittance of researchers into their facilities and networks permitted a thorough and publicly documented investigation of the GhostNet campaign.
- While the eleven norms agreed in the 2015 GGE report are directed at states, future international efforts to develop norms of responsible behaviour in cyberspace might consider what norms are applicable to non-state actors such as non-governmental organisations like the Central Tibetan Administration and the Tibetan civil society organisations affected by the campaign.
- As this attack was not conclusively attributed, norm C (states should not knowingly allow their territory to be used for intentionally wrongful acts using ICTs) of the 2015 UN GGE report may have been of relevance and utility.
- Some interview participants understood the targets affected by the campaign as critical infrastructure, which means norms F and G of the 2015 UN GGE report may be considered relevant to this campaign. Norm F indicates that states should not conduct or knowingly support activity that intentionally damages critical infrastructure while norm G indicates that states should take appropriate measures to protect their critical infrastructure from ICT threats. Future efforts

[35] Author interview.
[36] Author interview.
[37] Author interview.
[38] Author interview.
[39] Author interview.
[40] Author interview.
[41] Author interview.
[42] https://tibcert.org
[43] Author interview.
[44] 2015 UN GGE report https://undocs.org/A/70/174; author interview.

to develop and operationalise norms should offer greater clarity and specification on what constitutes critical infrastructure.

- In this case, non-state actors played a significant response role in investigating, documenting and responding to this campaign. As discussed in the section on the Heartbleed bug, norms to promote the neutrality of the technical community, incident responders and vulnerability analysts can help ensure effective and timely incident response and vulnerability mitigation.
- Some participants thought the norms would be of limited use in mitigating the campaign's effects on non-governmental organisations. Future efforts might contemplate whether states have special responsibilities to assist non-governmental organisations in cybersecurity-related matters *or* have particular responsibility to avoid adversely affecting the security of non-governmental organisations.

What Cyber Norms Have Arisen As a Result?

- The level of public reporting of the GhostNet campaign was uncommon at the time of the discovery of the campaign. Since the publication of the GhostNet report, thorough and *public* documentation of cyber espionage campaigns and other significant cybersecurity incidents is much more commonplace.

Stuxnet (2010)

A control systems breach was discovered at the Natanz Nuclear Complex in Natanz, Iran. Different from other malware that hijacked computers or stole information from them, the Stuxnet worm caused the destruction of the physical equipment controlled by infected industrial control systems. Specifically, the attackers designed a malware that could manipulate the Siemens's WinCC/PCS 7 Supervisory Control and Data Acquisition (SCADA) control software responsible for monitoring and controlling the centrifuges' speed. Siemens' WinCC/PCS 7 was the SCADA model used in the Natanz Nuclear Complex, in Iran, the target of the Stuxnet attack. Although most infections of the malware were found in Iran, the Stuxnet worm spread around the globe.

Highly complex, the Stuxnet worm combined several components, such as "zero-day exploits [unknown vulnerabilities], a Windows rootkit, the first ever PLC rootkit [programmable logic controller], antivirus evasion techniques, complex process injection and hooking code, network infection routines, peer-to-peer updates, and a command-and-control interface."[45] Interestingly, the worm only allowed each infected computer to infect up to three other devices and was designed to self-destruct. Simply put, Stuxnet was designed to reach a specific target.[46]

[45] Falliere, N.; Murchu, L.O.; & Chien, E. (February 2011). "W32. Stuxnet Dossier." Symantec, p. 1-2. https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf

[46] Singer, P. W. (2015). Stuxnet and its hidden lessons on the ethics of cyberweapons. *Case W. Res. J. Int'l L.*, *47*, 79.

Given that the computers were not directly connected to the Internet, it was not possible to launch the attack remotely; therefore, **the attack was designed to be launched through USB flash drives**. To reach Natanz Nuclear Complex, the attackers targeted five other organizations in Iran that would help get them to their final target, making these five organizations the attack's "patient zero." Four of these organizations have been identified.[47] These four organizations were contractors of the Natanz nuclear power plant, providing a gateway through which contractors' devices infected with Stuxnet could reach the attackers' final target.

The worm was probably damaging the centrifuges at the Natanz plant, in Iran, for about a year when discovered in July 2010. The attacks against the five Iranian organizations took place in June and July 2009, and later in March, April, and May 2010.[48] Notably, one year before, the nuclear power plants had already been attacked by an early version of the malware, which manipulated the valves on the centrifuges to increase the pressure inside them. Such an increase in pressure damaged not only the equipment but also the uranium enrichment process. The Stuxnet attack was unleashed as the nuclear power plant was recovering from the effects of this previous attack.

Although no country has taken responsibility for the Stuxnet attack, it is widely acknowledged that the attack was the result of a collaboration between the United States and Israel through the so-called "Operation Olympic Games."[49] Started during the Bush Administration, the "Operation Olympic Games" aimed to slow down the Iranian Nuclear Program to buy time for sanctions and diplomacy with Iran to take effect.

It has been presumed that the cyber-attack goal was to sabotage Natanz nuclear facility by reprogramming the PLCs to operate according to the attackers' instructions. Ultimately, the goal was to hamper Iran's nuclear bomb-making program. Although the attack targeted the Natanz nuclear facility, the Stuxnet worm spread around the world and infected other industrial control systems indiscriminately. **Stuxnet was considered the world's first digital weapon** and raised the concern of the destructive impact of cyber weapons.[50]

What Cyber Norms Could Have Been Helpful?

- The global consequences of the Stuxnet attack brought cyber warfare and digital weapons discussions into the forefront. While the impact of previous attacks was limited to the digital

[47] The companies identified were Foolad Technic, Behpajooh, Neda Industrial Group, and CGJ, believed to be Control Gostar Jahed. Zetter, K. (March 2014). "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." In *Wired*. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

[48] Zetter, K. (November 2011). "Report: Stuxnet Hit 5 Gateway Targets on Its Way to Iranian Plant." In *Wired*. https://www.wired.com/2011/02/stuxnet-five-main-target/

[49] Sanger, D. E. (June 2012). "Obama Order Speed Up Wave of Cyberattacks against Iran." In *The New York Times*. https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

[50] Lucas, G. R. (2014). Permissible preventive cyberwar: Restricting cyber conflict to justified military targets. In *The Ethics of Information Warfare* (pp. 73-83). Springer, Cham; Singer, P. W. (2015). Stuxnet and its hidden lessons on the ethics of cyberweapons. *Case W. Res. J. Int'l L.*, *47*, 79; Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon*. Broadway books.

realm, the Stuxnet worm caused physical damage and could be considered an "armed attack" by international law standards.[51] Despite avoiding the expansion of the Iranian nuclear program,[52] Stuxnet was neither in response to an armed attack nor self-defense, potentially violating the prohibition on the use of force set forth in Article 2(4) of the UN Charter.

