Henry Jackson Society

RESEARCH BRIEF

Centre on Cyber Security & Online Threats -

The SolarWinds Cyber Incident: Consequences & Policy Options

BY DR DANNY STEED

March 2021

Introduction

The SolarWinds cyber incident, reported in December 2020, marks a dark moment for cyber security through the compromise of the trusted update system. Much like the WannaCry and Not-Petya global ransomware attacks in 2017, SolarWinds signals yet another elevation of threat and vulnerability in cyberspace.

This policy briefing will examine what happened and the scale of the compromise, before outlining the six challenges it poses to British policymakers. The briefing will conclude with a series of domestic and international policy proposals to assist the British government in developing more substantive policies that do not focus exclusively on technology.

What happened?

On 8th December 2020, market-leading cyber security company FireEye announced that it had suffered a breach that resulted in the theft of numerous security tools, including highly prized ones used for penetration testing. Initially the main concern centred on how a major company - one that provides extensive cyber security products and services worldwide no less - had fallen prey to a security breach. It raised questions as to whether the tools used in the attack had proliferated to criminal and/or adversary state actors.

Had the attackers penetrated a company less sophisticated than FireEye, the SolarWinds breach might have been left completely undetected. Yet, it was their attack on FireEye that ensured the perpetrators' methods would be investigated by highly experienced specialists.[1] After looking through more than 50,000 lines of code, FireEye discovered that the backdoor was not there because of its own oversight, but was the result of using software called Orion from its trusted supplier, SolarWinds.

FireEye announced this unexpected finding on 13th December 2020,[2] describing the attacks as a 'widespread campaign' that extended far beyond FireEye: a 'highly evasive attacker' had leveraged the wider supply chain through SolarWinds. This global campaign used a backdoor named by FireEye as SUNBURST. Allegations were quickly levelled by American agencies towards Russian intelligence services, strongly suggesting they were the culprit.[3] They also claimed that the Russian intruders had been able to manipulate software updates for SolarWinds' popular Orion software (a network management product) at source and introduce a Trojan backdoor. The genuine update, with the Trojan embedded within it, was deployed by SolarWinds between March and June 2020 and subsequently downloaded by up to 18,000 corporate and government clients worldwide.[4]

The March to June release period represents an extremely long window of opportunity in which hackers could operate, meaning that global clients may have suffered some level of network compromise for up to nine months. FireEye further noted the sophistication of the backdoor, highlighting its initial dormant period of up to two weeks before executing commands. Those commands included the ability to:

- Transfer files
- Execute files
- Profile the system
- Reboot the machine
- Disable system services[5]

[1] *Turton, W. and Mehrotra, K., "FireEye Discovered SolarWinds Breach While Probing Own Hack", Bloomberg 15 December 2020, available at: https://www.bloomberg.com/news/articles/2020-12-15/fireeye-stumbled-across-solarwinds-breach-while-probing-own-hack, last visited: 30 January 2021.*

[2] *FireEye, "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor," FireEye, 13 December 2020, available at: https://www.fireeye.fr/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html, last visited: 30 January 2021.*

[3] *"Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA)", CISA, 5 January 2021, available at: https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure, last visited: 30 January 2021.*

[4] *Warrell, H., "SolarWinds Cyber Attack Linked to Tools Used by Russian Hacking Group", The Financial Times, 11 January 2021, available at: https://www.ft.com/content/e1b247d5-ef53-4e82-afc3-9e3c2d7c5e2c, last visited: 30 January 2021.*

[5] *FireEye, "Highly Evasive Attacker", 13 December 2020.*

The malware's ability to resolve a subdomain of avsvmcloud[.]com with a DNS response pointing to a Command and Control (C2) domain was also included among the multiple updates issued to the Trojan. In layman's terms, this type of malware can communicate outwards from a compromised network to facilitate hacker access from outside. This level of sophistication was only the beginning, the opening whence the attacker could exploit their new-found access to 18,000 clients or - as they had now become - targets.

What was the scale of the compromise?

