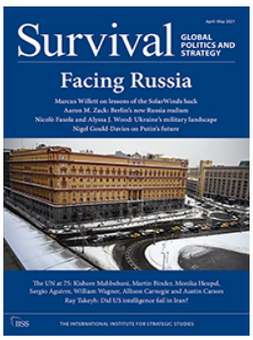


Routledge
Taylor & Francis Group

Survival
Global Politics and Strategy

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/tsur20

# Lessons of the SolarWinds Hack

Marcus Willett

**To cite this article:** Marcus Willett (2021) Lessons of the SolarWinds Hack, Survival, 63:2, 7-26, DOI: 10.1080/00396338.2021.1906001

**To link to this article:** https://doi.org/10.1080/00396338.2021.1906001

# Lessons of the SolarWinds Hack

**Marcus Willett**

In late 2020, the American cyber-security community discovered a widespread breach of private-sector and government networks. A primary vector for the breach appeared to be the hacking of software provided by the US information-technology company SolarWinds. The United States government identified the likely perpetrator as a Russian intelligence agency. Ever since, complex and painstaking technical investigations have been under way into the precise nature and extent of the breach. At the same time, debate has raged about the intent behind the hack and the implications for the cyber policies of the US, and states in general, including whether some form of retaliation is justified. This article examines issues raised by the SolarWinds hack with respect to the cyber-security, offensive-cyber and broader national-security policies of the US and its allies.

## What we know

The story first broke when FireEye, a top US cyber-security company involved in many major investigations and responsible for publicly identifying the perpetrators of numerous attacks (including the Russian intelligence services), announced in December 2020 that it had been hacked by a state with 'top tier' capabilities. Its own 'red-team' tools – developed by FireEye to test client defences based on previously detected capabilities – had been

**Marcus Willett** is IISS Senior Adviser for Cyber. During his previous career in GCHQ, he helped design UK cyber strategy, and initiated and led a number of national cyber programmes.

**Survival** | vol. 63 no. 2 | April–May 2021 | pp. 7–26 https://doi.org/10.1080/00396338.2021.1906001

accessed. FireEye further discovered that the vector used by the hackers was the IT company SolarWinds and that there were many other victims.

SolarWinds is a Texas-based company that supports its clients by supplying software called Orion to monitor and manage IT networks, including by aggregating, analysing and visualising large amounts of data. Investigations following FireEye's initial discovery showed that the hackers had infected SolarWinds' Orion software as early as October 2019, allowing them to use a routine software security update from SolarWinds in March 2020 to install malicious software in the company's clients' networks. The hackers may have taken advantage of lax security practices to penetrate SolarWinds in the first instance and, by hiding within that security update, evaded the clients' cyber-security defences. In that sense, it was an ingenious attack, with Microsoft suggesting that it might have taken '1,000 very skilled, very capable engineers' to design and execute it.[1] According to SolarWinds, 18,000 of its clients downloaded the infected software.

In February 2021, while acknowledging that the full extent of the breach was still under investigation, the US government stated that, as a result of a 'broad and indiscriminate effort', the hackers had gained access to the data and emails of at least nine US federal agencies, including the Department of the Treasury and the Department of Justice, and about 100 private companies.[2] These companies included major digital-technology outfits such as Cisco, Intel, Nvidia and Microsoft, as well as cyber-security companies like FireEye. There were also indications that the hackers may have hidden inside US cloud services (such as Microsoft's and Amazon's) to further exploit the results of their initial hack. As of mid-February, cyber-security experts also discovered that 30% of the identified victims of the hack had no direct connection with SolarWinds itself, with the possibility therefore remaining that SolarWinds was not the hackers' only initial launch point. Nevertheless, the infection has become widely known as the 'SolarWinds hack'.[3]

The US government attributed the hack to an 'advanced, persistent threat actor likely of Russian origin', meaning a Russian intelligence agency.[4] Some in the US have described it as one of the most significant attacks ever carried out against the US, arguably an act of war.[5] The extent to which it may have spread to other countries is unclear. Although experts believe the hack had a

US focus, clients of SolarWinds in Canada, Mexico, Europe, the Middle East and elsewhere may also have downloaded the infected software.

Given that the investigations are still under way, a great deal remains unknown about the hack. The information thus far publicly released about how the hack was detected may not tell the full story. It cannot be ruled out that secret US capabilities played a role behind the scenes. The use of sensitive government intelligence capabilities can be concealed behind other, less sensitive means of detection and attribution. Furthermore, classic counter-espionage operations can involve letting hostile activity continue and observing it to find out more, before potentially subverting it or revealing its detection. It is unclear whether there is sufficient coordination between private cyber-security companies and government agencies in the US to ensure that the right strategic decisions can be made about how and when to publicly reveal knowledge of such compromises.

In early March, the US revealed that further large-scale breaches unrelated to the Russian SolarWinds hack had been discovered. Attributed by Microsoft to a state-sponsored Chinese group and exploiting vulnerabilities in Microsoft's email servers, this new hack had apparently infected up to 30,000 public and private entities, mainly small businesses and local government. Other state and non-state cyber actors may have begun trying to exploit the initial hack in a race to beat installation of patches provided by Microsoft. Some speculated that this Chinese attack could turn out to be even more widespread than the Russian SolarWinds one. While the Chinese activity is not specifically analysed here, it is likely to have many of the same implications for US policy.