- Although the 2013 Tallinn Manual's International Group of Experts were divided on whether the Stuxnet attack reached the "armed attack" threshold, all members agreed that a cyber-attack alone could potentially cross such a threshold.[53] Tallinn Manual 2.0 International Group of Experts were also divided on whether the Stuxnet attack reached the armed attack threshold, but all agreed that the attack consisted of a use of force.[54] For the Group of Experts, whether the Stuxnet attack could be considered an international armed conflict remained unclear due to the challenges of attributing it to a State.[55] Some called the Stuxnet attack a "Pyrrhic victory;" that is, although the attack delayed the Iranian Nuclear Program, Stuxnet also revealed a blueprint for cyberweapons and opened the path for cyber armed attacks against countries' infrastructure.[56] Determining the threshold of "armed attack" for cyber operations is quite challenging.[57] For instance, the Heads of State and Government of NATO Allies have reaffirmed that the invocation of the Collective Defense in case of a cyber-attack against one Ally, set forth in Article 5 of the NATO Treaty, "would be taken by the North Atlantic Council on a *case-by-case basis*."[58]
- Given that Stuxnet was launched miles away from its target, and even months before infecting its final target, it is possible to consider Stuxnet "the first truly autonomous weapon."[59] Plus, despite acknowledging the participation of Israel and US in the attack, Stuxnet traced back to servers in Denmark and Malaysia, highlighting the challenge of determining the origin of the attack and attribution.[60] Aside from Stuxnet automated nature, the worm also engendered important ethical discussions regarding proportionality and discrimination in warfare. Although the Stuxnet attack caused less damage than traditional weapons, it also enabled **a preemptive attack that impacted not only its target but also other industrial control systems around the world**.[61] In other words, while the attack seemed to be in consonance with the proportionality principle in terms of the

[51] United Nations Institute for Disarmament Research – UNIDIR (2013). *The Cyber Index: International Security Trends and Realities*, p. xi. https://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf;

[52] In 2010, the International Atomic Energy Agency (IAEA) reports suggested problems with Iran's nuclear efforts, albeit being denied by Iranian authorities. https://www.nytimes.com/2010/11/24/world/middleeast/24nuke.html?_r=0

[53] Schmitt, M. N. (Ed.). (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press, p. 58, 83-84.

[54] Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press, p. 342.

[55] Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press, p. 384.

[56] Clayton, M. (September 2011). "From the man who discovered Stuxnet, dire warnings one year later." In *CSMonitor*. https://www.csmonitor.com/USA/2011/0922/From-the-man-who-discovered-Stuxnet-dire-warnings-one-year-later

[57] Schmitt, M. N., & Vihul, L. (2016). The nature of international law cyber norms. In Osula, A. M., & Rõigas, H. (Eds.). *International cyber norms: Legal, policy & industry perspectives*. NATO Cooperative Cyber Defence Centre of Excellence, p. 44.

[58] Brussels Summit Communiqué (June 14, 2021); Wales Summit Declaration (September 5, 2014)

[59] Singer, P. W. (2015). Stuxnet and its hidden lessons on the ethics of cyberweapons. *Case W. Res. J. Int'l L.*, *47*, 79, p. 83

[60] Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon*. Broadway books.

[61] Singer, P. W. (2015). Stuxnet and its hidden lessons on the ethics of cyberweapons. *Case W. Res. J. Int'l L.*, *47*, 79, p. 85.

physical impact caused, it violated the discrimination principle by infecting other computers beyond the SCADA systems of Natanz nuclear power facilities.

- Despite infecting other computers, the Stuxnet attack had some elements that revealed the attackers concern to avoid its indiscriminate spread, particularly civilian incidental damage. As mentioned, the Stuxnet worm was designed to infect up to three computers and self-destruct afterwards. When formulating its Rule 54 about the need to choose the means or methods to prevent or at least mitigate civilian collateral damage in the case of a cyber-attack, the 2013 Tallinn Manual's International Group of Experts believed that the Stuxnet attack seemed to "have been planned with this Rule in mind" since it "seek out a specific type of industrial process-control systems."[62] Indeed, to lessen the collateral damage beyond the Natanz facilities and ensure its effectiveness against the Iran Nuclear Program, it is believed that Stuxnet was tested first in Israel to better understand how the worm would affect the industrial control systems.[63]
- Some authors have argued that **post-incident forensic analysis could help determine whether an automated cyber-attack was indiscriminate in nature** and whether the attack was in accordance with the legal principles of distinction and discrimination. In the case of the Stuxnet worm, studies revealed that: the attackers collected painstaking information about Natanz Nuclear Complex to ensure that the attack vector would access the specific networks and systems employed in the Natanz facility; despite spreading beyond its initial targets, Stuxnet did not damage other systems as it was designed to harm a system with the specific configurations identified at Natanz.[64]

What Cyber Norms Have Arisen As a Result?

- The 2015 and 2021 reports of the UN Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security (UN GGE) stressed the application of the UN Charter and other international law to the use of information and communications technologies (ICT) by States, urging them to refrain from using force against other States in consonance with such norms. The UN GGE also underscored the principles of proportionality and distinction, and that the international humanitarian law only applies in cases of armed conflict. Notably, the 2021 UN GGE report also pointed out "the need for further study on *how* and *when* these principles apply to the use of ICTs by States."[65]
- The impact of the Stuxnet attack pushed Iranian authorities to the negotiation table, and ultimately resulted in the "Joint Comprehensive Plan of Action," an agreement signed between Iran and the United States, France, Germany, the United Kingdom, Russia, and China in July 2015.

[62] Schmitt, M. N. (Ed.). (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press, p. 168-170.

[63] Broad, W. J. et al (January 2011). "Israeli Test on Worm Crucial in Iran Nuclear Delay." In *The New York Times*. https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

[64] Kaminska, M., Broeders, D., & Cristiano, F. (2021, May). Limiting Viral Spread: Automated Cyber Operations and the Principles of Distinction and Discrimination in the Grey Zone. In *Kaminska, M., Broeders D., and Cristiano, F.(2021)." Limiting Viral Spread: Automated Cyber Operations and the Principles of Distinction and Discrimination in the Grey Zone", 13th International Conference on Cyber Conflict:'Going Viral* (pp. 59-72). https://ccdcoe.org/uploads/2021/05/CyCon_2021_Kaminska_Broeders_Cristiano.pdf

[65] UN GGE (2021). A/76/135 Report of the Group of Governmental

Through the JCPOA, Iran started providing the International Atomic Energy Agency (IAEA) information related to nuclear activities in the country.[66]

Snowden disclosures (2013)

In June 2013 two Western media outlets -- the US's Washington Post[67] and the UK's Guardian[68]-- released reports of top secret documents that were leaked from the US federal government by intelligence contractor Edward Snowden inculpating the US, Canada, UK, Australia and New Zealand in operating a global surveillance network.