The scale of the compromise must be contextualised in terms of client type as well as quantity; it was not just the number of clients, but the nature of the list of those affected. It reads like a Who's Who of American corporate, academic, and government entities, including: AT&T; Harvard University; Kennedy Space Center; Lockheed Martin; PWC; the US Air Force; The Economist; Symantec; Time Warner Cable; the New York Times; Booz Allen Hamilton, just to name a few.

There was also a near wholesale installation of the software across US Federal agencies, including the State Department and US Cyber Command. Even Microsoft confirmed on 31st December 2020 that it had been affected, noting that 'we discovered one account had been used to view source code in a number of source code repositories.'[6]

This is not to say definitively that each of the estimated 18,000 clients fell victim to malicious activity or had their networks penetrated. Given the almost immediate attribution of the breach to the Russian SVR foreign intelligence branch,[7] it is highly unlikely such a download was sufficiently resourced that every breach was accompanied by a full network exploitation. Instead, this novel method of intrusion was more likely part of a speculative attempt to gain access to a more refined target list.

Quality, not quantity, of access was the most likely objective yet the sheer number of potential victims is still alarming. It has confirmed longstanding concerns over the fragility of global supply chains. Indeed, the National Cyber Security Centre (NCSC) has long advanced this argument, and provided openly available guidance for supply chain security as far back as January 2018.

[6] *Microsoft, "Microsoft Internal Solorigate Investigation Update", Microsoft, 31 December 2020, available at: https://msrc-blog.microsoft.com/2020/12/31/microsoft-internal-solorigate-investigation-update/, last visited: 30 January 2021.*

[7] *Greenberg, A., "The SolarWinds Hackers Shared Tricks with a Notorious Russian Spy Group", Wired, 11 January 2021, available at: https://www.wired.com/story/solarwinds-russia-hackers-turla-malware/, last visited: 30 January 2021.*

The words of the NCSC are prophetic in this regard as they warned that 'very few UK businesses set minimum security standards for their suppliers'[8]

Why does SolarWinds matter?

For the Americans in particular this is the most significant cyber compromise since the Office of Personnel Management (OPM) hack in 2013, when security vetting files on federal employees dating back decades were stolen wholesale.[9] Most attribute the latter to the Chinese state and the FBI arrested a Chinese national involved.[10] Many of the same voices have emerged to condemn this incident in the strongest terms, attributing it to Russia. *Wired's* Lily Hay Newman declared 'Russia's campaign should serve as the final wake-up call.'[11] 'This is classic espionage', according to Professor Thomas Rid at John Hopkins University.[12] Robert Muggah at *Foreign Policy* added that the exploit 'is a reminder of the blurred lines between espionage and warfare, and the difficulty of formulating a proportionate response.'[13] It is of course, within these blurred lines that the Russian state has positioned itself over the past decade, as reflected in the wide, sometimes conflicting, array of terms, that try to articulate the blended and irregular nature of Russian aggression with terms such as "grey zone".[14]

The incident has also drawn strong comment from both politicians and practitioners. In the UK, former Home Secretary Amber Rudd has argued that the UK should urgently review its own security to recognise that '(t)his is the worst-ever US government cyberattack.'[15] While Rudd's analysis is flawed in that she is calling simply for more technology as the solution, her observation of the increased

[8] *NCSC, "Supply Chain Security Guidance", NCSC, 28 January 2018, available at: https://www.ncsc.gov.uk/collection/supply-chain-security, last visited: 30 January 2021.*

[9] *"The OPM Data Breach: How the Government Jeapordized our National Security for more than a Generation", US Committee on Oversight and Reform, 7 September 2016, available at: https://republicans-oversight.house.gov/report/opm-data-breach-government-jeopardized-national-security-generation/, last visited: 30 January 2021.*

[10] *Chalfant, M., " FBI Arrests Chinese National Linked to OPM Hack Malware", The Hill, 24 August 2017, available at: https://thehill.com/policy/cybersecurity/347897-fbi-arrests-chinese-national-linked-to-opm-hack-malware-report, last visited: 30 January 2021.*

[11] *Hay Newman, L., "Russia's Hacking Frenzy is a Reckoning", Wired, 16 December 2020, available at: https://www.wired.com/story/russia-hack-supply-chain-reckoning/#:~:text=This%20week%2C%20several%20major%20United,a%20months%2Dlong%20espionage%20operation, last visited: 30 January 2021.*

[12] *Thomas Rid quoted by Timberg, C. and Nakashima, E., "Russian Hack was 'Classic Espionage' with Stealthy, Targeted Tactics", The Washington Post, 14 December 2020, available at: https://www.washingtonpost.com/technology/2020/12/14/russia-hack-us-government/, last visited: 30 January 2021.*

[13] *Muggah, R., "Why the Latest Cyberattack was Different", Foreign Policy, 11 January 2021, available at: https://foreignpolicy.com/2021/01/11/cyberattack-hackers-russia-svr-gru-solarwinds-virus-internet/, last visited: 30 January 2021.*

[14] *JCN 2/18: Information Advantage, MoD, 18 September 2020, p. iii, available at: https://www.gov.uk/government/publications/information-advantage-jcn-218, last visited: 30 January 2021.*

[15] *Rudd, A., "Britain Must Improve its Cyber Defences Against New Threats", The Times, 19 January 2021, available at https://www.thetimes.co.uk/article/britain-must-improve-its-cyber-defences-against-new-threats-5f2f3sdhr, last visited: 30 January 2021.*

exploitation of cyber methods 'in geopolitical conflict' is very correct. Rudd echoed former GCHQ Director Robert Hannigan's earlier comments, namely that SolarWinds 'may turn out to be the most serious nation-state espionage campaign in history.'[16]

It is not just observers and former practitioners issuing bold statements on SolarWinds either, but big tech as well. Microsoft – before acknowledging it was itself affected – declared the incident 'a moment of reckoning' in a blog post from its president, Brad Smith. In an at times impassioned blog post, Smith called for 'a major step forward in the sharing and analysis of threat intelligence'; the strengthening of international rules 'to put reckless nation-state behaviour out of bounds'; and 'stronger steps to hold nation-states accountable' for such activities.[17]

There is a clear consensus from observers and commentators that SolarWinds 'is not "espionage as usual", even in the digital age',[18]. The nature and the scale of this incident represents another landmark in cyber security, as it underlines six realities in cyber security that must be recognised:

1. *A new level of compromise*

Cyber security incidents have become all too common and often follow an all too predictable pattern. Typically, a big name will suffer either some type of data breach, falling foul of numerous data protection statutes as a consequence. Or, they will fall victim to some strain of ransomware, being held hostage while their business operations are paralysed. Just two well-known examples include British Airways having their payment system subverted in 2018[19] – resulting in a revised £20 million fine[20] – to Sony having their most intimate business files released by North Korean state actors following the release of satire movie *The Interview*.[21]

When it comes to ransomware, the two headline examples are the NHS falling prey to the WannaCry variant in 2017, paralysing a full 35% of NHS Trusts.[22] This was followed a month later by the Not-Petya ransomware attack, which resulted in more than

[16] Hannigan, R., "SolarWinds Hack Exploited Weaknesses we Continue to Tolerate", The Financial Times, 20 December 2020, available at: https://www.ft.com/content/2bed3013-b21f-4b2c-8572-b2da016d1b4e, last visited: 30 January 2021.

[17] "A Moment of Reckoning: The Need for a Strong and Global Cybersecurity Response", Smith, B., – President, 17 December 2020, available at: https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/, last visited: 30 January 2021.

[18] Ibid.

[19] Hay Newman, L., "How Hackers Slipped by British Airways' Defences", Wired, 11 September 2018, available at: https://www.wired.com/story/british-airways-hack-details/, last visited: 30 January 2021.

[20] "British Airways Penalty Notice", ICO, 16 October 2020, available at: https://ico.org.uk/action-weve-taken/enforcement/british-airways/, last visited: 30 January 2021.