Now known as "the Snowden Disclosures", most major outlets across the five countries covered the disclosures in significant detail during 2013 and in the eight years afterwards, including The New York Times, the Canadian Broadcasting Corporation, the Australian Broadcasting Corporation, Der Spiegel, O globo, Le Monde, and L'espresso. Around 1.7 million US intelligence files,[69] 58,000 British intelligence files,[70] and 20,000 Australian intelligence files[71] were shared with journalists. It is unclear whether all the files shared with journalists have been disclosed to the public.

The files and subsequent reporting showed the existence of a broad global surveillance network implemented through treaties that enabled intelligence sharing between the five countries and other partners, including Sweden, Germany, Denmark, France, the Netherlands, Italy, Norway, Spain, Switzerland, Singapore, and Israel. The disclosures laid out the mechanisms by which these intelligence agencies gathered information broadly and deeply, including through the NSA's ability to access phone calls and emails of foreigners and US citizens, through a program developed by the NSA to record a foreign country's telephone calls, and through the use of XKeyscore, a program, to penetrate internet traffic and monitor targets in Europe and Africa.[72] The revelations also showed that private sector companies like Verizon complied with the NSA's data collection,[73] while others like Microsoft, Google, Yahoo, and

[66] https://www.armscontrol.org/factsheets/JCPOA-at-a-glance

[67] Barton Gellman, Aaron Blake & Greg Miller, *Edward Snowden comes forward as a source of NSA leaks*, Wash. Post. (June 9, 2013), https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html

[68] Glen Greenwald, Ewen MacAskill & Laura Poitras, *Edward Snowden: the whistleblower behind the NSA surveillance revelations*, The Guardian (June 11, 2013), https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

[69] Chris Strohm & Del Quentin Wilber, *Pentagon Says Snowden Took Most U.S. Secrets Ever: Rogers*, Bloomberg News (Jan. 9, 2014), http://www.bloomberg.com/news/2014-01-09/pentagon-finds-snowden-took-1-7-million-files-rogers-says.html.

[70] *David Miranda row: Seized files 'endanger agents'*, BBC (Aug. 30, 2013), https://www.bbc.com/news/uk-23898580.

[71] Cameron Stewart & Paul Maley, *Edward Snowden stole up to 20,000 Aussie files*, The Australian (Dec. 5, 2013), https://www.theaustralian.com.au/national-affairs/foreign-affairs/edward-snowden-stole-up-to-20000-aussie-files/news-story/5c082d0996d2435a412aa603fefa60ae.

[72] *See generally Snowden Revelations*, Lawfare (Oct. 30, 2021), https://www.lawfareblog.com/snowden-revelations.

[73] Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, The Guardian (June 6, 2013), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

Facebook complied with requests for cooperation with the NSA and GCHQ to weaken commercial encryption.[74]

The Snowden revelations had significant impacts globally, and for Snowden himself. In the US, various groups filed suit against the NSA[75] and have voiced support for Edward Snowden.[76] The public in the affected countries categorically disapproved of US surveillance.[77] The revelations also prompted governmental reviews of surveillance systems across the accused countries,[78] including President Obama's creation of an intelligence and communications technology review.[79] Simultaneously, the U.S. government charged Snowden with espionage and revoked his passport,[80] and multiple lawmakers across the Executive[81] and Congress[82] have called for his prosecution.

What Cyber Norms Apply?

- Deterrence: the Snowden revelations gave credibility to US cyberdefense and cyberwarfare capabilities, giving the US a stronger hand in bargaining with other states that engage in cyberattacks.[83]

What Cyber Norms Could Have Been Helpful?

- Enable journalists to coordinate with incident responders to prevent details about vulnerabilities in commonly-used software being shared with the public, since that information could be misused by malicious actors. Similarly, creating direct channels of communication to prevent the sharing or spread of software that could facilitate hacking or other types of cyberattacks.

[74] *See, e.g.*, Jeff Larson, *Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security*, ProPublica (Sept. 5, 2013), https://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption.

[75] *See, e.g.*, Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013); ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015).

[76] *See, e.g.*, *US: Statement on Protection of Whistleblowers in Security Sector*, Human Rights Watch (June 18, 2013), https://www.hrw.org/news/2013/06/18/us-statement-protection-whistleblowers-security-sector#.

[77] *Global Opinions of U.S. Surveillance*, Pew Research Center (July 14, 2014), https://www.pewresearch.org/global/interactives/global-opinions-of-u-s-surveillance/.

[78] *See, e.g.*, Nick Hopkins, Patrick Wintour, Rowena Mason & Matthew Taylor, *Extent of spy agencies' surveillance to be investigated by parliamentary body*, The Guardian (Oct. 17, 2013), https://www.theguardian.com/uk-news/2013/oct/17/uk-gchq-nsa-surveillance-inquiry-snowden.

[79] *See, e.g.*, Ewen MacAskill, *White House insists James Clapper will not lead NSA surveillance review*, The Guardian (Aug. 13, 2013), https://www.theguardian.com/world/2013/aug/13/white-house-james-clapper-nsa-surveillance-review.

[80] Peter Finn & Sari Horwitz, *U.S. charges Snowden with espionage*, Wash. Post (June 21, 2013), https://www.washingtonpost.com/world/national-security/us-charges-snowden-with-espionage/2013/06/21/507497d8-dab1-11e2-a016-92547bf094cc_story.html.

[81] Aaron Blake, *Clapper: Leaks are 'literally gut-wrenching,' leaker being sought*, Wash. Post (Aug. 8, 2013), https://www.washingtonpost.com/news/post-politics/wp/2013/06/09/clapper-leaks-are-literally-gut-wrenching-leaker-being-sought/.

[82] *Edward Snowden: Ex-CIA leaker drops out of sight, faces legal battle*, Chicago Tribune (June 10, 2013), https://www.chicagotribune.com/news/ct-xpm-2013-06-10-chi-edward-snowden-nsa-leaks-20130610-story.html.

[83] Henry Farrell, *The political science of cybersecurity IV: how Edward Snowden helps U.S. deterrence*, Wash. Post (Apr. 12, 2014), https://www.washingtonpost.com/news/monkey-cage/wp/2014/03/12/the-political-science-of-cybersecurity-iv-how-edward-snowden-helps-u-s-deterrence/; *see also* Matthew Waxman, *Snowden Disclosures and Norms of Cyber-Attacks*, Lawfare (Mar. 20, 2014), https://www.lawfareblog.com/snowden-disclosures-and-norms-cyber-attacks.