[21] VanDerWerff, E., and Lee, T.B., "The 2014 Sony Hacks, Explained", Vox, 3 June 2015, available at: https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea, last visited: 30 January 2021.

[22] Investigation: WannaCry Cyber Attack and the NHS, NAO (2017), available at: https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/, last visited: 30 January 2021.

$10 billion in global losses, with the global shipping company Maersk among the most affected victims.[23]

Unlike the now familiar headlines of the past decade, which have focussed on which corporation or government body had endured a cyber-compromise of some kind, SolarWinds represents a new level of breach. Accordingly, SolarWinds is not simply a story of which company has displayed its poor practices, or fallen foul of regulatory standards, or even just been unlucky in the face of pernicious cyber criminals.

Instead, SolarWinds needs to be recognised as a new type of compromise that affects not the cyber security of one – or even 18,000 – companies. This incident is one that puts the entire concept of cyber security in question. As Bruce Schneier has argued, 'the entire world is at risk'[24] through the specific targeting of the trusted update system upon which the global digital supply chain relies. Microsoft president Brad Smith mirrored Schneier's point when he stated: 'this is not an attack on specific targets, but on the trust and reliability of the world's critical infrastructure in order to advance one nation's intelligence agency.'[25]

SolarWinds is not just another corporate entity falling prey to cyber criminality. It is a harbinger of a new level of compromise, one that threatens the very trust we place in our ability to secure our systems.

2. *Trust is further fractured*

Trust is a crucial factor, and one that has been further fractured by the SolarWinds incident. The entire history of cyberspace, with reliance on universal protocols such as TCP/IP and DNS, has been built upon a shared trust that the underlying systems operate as designed. Numerous activities in recent decades have served to fracture this trust, but SolarWinds introduces a new reason to query it.

Questions may well be raised as to why many of those 18,000 clients who downloaded the infected Orion update – especially major corporations and government agencies – did not have some form of early warning system for compromises. This is especially so for the US government, which has diverted considerable funds towards

[23] Greenberg, A., "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/, last visited: 30 January 2021.

[24] Schneier, B., "The US Has Suffered a Massive Cyber Breach. It's Hard to Overstate How Bad It Is", *The Guardian*, 23 December 2020, available at: https://www.theguardian.com/commentisfree/2020/dec/23/cyber-attack-us-security-protocols, last visited: 30 January 2021.

[25] Smith, "A Moment of Reckoning", 17 December 2020.

its Einstein 3[26] intrusion detection system, which clearly failed in this case.

In this case, Einstein 3 proved unfit for purpose 'because it doesn't detect *new* sophisticated attacks.'[27] *Wired's* Lily Hay Newman has deployed the analogy of a nightclub bouncer to illustrate that a system like Einstein 3 is designed to keep out known names.[28] The analogy needs to be developed further, however, to illustrate just how far SolarWinds presents a new problem to trust.

Early warning systems, or other security measures like anti-virus, operate by building a list of known threats that are distributed, in order to prevent access - exactly as a bouncer would. The trouble with SolarWinds, however, is that they were on the trusted list. The Orion update did not slip any defensive safeguard because it was not recognised as a known threat; it was given access because it was recognised and seen as an update from a trusted source. In this analogy, the bouncer did not "turn a blind eye"; for 18,000 clients their respective bouncers all held the door open for the update and smiled as they let it in, recognising a trusted regular.

This is why trust has been severely fractured; the compromise of the software updating process itself as a means of mass deployment has created a new level of concern in the digital supply chain. Instead of trying to mitigate against phishing emails with malicious links and staff mistakes, this is now about preserving the integrity of the entire distribution system of software updates. The actions of a nation state here have proven that the global system itself can now be credibly threatened and successfully targeted.

3. *Our supply chain fears have been confirmed*

Commentators have warned for several years of the risks posed by supply chains across all industries, noting that they pose a wide array of risks. The ex-CEO of the NCSC, Professor Ciaran Martin, labelled it 'the hardest nut to crack'[29] because there is no globally recognised set of security standards for software and, consequently, no form of enforcement for standards either.

As a result, the market was left to its own devices, with the hope being that market innovation will generate the

[26]"Einstein 3 Accelerated", *CISA*, 19 April 2013, available at: https://www.cisa.gov/publication/einstein-3-accelerated, last visited: 30 January 2021.
[27] Schneier, "The US Has Suffered a Massive Cyber Breach", 23 December 2020.
[28] Hay Newman, "Russia's Hacking Frenzy is a Reckoning", 16 December 2020.

[29] Professor Ciaran Martin quoted by Murphy, H., "The Great Hack Attack: SolarWinds Breach Exposes Big Gaps in Cyber Security", *The Financial Times*, 18 December 2020, available at: https://www.ft.com/content/c13dbb51-907b-4db7-8347-30921ef931c2, last visited: 30 January 2021.

best-in-class standards spontaneously, without government or international regulatory intervention. For governments, supply chain fears are viewed in two ways. First, there is the fear of blunting the market competitiveness of our most successful businesses, resulting in theft of their intellectual property and gradual reduction of their market share. Second, there are national security concerns that government agencies are being infiltrated via their supply chains, in most cases for espionage. However, as Amber Rudd correctly pointed out, 'the exact same access will also lay the groundwork for disruption and sabotage operations.'[30]

SolarWinds represents a realisation of many of these fears Whether a perpetrator seeks to undermine our corporate economic competitiveness by carrying out large scale espionage operations or to lay the groundwork for acts of sabotage and warfighting operations against critical national infrastructure – SolarWinds now serves as the proof of concept for cyber operations that can successfully compromise the global digital supply chain.

4. *Technology alone is not the solution*

There is a dangerous tendency in cyber security to focus on market solutions to each and every technical vulnerability that appears. This has led to an explosion of market produced solutions of increasing complexity. From endpoint protection services, to AI-enabled threat detection, and from network monitoring services to cloud provisions with guaranteed secure enclaves, the list can appear endless.

By focussing on the range of possible solutions, one can forget that technology can only be part of, rather than the whole, solution to establishing cyber security. Government, too, has a large role to play in shaping the market environment through regulation, where necessary, and facilitating wide-ranging discussion of the issues at stake.

Consider someone purchasing a car; we trust not only that the vehicle meets basic regulatory standards for production and safety, but that the roads we operate the vehicle on have established rules and expectations of driver behaviour. The environment in which the vehicle operates must be governed to ensure an acceptable level of safety; but this is absent in cyberspace.

Instead, we have a market crowded with speculative, venture-backed start-ups who regularly make outlandish claims about yet another layer of technology ostensibly

[30] *Rudd, "Britain Must Improve", 19 January 2021.*

indispensable to securing the operations of every enterprise business and government department. Unsurprisingly, this then leads to government departments and businesses facing a mounting bill of countless security add-ons, creating an extremely complex digital estate (itself a recipe for insecurity), as well as disproportionate financial costs to providing an often false sense of security.

Interestingly, the strongest calls for bolder policy action to help ensure a safer cyberspace come not from the policy world, but from industry. In his aforementioned post, Brad Smith called for a coalition of governments and big tech firms and issued three actions to address systemic cyber security problems; yet, only one of the three is technologically focused.[31] The strengthening of international rules, and measures for holding nation-states directly accountable are political issues, requiring significant political investment to find solutions that ensure the stability of cyberspace.

Jody Westby, co-author of the UN publication *Quest for Cyber Peace*, remarked dryly that 'here we are…a dozen years after the Estonia attacks, with little progress toward a state of stability' for the use of cyberspace.[32] Even the UK's own National Cyber Security Strategy,[33] with its Chapter 4 on International Action, has seen precious little to zero progress since its publication in 2016 due to Brexit's dominance in the political debate.

A key conclusion should be apparent from the experiences of the 2010s: technology alone will not solve the policy problems that lie at the heart of cyber security. A concerted, long-term policy vision is needed to make headway in taming an environment that offers so much opportunity to criminality and malevolent geopolitical behaviour.