- Cyber norms for reporters and whistleblowers alike on what kind of information could be shared without endangering at-risk populations under authoritarian regimes implicated in intelligence operations might have been helpful.

What Cyber Norms Have Arisen As a Result?

- While norms deliberations rarely cite the Snowden Disclosures in plain terms because of the political difficulties that would create if any U.S. government representative was part of the body, many trends in norms setting post-Snowden can be inferred:
  - Somewhat strengthened oversight on data sharing and the breadth of surveillance programs.
  - More scrutiny over private-public cooperation in surveillance. After the disclosures, President Obama moved to split the NSA and US Cyber Command under different leaders. The NSA continued its activities under Title 50, whereas the US Cyber Command had Title 10 authority to conduct offensive cyber operations against adversaries.
  - Storage of metadata is now in the hands of telecom companies, rather than with the NSA at Fort Meade. The NSA now needs to obtain a warrant to access specific files that are relevant to any investigation.
  - Stronger collaboration, including notice to allies, when US cyber operations encroach on allies' territories.

Heartbleed (2014)[84]

The Heartbleed Bug is a serious vulnerability in the widely used popular OpenSSL cryptographic software library which was inadvertently introduced in April 2014. It was created after Robin Seggelmann, a programmer based in Germany, submitted an update code at 11:59 pm on New Year's Eve 2011. His update enabled the TLS extension "Heartbeat," but an error in his update code led to major ramifications, accidentally creating the "Heartbleed" vulnerability, as reported by the Guardian in 2014.[85]

The vulnerability was independently discovered by a team of security engineers at Codenomicon and a security researcher from Google Security, who first reported it to the OpenSSL team. Regarding its exploitation it is unknown if the vulnerability was abused in the wild. There are still discussions that, based on examinations of audit logs by researchers, it may have been exploited by attackers at least five months before discovery, announcement and mitigation. Later Codenomicon created the website

[84] Through interviews with Rauli Kaksonen, who worked at Codenomicon at the time of the discovery of the Heartbleed vulnerability and who is now a senior security specialist at the University of Oulu in Finland; Igor Kumagin, a cybersecurity expert at Kaspersky with more than 11 years of experience and work in Kaspersky Research and Development (RnD). Igor was the person responsible for vulnerability mitigation at Kaspersky and later building the company's vulnerability management and disclosure processes; Art Manion, a senior member of the Vulnerability Analysis team in the CERT Program at the Software Engineering Institute (SEI), Carnegie Mellon University. At the time of the discovery of the Heartbleed vulnerability, Art was a key expert coordinating the vulnerability notification from CERT/CC to its vendors and community.

[85] https://www.theguardian.com/technology/2014/apr/11/heartbleed-developer-error-regrets-oversight

heartbleed.com[86] to raise awareness about the vulnerability to both the wider public and those operating impacted websites and services.

The impact of the vulnerability was global and risks from exploitation were significant. Due to the popularity of OpenSSL many applications were impacted which enabled attacks that obtain a huge amount of sensitive data. It is not a design flaw in the SSL/TLS protocol specification, but an implementation problem, i.e. programming mistake in the popular OpenSSL library that provides SSL/TLS cryptographic resources to applications and services. This compromised the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content, as well as allowed attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users. This weakness allowed stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet.[87]

Discussing the response to this vulnerability, it should be noted that immediately after the discovery of the bug, NCSC-FI took up the task of verifying it, analyzing it further and reaching out to the authors of OpenSSL, and to software, operating system and appliance vendors, which were potentially affected. Later, however, the vulnerability had been found by others and the mitigation was completed by several researchers. Particularly, Bodo Möller and Adam Langley of Google prepared the fix for Heartbleed, while the resulting patch was added to Red Hat's issue tracker on 21 March 2014. Stephen N. Henson applied the fix to OpenSSL's version control system on 7 April 2014, and the first fixed version, 1.0.1g, was released on the same day. The Heartbleed vulnerability was a classic example of a coordination failure: two organizations Codenomicon and Google, both discovered the vulnerability around the same time, but when the vulnerability was reported a second time to the OpenSSL team, they assumed a possible leak and the vulnerability was quickly disclosed publicly. “A more coordinated response may have allowed further remediation to be available immediately at disclosure time”, said[88] Garret Wassermann, Vulnerability Analyst at CERT/CC.

What Cyber Norms Apply?

- Responsible reporting of vulnerabilities (Norm J of the UN 2015 GGE report[89]): the Heartbleed vulnerability triggered higher awareness of the industry and policy-makers of significant vulnerabilities and thus led to continuous improvement and development of vulnerability management and vulnerability disclosure best practices across public and private sectors.

What Cyber Norms Could Have Been Helpful?

- Norm on vulnerability exchange and coordination between states as well as non-state actors (including private sector, technical community, academia). We have heard from experts that still today not all technical experts can freely exchange vulnerability information with companies or

[86] https://heartbleed.com/
[87] https://us-cert.cisa.gov/ncas/alerts/TA14-098A
[88]https://insights.sei.cmu.edu/blog/cvd-series-principles-of-coordinated-vulnerability-disclosure-part-2-of-9/
[89] https://dig.watch/un-gge-report-2015-a70174

CERTs located in not like-minded or allied countries, which create security and safety risks for all. Therefore, **cyber norms promoting neutral status of technical community, incident responders, vulnerability analysts and researchers as well as CERTs** are important to ensure the effective and timely incident response and vulnerability mitigation.

- Norm on greater transparency in vulnerability handling by both the public and private sector to shed light on vulnerabilities, once they are discovered. In the ideal case and ideal world, all vulnerabilities should be reported (as a next step after discovery) to code owners and vendors responsible for development of vulnerability mitigation. In a real world, if vulnerabilities are retained and kept private, the global community needs greater transparency into why, under which criteria such vulnerabilities could be retained and who has access to this information to ensure the security and confidentiality of actors involved in vulnerability handling. The Global Commission on the Stability of Cyberspace (CSCS) already suggested the norm[90] for States to create a vulnerabilities equities process, and this could be taken as a basis for promoting further the norm across both public and private actors.

What Cyber Norms Have Arisen As a Result?

- Industry and technical community has matured and advanced vulnerability management and coordinated vulnerability disclosure processes and guidelines (especially since the Heartbleed vulnerability has become a case of uncoordinated efforts taken by independent researchers). The Heartbleed vulnerability led to greater cross-industry collaboration on vulnerability analysis, management and disclosure, and for instance FIRST (Forum of Incident Response and Security Teams) called[91] in 2015 for members, security and IT vendor communities to join forces and participate in a new Special Interest Group (SIG) on Vulnerability Coordination which later produced the fundamental Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure (updated in May 2020)[92].
- Greater awareness of precarity of open source software (OSS) and the necessity to standardize secure software development given its widespread use even in proprietary software. The Heartbleed vulnerability highlighted the existing lack of security practices for OSS and, particularly, the incident led to the establishment of the Core Infrastructure Initiative (CII), a project of the Linux Foundation to support free and open-source software projects that are critical to the functioning of the Internet and other major systems. The CII funds specific tasks such as providing compensation to developers to work full-time on an open-source software project, conducting reviews and security audits, deploying test infrastructure, and facilitating travel and face-to-face meetings among developers. The CII has been replaced by the Open Source Security Foundation (OpenSSF)[93]. Thus the goal was to change failed 'software economics' where multiple developers create a highly complex code for open-source software which is not properly tested.

[90] https://cyberstability.org/norms/#toggle-id-6
[91] https://www.first.org/newsroom/releases/20150325
[92]https://www.first.org/global/sigs/vulnerability-coordination/multiparty/FIRST-Multiparty-Vulnerability-Coordination.pdf
[93] https://openssf.org/

- Greater awareness across the industry to responsible vulnerability discovery and analysis. The Heartbleed vulnerability also led to the establishment of Google’s Project Zero which is tasked with finding zero-day vulnerabilities to help secure the Web and society.

Aadhar data breach (2018)

In early 2018 the largest Indian personal identification database, Aadhar, was reported to be leaking information on every registered Indian citizen (around 1.2 billion citizens which is almost 89% of India’s population in 2018), including names, bank details and sensitive personal data such as biometrics.[94]

The ‘Aadhaar Card’ collects citizens’ fingerprints, retina scans, and face photos. That information is connected to the users’ banking system. A journalist found that anyone can buy the Aadhaar card details from an anonymous group on WhatsApp at a very low price. The journalist bought the package and used the information to access the database for individual information easily. The data leak was first revealed after anonymous sellers over Whatsapp provided unrestricted access to the Aadhar database for nominal costs. As a result Indian citizens may face personal identity forgery or privacy exposure.

The Unique Identification Authority of India (UIDAI) refused the media report claiming there were no data leaks. They claimed there were no internal or external risks to the database, and the database is constitutional. There were also reports that this was not an actual leak, and attempted to make an arbitrary distinction that instead it was just a security mistake on the part of the government.

What Cyber Norms Apply?

- **The necessity to ensure the protection of personal data, including sensitive personal data.**

What Cyber Norms Have Arisen As a Result?

- In 2019 the Indian government also proposed the Personal Data Protection Bill to introduce a legal framework for protection of personal data of Indian citizens.

[94] https://www.google.com/url?q=https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/&sa=D&source=docs&ust=1637598921355000&usg=AOvVaw2rIGLXgGu-DErFYotbAyNO

Solarwinds (2020)

The SolarWinds breach occurred as part of a routine update for its Orion IT software. As with other client software, Orion was designed to download updates. A custom-made backdoor program then enabled attackers to gain access to the SAML and add malicious payload.

The breach, named Sunburst, was installed during routine updates, initiating the compromise. The program was hidden in legitimate software to appear as though it was a telemetry sending program. The program did not execute immediately. It was designed to evade antivirus (AV) protection and sandboxes. It tried to identify what monitoring or management software was running or blocking.

Sunburst was designed to provide the attackers with information about the entity through sending encoded DNS requests to the C&C server. The initial attack targeted more than 18,000 users with the attackers carefully selecting 100 entities for a deeper second stage attack. This deeper exploitation involved installing additional malware and/ or persistence mechanisms that allowed the exfiltration of data. The sophistication and targeted nature of the attack suggests extensively resourced, likely state supported attackers. The threat actor modified an Orion platform plug-in called SolarWinds.Orion.Core.BusinessLayer.dll. The sophisticated attack changed specific code in memory to avoid detection in the build process.[95]

"The malware masquerades its network traffic as the Orion Improvement Program (OIP) protocol and stores reconnaissance results within legitimate plugin configuration files allowing it to blend in with legitimate SolarWinds activity. The backdoor uses multiple obfuscated blocklists to identify forensic and anti-virus tools running as processes, services, and drivers."[96]At first there appeared to be no obvious connections to any previously observed tactics, techniques or procedures (TTP). The unknown attacker named UNC2452 or Dark Halo, appears to be a variant of the .NET module.

The actual time line was found to have started with secondary attacks in April 2020. The breach targeted confidential information belonging to multiple government agencies, organizations including the financial sector, universities and medical institutions, and cybersecurity companies. Victims included 425 of the US Fortune 500, the top ten US telecommunications companies, the top five US accounting firms, all branches of the US Military, the Pentagon, the State Department, as well as hundreds of universities and colleges worldwide. The second stage attack carefully extracted further targeted material. The sensitivity of the breach may mean that the full extent of this breach may never be publicly released and may be restricted to the international intelligence community.

[95] https://www.msn.com/en-us/news/politics/solarwinds-update-server-could-be-accessed-in-2019-using-password-solarwinds123-report/ar-BB1bXgXC

[96] https://www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html

Espionage and data theft are some of the motives behind the SolarWinds Hack, albeit the size and scope of the incident suggest that the threat acts might have had broader reasons, including the possibility of using the intelligence gathered to launch a cyber-attack. By injecting a hidden code into the SolarWinds' Orion software updates, the hackers could remotely access the networks and systems of SolarWinds' customers who downloaded the compromised software updates. This 'backdoor' gave the threat actors access to the systems of several thousand public and private organizations in the US and around the globe that use SolarWinds' products. Given that SolarWinds is widely employed by US federal government agencies and other key organizations worldwide, this incident appears to be an intelligence reconnaissance operation that offered threat actors a unique opportunity to spy on these organizations' systems and networks. For this reason, the SolarWinds attack is considered one of the most sophisticated cyber-attacks.

What Cyber Norms Apply?

- The most important norm violations are 1., the non interference of the public core of the internet and 8., offensive cyber operations by non-state actors.[97]

What Cyber Norms Could Have Been Helpful?

- **Attribution.** State level attribution followed rapidly. In January 2021, the US Biden administration attributed the hacking campaign to Russia's Foreign Intelligence Service (SVR). US Agencies, the FBI, CISA, ODNI, and the NSA characterized the SolarWinds incident as "an intelligence gathering effort" by "an Advanced Persistent Threat (APT) actor, likely Russian in origin"[98] The Washington Post attributed the attack to APT29(Cozy Bear).[99] After further investigation, the cybersecurity firm FireEye[100] also officially attributed the incident to Russian state affiliated actors. The full attribution came in April 2021, when the Biden Administration and the UK Government formally named Russia's Foreign Intelligence Service (SVR)– also known as APT29, Cozy Bear, and the Dukes – as the perpetrator of the SolarWinds cyber-attack[101]. Further investigation centered on the attackers' code Sunburst and its similarity to Casure, in its ability to calculate a unique victim ID. The nature of the signature was found to be connected to the APT29 and Zebra C campaigns, DLL and more recently as NOBELIUM.[102] Arguably, with numerous articles blaming cyber criminals, the initial attribution may not be quite so clear cut. Our interview with Kaspersky provided an important guide, suggesting that what is needed is a Geneva Convention for cyber security norms. In addition, as a supply chain attack, the breach's success was helped by its complexity.