5. Intelligence operations increasingly blur the boundaries

SolarWinds has exposed in Russian intelligence operations what the illegal Snowden disclosures did of Anglo-American intelligence operations in 2013. In the words of former National Security Agency (NSA) director Michael Hayden, in 2013 Western intelligence services were "playing to the edge" of the rules,[34] much like elite athletes pushing the boundaries and

[31] *Smith, "A Moment of Reckoning", 17 December 2020.*

[32] *Westby, J., "Russia has Carried out 20-Years of Cyber Attacks that call for International Response", Forbes, 20 December 2020, available at: https://www.forbes.com/sites/jodywestby/2020/12/20/russia-has-carried-out-20-years-of-cyber-attacks-that-call-for-international-response/, last visited: 30 January 2021.*

[33] *"National Cyber Security Strategy 2016 to 2021", The Cabinet Office (2016), Ch. 4. Available at: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021, last visited: 30 January 2021.*

[34] *Hayden, M. V., Playing to the Edge: American Intelligence in the Age of Terror (New York: Penguin Press, 2016), foreword.*

interpretations of the permissible to their limit. In the case of SolarWinds, Russian intelligence operations clearly recognise no lines, flout norms, and are operating beyond the already poorly established rules of acceptable behaviour. In short, they have no qualms putting the global architecture of trusted software updates at risk to pursue their own interests.

Intelligence operations have revealed themselves to be the biggest area of concern for long-term cyber security practices. In contrast to cyber criminality, which predominantly exploits user behaviour rather than any technical innovations, intelligence operations have proven themselves willing and able to compromise entire global networks, causing disproportionate harm. SolarWinds is the latest example, and perhaps the most concerning, of an intelligence actor executing an untargeted strategy by means of compromising the system of trust in software upgrades.

A key question faces the governments of Western liberal democracies: how to establish rules and laws of acceptable behaviour in the face of Russian activities with SolarWinds? This is no recent revelation, with British efforts dating back to the days when William Hague was the Foreign Secretary,[35] but it certainly remains unresolved.

Notwithstanding the arguments about Edward Snowden's motivations, one thing that is clear was his impact on public debate and how the rules were changed by the state. In the UK, wholesale legislative updates were catalysed; it is no exaggeration to say that had it not been for Snowden there would never have been demand for the Investigatory Powers Act, 2016. Domestically at the time, the British government recognised the need to update the rules by which intelligence services operated. This is reflected in the continuing evolution of British statute governing the intelligence services, with the Official Secrets Act next in line for overhaul, following sharp criticism from the Intelligence and Security Committee's *Russia Report* in July 2020.[36]

However, such rules need to be established internationally. While it is clear that international law permits espionage *per se* – as declared in the much vaunted Tallinn Manual on international law and cyberspace[37] – that should not be free licence to threaten the safety of cyberspace for all.

[35] *Hague, W., "Speech: Security and Freedom in the Cyber Age – Seeking the Rules of the Road", Gov.uk, 4 February 2011, available at: https://www.gov.uk/government/speeches/security-and-freedom-in-the-cyber-age-seeking-the-rules-of-the-road, last visited: 30 January 2021.*

[36] *"Russia Report", ISC, 21 July 2020, available at: http://isc.independent.gov.uk/news-archive/21july2020, last visited: 30 January 2021.*

[37] *Schmitt, M. N. (Ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge: CUP, 2017).*

Intelligence operations increasingly blur the lines of acceptable conduct, by demonstrating what is possible in the pursuit of geopolitical objectives through cyberspace. Traditionally, espionage was permitted in the spirit of being a "steam valve" in the international order, carrying out activities to prevent escalation from ever occurring. Today, by contrast, espionage paired with cyberspace may soon find itself a highway to escalation if left unchecked by its political masters.