[97] https://cyberstability.org/norms/#toggle-id-8
[98] https://www.justsecurity.org/75779/solarwinds-accountability-attribution-and-advancing-the-ball
[99] https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html
[100] How FireEye attributed the SolarWinds hacking campaign to Russian spies (cyberscoop.com)
[101] https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/
[102] https://thestack.technology/microsoft-customer-support-hacked-nobelium-apt29-solarwinds/

- **Financial sanctions.** In the aftermath of the SolarWinds hack, the Biden Administration signed the 'Executive Order Targeting the Harmful Foreign Activities of the Russian Government' in April 2021. The Executive Order aims to hold Russia accountable for the SolarWinds cyber-attack and signal that the US will impose costs on Russia if it keeps facilitating malicious activities in cyberspace against the US and its allies. As a result, the US Department of Treasury issued a directive prohibiting US financial institutions from purchasing bonds from Russia's Central Bank, National Wealth Fund, or the Ministry of Finance, and from lending funds to these institutions. Notably, the Executive Order also mentioned that the US Government might expand the sanctions on Russian sovereign debt as appropriate.
- **Company and personnel sanctions.** Additionally, the US Government would sanction six Russian technology companies that supported Russian SVR and 32 individuals involved in Russia's attempts to influence the 2020 US presidential election and other disinformation campaigns. Ten personnel from the Russian diplomatic mission in Washington, DC, were also expelled from the US. In retaliation, Russia asked 10 US diplomats to leave the country.
- **Implementing training.** Alongside the US Government's formal attribution of the SolarWinds hack to Russia, the US National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI) jointly published a Cybersecurity Advisory. This document described tactics and techniques used by the Russian SVR to exploit five publicly known vulnerabilities to target US and allied networks. Moreover, the US will promote the so-called "framework of responsible state behaviour in cyberspace" by offering a course to equip policymakers worldwide with "policy and technical aspects of publicly attributing cyber incidents". This course's first edition will take place this year at the George C. Marshall Centre, in Germany.
- **Implementing enhanced cybersecurity**. The SolarWinds attack also prompted President Biden to sign the "Executive Order on Improving the Nation's Cybersecurity" on May 12, 2021. This order: eliminates obstacles for private sector organizations to share cyber incident information with the government, requires the Federal Government to set the example, and implement robust cybersecurity standards (e.g., zero-trust architecture, encryption, multi factor authentication, and cloud security); enhances software supply chain security; creates a Cybersecurity Safety Board with representatives from the public and private sectors; creates a playbook for the Federal Government to respond to cyber incidents; aims to improve detection of cyber threats on Federal Government networks, and improves Federal Government investigation capability by requiring IT service providers of federal departments and agencies to collect and maintain information from network and system logs to facilitate the investigation of cyber incidents.
- **Implementing increased collaboration and policy at the level of nation states.** At the international level, following the US announcements about Russia's involvement in the SolarWinds hack, the European Union and its Member States and the North Atlantic Treaty Organization (NATO) stood in solidarity with the US. The EU and its Member States reinforced the importance of international efforts to establish a Programme of Action to Advance Responsible State Behaviour in Cyberspace within the United Nations (through the UN Group of Governmental Experts and Open-Ended Working Group). NATO also affirmed that Russia's actions

threatened Euro-Atlantic security and urged the country to cease its disrupting behaviour. This outcome of collaboration links closely with the immediate responses in implementing training and cyber security initiatives as above.

In conclusion, the effects of the Biden Administration's decision to formally attribute the SolarWinds attack to the Russian Government and impose sanctions will be closely watched. Yet, on balance sanctions may not be enough to discourage cyber criminal gangs from carrying out similar attacks in the future.

The US Government signalled that it could adopt more sanctions in the future. Commentators suggest that escalating tension between countries, particularly considering that cyber espionage is common among countries, including the US and its allies. In this context, the threshold of acceptable and unacceptable espionage practices in cyberspace is yet to be clarified. Many experts believe that the retaliations against the SolarWinds incidents was a proportionate response; both countries left the door open for dialogue. The first face-to-face summit between President Biden and President Putin took place in Geneva, Switzerland, in June 2021. Both countries showed interest in re-establishing US-Russian relationships and bringing ambassadors back to their posts in Moscow and Washington.

At the same time, rapid responses in policy development and implementation, including preventative training and improved cybersecurity together with increased collaboration among nation states and organizations point to a promising alternative avenue to punitive measures.

NSO Group’s Pegasus (2016--)

Since 2016 nation-state attackers have depended upon a privately-developed spyware called Pegasus to infect and monitor the devices of journalists, human rights defenders, politicians, activists and a range of others.[103] Pegasus was developed by NSO Group, an Israeli based company that is perhaps the most well-known of many in the private surveillance tech/spyware industry. Their success has led to a proliferation of sophisticated spyware and a “democratization” of access[104] - making such surveillance technology that was once available only to a few elite intelligence agencies now procurable by essentially any government with the desire to surveill.

While, according to NSO Group, Pegasus was built and sold as a tool for governments to help stop threats such as terrorism, and crime, including human trafficking,[105] it has been clear for some time that Pegasus has been used without respect for human rights and sold to non rights-respecting states. Reporting in the summer of 2021 by a consortium of investigative journalists revealed the scope of Pegasus’ sale to nation

[103] https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/
[104] https://www.occrp.org/en/the-pegasus-project/where-nso-group-came-from-and-why-its-just-the-tip-of-the-iceberg
[105] https://www.theguardian.com/news/2021/jul/18/response-from-nso-and-governments

states and the wide-ranging use of the tool.[106] Pegasus was sold to nation states including the UAE, Mexico, Saudi Arabia, Bahrain, Morocco, Hungary, Togo, Rwanda, India, Azerbaijan, Kazakhstan, and presumably others, and has targeted hundreds of people.[107]

Pegasus is noteworthy not only because it is a privately developed spyware exported and sold to nation-states for conducting surveillance (often unlawfully), but also because of its technical sophistication. The spyware allows for “zero click” exploits, a term referring to attacks that need no action on the part of the victim to succeed.[108] According to a security researcher we interviewed, the “development in exploitation technology and the way (these technologies) are being weaponized does not allow for any ability to challenge them.” According to that same researcher, “while in the past you could still address (vulnerabilities) at least on an operational security level….that is no longer possible, especially with the advent of these so-called ‘zero click’ vulnerabilities where there is literally nothing visible and nothing you’ve done wrong.” As the researcher stated, “it’s a completely asymmetric power imbalance, one that until very recently wasn’t even conceived in people’s minds as possible, especially on the side of those being targeted.”[109]

What Cyber Norms Apply?

- Two key norms from the UN 2015 GGE report aimed at promoting an open, secure, stable, accessible and peaceful ICT environment most clearly apply to this case. Those norms include recognizing the promotion, protection and enjoyment of human rights on the Internet (Norm E[110]), encouraging the responsible reporting of ICT vulnerabilities and sharing associated information on available remedies (Norm J[111]). In addition, the Global Commission on the Stability of Cyberspace’s proposed norm against offensive cyber operations by non-state actors is quite relevant - particularly given the role of private entities such as NSO Group in the spyware industry. According to this norm, “non-state actors should not engage in offensive cyber operations and state actors should prevent such activities and respond if they occur.”[112]

While potentially relevant, it would appear that these norms have as of now done very little to limit the presence and impact of Pegasus in particular, and targeted surveillance technologies more generally. Such is certainly true of the regulatory space as well. As the former UN Special Rapporteur on Freedom of Opinion and Expression David Kaye has noted: “It is insufficient to say that a comprehensive system for control and use of targeted surveillance technologies is broken. It hardly exists. While human rights law provides definite restrictions on the use of surveillance tools, States conduct unlawful surveillance without

[106] https://forbiddenstories.org/case/the-pegasus-project/
[107] https://docs.google.com/spreadsheets/d/1lUv-hoQWGZagZi-8DbX9bLiC_WUWpL-o3f7NRyZmA04/edit#gid=0
[108] https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/
[109] Author interview, October 26th, 2021.
[110] https://undocs.org/A/70/174
[111] https://undocs.org/A/70/174
[112] https://cyberstability.org/norms/#toggle-id-8

fear of legal consequence. The human rights law framework is in place, but a framework to enforce limitations is not."[113]

What Cyber Norms Could Have Been Helpful?

- **Enhance the norms for states to respect human rights, and expand this norm to apply to the private sector**. Even before the most recent, explosive revelations about Pegasus, it was clear to the now former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, that the private spyware industry was operating without much oversight or guidance, particularly when it came to human rights concerns. Kaye wrote in July 2019 that private surveillance companies had a responsibility "to respect freedom of expression, privacy and related human rights, and integrate human rights due diligence processes from the earliest stages of product development and throughout their operations."[114] More recently, Kaye has called for "genuine implementation of the UN Guiding Principles (on Business and Human Rights) and Human rights policies baked into company practice."[115] While expanding the norm on respecting human rights to the private sector could have been helpful, so too would an enhanced norm around respecting human rights for states. Ultimately, Pegasus was procured from the NSO group by states - some of whom participated in the 2015 UN GGE process that developed this norm. According to the former Special Rapporteur, "States that purchase or use surveillance technologies should ensure that domestic laws permit their use only in accordance with the human rights standards of legality, necessity and legitimacy of objectives, and establish oversight mechanisms."[116]
- Norms related to spyware exports and licensings. According to a security researcher who studied the impact of Pegasus, one of the most significant normative gaps relates to a lack of export and license controls. According to this researcher, prior efforts at license and export control[117] "have been a useful stepping stone, but evidently not sufficient to curb what has been a pretty wild industry".[118] In response to this issue, various actors have made concrete normative (and policy-based) recommendations. Civil society organizations have made strong calls for action in this space[119]. Former Special Rapporteur David Kaye has argued for normative enhancements, stating that "**states that export or permit the export of surveillance technologies should ensure a transparent process that solicits public input**, and exporting states should join the Wassenaar Arrangement, which should be updated to be consistent with human rights standards."[120] Kaye also argued in that same report that such states participating in Wassenaar should "develop a framework by which the licensing of any technology would be conditional upon a national human

[113] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Report: Surveillance and Human Rights*, 28 May 2019, UN Doc. A/HRC/41/35, para. 46
[114] https://undocs.org/A/HRC/41/35
[115] https://www.youtube.com/watch?v=yrP9vEH63HA
[116] https://undocs.org/A/HRC/41/35
[117] https://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/
[118] Author interview, October 26th, 2021.
[119] https://www.hrw.org/news/2021/09/08/eu-robustly-implement-new-export-rules-surveillance-tech#
[120] https://undocs.org/A/HRC/41/35

rights review and companies' compliance with the Guiding Principles on Business and Human Rights."[121]

- Expand and strengthen norms around vulnerability disclosure to the private sector. According to multiple security researchers and journalists interviewed, expanding Norm J of the UN 2015 GGE related to vulnerability disclosure to include technology companies such as device and operating system developers, if done responsibly and with proper considerations to the risks such disclosures can raise, could be very helpful.[122] [123]
- Norm around investment in rapid mitigation. According to one security researcher, one area of focus should be "raising the costs of exploiting the vulnerabilities successfully and introducing mitigations wherever possible. That's where I'd like to see more concrete investment, and ownership and responsibility. **[New mitigations] should not be sacrificed for economic or business reasons**, which unfortunately tends to be the case in some situations. From a technical standpoint, (it's important) to push companies to embrace the latest available mitigations even if that's an economic cost that doesn't seem favorable to a large customer base, but is vital to a small user base that are nevertheless customers of theirs… facing sophisticated threats from the likes of governments and corporates."[124] Perhaps a sign that this type of investment is starting to grow, Apple - whose iOS devices were among those targeted by Pegasus spyware - recently announced a pledge of at least $10 million dollars to support cybersecurity researchers. As part of that same announcement, Ivan Krstić, head of Apple Security Engineering and Architecture, emphasized the company's commitment to "analyze new threats, rapidly patch vulnerabilities, and develop industry-leading new protections in our software and silicon."[125]
- Norm around legal accountability for companies for misuse of their products. A lack of legal accountability, according to the aforementioned security researcher, is another limiting factor: "If there would be legal accountability for misuse of their (spyware developers') products that would be a deterrent for uncontrolled proliferation of this sort of (technology)." Despite some examples of past legal action against spyware company executives[126], legal accountability has been far from a norm.

What Cyber Norms Have Arisen As a Result?