6. *Cyber is now a central tool in geopolitics*

Cyber criminality is a given, and has been for many years. Ransomware regularly tops surveys of corporate fears, and is responsible for huge financial losses. What Western governments have been slow to recognise, however, is the increasing centrality of cyberspace in the pursuit of geopolitical objectives.

Campaigns such as SolarWinds should not be seen as aberrations, but the latest in a series of concerted efforts by adversarial nation-states to pursue their objectives against Western interests. When assessing the Russian playbook, SolarWinds appears much in the same strategic vein as Moonlight Maze from the 1990s, which extensively targeted sensitive American research institutes.[38] In contrast, Chinese state hackers through their Cloud Hopper campaigns compromised eight global IT service providers in order to target end users - corporations such as Fujitsu, NTT Data and IBM – for the purposes of industrial espionage.[39]

The deliberate ambiguities present in international law, useful for so long in enabling flexible policy options, are also a liability due to their cynical exploitation by authoritarian states. These actors empower their intelligence services to use cyber tools and deliberately exploit international legal ambiguities to pursue geopolitical interests. This is a geopolitical battle ground that Western governments are reticent to admit is even taking place, and even slower still to take tangible action to redress.

Like it or loathe it, cyberspace is now central to 21st century geopolitics. Nation-states who are adversarial to any notion of the current rules-based international order have and continue to mercilessly exploit cyberspace to target Western states and economies. This author has previously argued the

[38] *See Thomas Rid's presentation to the Kaspersky Security Analyst Summit 26 April /2016, available at: https://www.youtube.com/watch?v=zSrjkWDXSS8, last visited: 30 January 2021.*

[39] *Stubbs, J., Menn, J., and Bing, C., "Inside the West's Failed Fight Against China's 'Cloud Hopper' Hackers", Reuters, 26 June 2019, available at: https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/, last visited: 30 January 2021.*

case for cyberspace now being a decisive geopolitical arena this century.[40] This is a reality all Western governments must accept and prepare themselves to act accordingly.

suffers from minimal use, especially in the SME market.

What can UK policy do?

There are a range of policy options open in response to SolarWinds. Domestically, the UK can initiate basic tangible measures as well as longer term statutory changes.

Drop the price for Cyber Essentials and Cyber Essentials Plus

First, to help incentivise UK businesses to improve their cyber security measures, the price of national schemes such as Cyber Essentials and Cyber Essentials Plus must be radically decreased.

The cost of these schemes – now requiring annual renewal – are prohibitive in particular to SMEs. This ultimately acts as a deterrent to companies investing in certification, preferring instead to gamble on the punitive fine structure of GDPR, which companies understand much better. Reducing the costs of these schemes by at least half will surely result in far greater take up of a scheme that

Strengthen the Official Secrets Act (OSA)

The UK needs to become a more hostile environment for foreign espionage operations. The *Russia Report's* findings notwithstanding, statutory measures preventing the operation of espionage in the UK must not fall prey to a literal physical interpretation; they must also recognise cyber-attacks that begin from overseas.

An act of cyberespionage against UK-based infrastructure, corporate entities, and government agencies should be viewed in the same way as an act of more traditional espionage. Discussions to revise the OSA must include a strong component on how to handle digitally executed espionage, and establish a statutory opinion to guide law enforcement and intelligence services.

Whatever learning takes place from the fallout of SolarWinds, it is important that policy approaches adapt accordingly. Immediate actions

[40] *Steed, D., The Politics and Technology of Cyberspace (Abingdon: Routledge, 2019), p. 98.*

to adapt will include cyber espionage within any scope of reference for revising the OSA.

Institute supply chain standards with regulators

While there remain no accepted international standards, with different industries possessing different requirements, there is scope for UK regulators to create a UK framework for supply chains. Whether one refers to OFCOM, the FSA, CQC, the Law Society, ICO, CAA, or the ONR - among others – we are able to establish significant and industry-tailored standards.

As an example, the Ministry of Defence (MoD) alongside British Aerospace (BAE) operates the Defence Protection Partnership Cyber Security Model, with the purpose of reducing supply chain risks. The central requirement of all MoD suppliers is to attain at least Cyber Essentials before being eligible for contract awards.