- A few concrete actions have taken place from both state and non-state actors in response to the significant Pegasus revelations since the recent revelations in the summer of 2021, as well as to the use of private spyware stretching back years prior. While perhaps too regulatory in nature or too specific to be called norms, these actions offer a glimpse into what normative responses might develop in the future in response to Pegasus and the broader private spyware industry:

[121] https://undocs.org/A/HRC/41/35
[122] Author interview, October 19th, 2021.
[123] Author interview, October 26th, 2021.
[124] Author interview, October 26th, 2021.
[125] https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/
[126] https://www.technologyreview.com/2021/06/22/1026777/france-spyware-amesys-nexa-crimes-against-humanity-libya-egypt/

- The United States recently blacklisted NSO Group and, as a result, American companies are prohibited from selling technology to it or its subsidiaries.[127] Such a step is by far the strongest ever taken by one of the world's most impactful economic actors against a private spyware firm.
- Private companies including Apple and WhatsApp filed lawsuits against NSO Group. Both lawsuits focus on NSO Group's misuse of the plaintiffs' platforms and resources, in some cases explicitly against terms of service, to cause a wide range of damages in violation of US law (given that both companies are based in the United States.)[128] In the case of Apple's lawsuit, they seek "redress for Defendants' multiple violations of federal and state law arising out of their egregious, deliberate, and concerted efforts in 2021 to target and attack Apple customers, Apple products and servers and Apple through dangerous malware and spyware."[129] It is important to note that Apple's lawsuit emphasizes that while NSO Group did not breach data contained on Apple's servers, the abuse of Apple services and servers to perpetrate attacks on Apple's users and data stored on users' devices still constitutes a breach of law.[130] According to Ivan Krstić, head of Apple Security Engineering and Architecture, Apple's decision to bring this lawsuit "will send a clear message: In a free society, it is unacceptable to weaponize powerful state-sponsored spyware against those who seek to make the world a better place."[131]
- The Supreme Court of India ordered an inquiry into the Indian government's alleged use of Pegasus spyware against journalists and political opposition.[132] This is one of the first examples of potential domestic legal oversight and transparency related to the recent Pegasus revelations in a country that has been accused of using the spyware itself.
- Private entities have adopted strategic divestment from states revealed to have used Pegasus spyware for human rights abuses, as was the case with Cambridge University halting a 400 million Euro deal with the UAE.[133]

- It is also important to note that even before 2021, the existence of the private spyware industry has drawn considerable attention and led to many recommendations for global norms and regulations related to the industry. Perhaps the most succinct are those listed in the aforereferenced 2019 report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on Surveillance and Human Rights.[134] While recommendations such as these are still being debated and are not yet widely recognized or adopted, the revelations of 2021 have given them new attention and focus on the global stage.

[127] https://www.nytimes.com/2021/11/03/business/nso-group-spyware-blacklist.html
[128] https://www.apple.com/newsroom/pdfs/Apple_v_NSO_Complaint_112321.pdf
[129] https://www.apple.com/newsroom/pdfs/Apple_v_NSO_Complaint_112321.pdf
[130] https://www.apple.com/newsroom/pdfs/Apple_v_NSO_Complaint_112321.pdf
[131] https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/
[132] https://www.theguardian.com/news/2021/oct/27/indian-supreme-court-orders-inquiry-into-states-use-of-pegasus-spyware
[133] https://www.theguardian.com/education/2021/oct/14/cambridge-university-halts-400m-deal-with-uae-over-pegasus-spyware-claims
[134] https://undocs.org/A/HRC/41/35

Conclusions

In many ways, the cyber norms we have today would have helped mitigate many of the notorious cyber events of the past. However each analysis uncovers a missing nuance from deeper stakeholder involvement to application of existing legal frameworks.

Our findings

- In the case of the 1999 CIH virus, the government of Taiwan passed a cybercrime law while the private sector company Microsoft issued its first normative framework on trust in computing and software development.
- The shocking DDoS attacks against the nation state of Estonia in 2007 led to intergovernmental action in order to 1) clarify the application of existing international law to cyberspace in the Tallinn Manual as well as 2) provide a coherent cybersecurity strategy and intergovernmental cyber defense policy among NATO members.
- Similarly the use of NSO Group's Pegasus by nation states begs stronger application of existing international human rights law in addition to an expansion to include private sector responsibility.
- The GhostNet event of 2009 highlighted that cyber resilience should be a community-level concern that when addressed at the hyperlocal level, lends capacity to at-risk groups to shift into monitoring mode and can respond to the evolution of threats over time.
- The technical details of the Stuxnet worm mattered a great deal in debates about how to mitigate it and future "digital weapons". How it worked (without internet), what it did (hardware target), whether it was indiscriminate in its damage, as well as attribution questions all inform whether or not it fell in accordance with the legal principles of distinction and discrimination.
- Both the Snowden Disclosures and Heartbleed events highlight the need to ensure that the roles of journalist and whistleblower are directly considered in norm development to avoid inadvertent revelations of software vulnerabilities and to enable responsible oversight of intelligence operations.
- Heartbleed and the NSO Group's Pegasus events illustrate that cyber norms must promote a neutral status of and specific role for the technical community, incident responders, vulnerability analysts and independent security researchers as well as CERTs in identifying and mitigating cybersecurity events.
- NSO Group's Pegasus shows what can go right when the private sector, in this case Apple, takes action against the misuse of its hardware and software, demonstrating investment, and ownership and responsibility over its users, no matter how targeted or at-risk of attack.
- The SolarWinds breach resulted in increased levels of collaboration and the implementation of training and new cybersecurity initiatives by Governments and the UN; approaching what many stakeholders have formally and informally called for as an approximate "Geneva Convention for cyberspace."

- SolarWinds indicated additional outcomes on attribution and financial sanctions that may prove controversial and therefore require additional and thorough interrogation before fully fleshed adoption in norms packages.
- The Estonian DDoS attacks and the Aadhar data breach both targeted digital, nation state infrastructure designed to provide domestic social services, though they occurred 11 years apart. In the first case norms development at the intergovernmental level was sparked and systems redesigned. In the latter case only a domestic data protection policy appears to have been a direct result.

Future work

There is certainly more qualitative research that could be done to understand better the barriers and benefits to focussing on normative frameworks for those closest to cybersecurity incidents, past and present, in order to better mitigate future events. It is clear from the differential in depth of analysis between the events with desk research only versus those for which qualitative interviews were also conducted: the voices of those most affected by cybersecurity events provide key nuance not present in secondary source reports or tertiary source reporting.

Our distilled findings coalesce around two main themes. They point to a gap in understanding the roles of a wide variety of actors and stakeholders in mitigating cybersecurity incidents. And they show a persistent disclarity in the interplay of norms, policies and laws.

To bridge this gap, we recommend future research work that is focussed on understanding the interplay of cybersecurity norms and cybercrime legislation, where they overlap, align or work in opposition, with an aim to introduce greater stakeholder participation in the creation, enforcement and response mitigation as outlined in cybersecurity norms.