Some industries in the UK already take proactive measures to harden supply chains. Regulators, operating with government guidance, can make great strides in helping UK industries move towards the right levels of acceptable cyber security certification.

Openly acknowledge our cyber adversaries

The last iteration of the National Cyber Security Strategy focused overwhelmingly on resilience. This is a necessary, but not sufficient, condition for cyber security. Any strategy relying only on resilience is inherently reactive, accepting an increasingly anarchic environment in cyberspace without taking action to shape that same environment for increased safety.

That insular perspective of the NCSS has enabled, arguably even emboldened, nation state adversaries in their use of increasingly aggressive cyber methods. The next NCSS must openly acknowledge the adversarial geopolitical contest taking place in cyberspace, and call out the key threat to the vision of a free and open internet. That threat is the concept of Cyber Sovereignty, with its main patrons, Russia and China.

This is not to declare these nations as enemies, but to declare their vision of cyberspace as being contrary to our own. The political vision of Cyber Sovereignty opposes democratic values, undermines a free and open Internet, and needs challenging; this is a reality that needs to be explicitly recognised in our national strategy.

Incentivise corporate participation in international standards

Internet governance has no single governing body. Instead, a multiverse of bodies exists to safeguard the many technical standards on which cyberspace's operation depends. To ensure adequate representation, the UK government should convene a standing group whose task is to incentivise and coordinate corporate and technical participation in these bodies.

Such participation has mostly been voluntary, based on the good will of those seeking to ensure the stable operation of cyberspace. It is time to professionally structure a process that ensures full UK representation from private business, academia, and government to shape internet governance.

Any such working group could easily benefit from NCSC participation and liaise with stakeholder government departments. The centrality of cyberspace to all industries makes such a task an inherently cross-departmental and trans-industrial venture.

A diplomatic surge at the UN's Government Group of Experts (GGE) on cyber (and beyond)

For too long, it has been beneficial to authoritarian nations to paralyse the GGE working group on advancing responsible state behaviour in cyberspace.[41] As the leader of the US delegation to the GGE, Michele Markoff, stated, some nations believe that they 'are free to act in or through cyberspace [...] with no limits or constraints on their actions [...] This is a dangerous and unsupportable view.'[42]

With Brexit complete, the time is ripe for British thought leadership to engage the diplomatic arena on cyberspace, building on existing structure like the UN GGE; any vision for Global Britain should include a leadership effort to make cyberspace a safer place for all, based on liberal values. There is an opportunity for Britain to become a diplomatic leader in cyber security efforts and it should be taken as quickly as possible.

[41] *Grigsby, A., "The Year in Review: The Death of the UN GGE Process?" CFR, 21 December 2017, available at https://www.cfr.org/blog/year-review-death-un-gge-process -:~:text=The%20Year%20in%20Review:%20The%20Death%20of%20the,Guest%20Blogger%20for%20Net%20Politics%20December%2021,%202017, last visited: 26 February 2021.*

[42] *Michele Markoff quoted in Bowcott, O., "Dispute Along Cold War Lines Leads to Collapse of UN Cyberwarfare Talks", The Guardian, 23 August 2017, available at https://www.theguardian.com/world/2017/aug/23/un-cyberwarfare-negotiations-collapsed-in-june-it-emerges, last visited: 26 February 2021.*

Conclusion

To conclude, the SolarWinds incident has realised some of the deepest fears of the cyber security community. By proving the global digital supply chain can be put at risk and successfully targeted, it is clear that the problem of cyber *in*security goes far beyond matters of technology. It is also a fundamentally political problem about geopolitical rivalry and the behaviour of actors in the international system.

The UK has a choice in its response to the SolarWinds: it can be narrow-minded and treat it as one in a long line of cyber security incidents with limited results, sticking to a reactionary approach. Or, Britain can start thinking beyond the technology alone, and begin to craft both short term domestic and long term international policy responses that help shape the free and open cyberspace for the benefit of all.