## The hackers' intent

Although the SolarWinds hack has been labelled a cyber 'attack', initial analysis indicates that it was intended not to damage, disrupt or destroy networks, but rather to gain intelligence. Known as a 'supply-chain operation' since it used suppliers of IT services to get inside their clients' networks, and using clever techniques to evade detection, the SolarWinds hack appeared designed to infect multiple networks to gain broad access to potentially interesting data and emails. Thus, it does not appear to have the hallmarks

of being targeted, surgical espionage. Furthermore, there seems to be no evidence thus far that it infected classified US networks. In that regard, it is not as serious as a widely reported Russian hack in 2008, which used an infected USB stick to leap the air gap onto US Department of Defense classified networks. Overall, therefore, the SolarWinds hack looks like an intelligence 'fishing trip' or reconnaissance operation unleashed on open networks, similar in intent to many other state cyber operations, such as the Chinese hack of the US Office of Personnel Management that occurred from 2013 to 2015.

It is perhaps equally instructive to compare the SolarWinds hack with a 2017 Russian operation that used malware called 'NotPetya' to target networks in Ukraine. NotPetya was a 'worm': self-replicating malware that spreads through networks in a fundamentally uncontrolled way. The SolarWinds hack was also designed to gain an initial presence on a large number of networks. Strictly speaking, though, it was not a worm, with the Russians appearing to retain sufficient control to be able to deactivate selected operations. Both were supply-chain operations, with NotPetya delivered via a back door in an automatic update to some popular Ukrainian tax-preparation software supplied by the company Intellect Services. But NotPetya appeared specifically designed to infect Ukraine's critical national infrastructure (its energy companies, power grid, transport sector and banks) and to damage devices rather than just collect intelligence. This highlights the difference between a large-scale offensive cyber attack, like NotPetya, and large-scale cyber espionage, like the SolarWinds hack.

There are other potentially relevant differences between the two operations. While the use of the tax software as the vector for the NotPetya attack clearly targeted Ukraine, the operation also made some use of a leaked tool developed by the US National Security Agency and sold for auction by the mysterious 'Shadow Brokers' group in April 2017. The tool exploited a widespread vulnerability in a Microsoft Windows protocol, which allowed hackers to remotely run code on unpatched machines. The Russian use of a worm in combination with such a widespread IT vulnerability meant that an attack targeting Ukrainian critical infrastructure infected many unintended networks the world over, including those used by the Danish shipping line Maersk

and the US delivery company FedEx. An alternative interpretation of the SolarWinds hack is that, among the many unintended victims, the Russians likewise had specific targets in mind. For example, given that they accessed FireEye's red-team hacking tools, one aim could have been to penetrate the US cyber-security community or US cloud-service providers to bolster Russia's own arsenal of offensive tools, and to develop new supply-chain opportunities for potentially even more valuable operations in the future.

Whether intended as broad-gauge reconnaissance or with specific targets in mind, the result of the SolarWinds hack is that the Russians are present on a range of US governmental networks and, potentially, parts of the United States' critical national infrastructure. While the intent seems to have been to gather intelligence, the operations could be technically repurposed by the Russians at a time of their choosing to deliver a destructive effect. Their operations could also be hijacked by others with hostile intent, or could malfunction, causing an unintended accident. Furthermore, with such reconnaissance operations by states occurring every day in cyberspace, any one of them could be misinterpreted by the victim as an actual attack. Ultimately, though, it is the broad vulnerability caused to a state by an attack like the SolarWinds hack, regardless of intent and the actual damage that results, that could lead that state to conclude that a penetration of its networks went unacceptably beyond the routine daily attrition of state-on-state cyber operations and therefore called for retaliation. Broader escalation could easily follow. As Microsoft president Brad Smith put it, the SolarWinds operation is like a 'burglar who wants to break into a single apartment but manages to turn off the alarm systems for every home and every building in the entire city. Everybody's safety is put at risk.'[6] Such considerations raise the question of how the US might legitimately be able to respond if it were to discover that the Russians had penetrated, say, its power grids, irrespective of original intent.

## How to respond

US private-sector companies have detected and are disrupting a large-scale Russian cyber-espionage operation. There is plenty of evidence in material leaked from the US government that the US engages in similar

cyber-espionage operations, including using supply chains. So we should not conclude that Russia is in any way the master of the internet, or that it outclasses the US at cyber operations. Far from it – Russia is so worried about what it has learned about US and allied cyber capabilities from US intelligence leaks (especially Edward Snowden's) and by US commercial dominance of internet technology (exemplified by US pressure on the Chinese IT company Huawei) that the Russian government is seeking ways to isolate Russia physically from the global internet, despite the economic and social disadvantages of doing so.[7] Like China, Russia seems to recognise serious deficiencies in its own cyber security, with its low ranking in the relevant international cyber-security indices an indicator.[8]

*SolarWinds was not an act of war*

Given that the SolarWinds hack therefore appears to constitute reconnaissance and espionage of the sort that the US itself excels at, it is neither accurate nor sensible for US commentators to characterise it as an act of war requiring warlike retaliation.[9] If using spy planes, satellites and double agents to gather intelligence from inside the Soviet Union was normal business during the Cold War, the same is true of an operation like SolarWinds in the digital age.[10] The US would not have invoked Article V of the North Atlantic Treaty if it thought an adversary might have been able to blow up the Twin Towers on account of having hacked the power supply, for example; it invoked Article V because of the death and destruction caused by an actual attack.

The US did agree to a bilateral treaty with China in 2015 intended to limit cyber-espionage operations, but it was designed specifically to put large-scale commercial espionage off limits, not to stop other types of cyber espionage. Attempts to steal state secrets in peacetime are internationally tolerated because, among other things, they can reduce the chance of a misunderstanding that could lead to a real conflict. Broadly accepted retaliatory protocols for such activities have developed over time. When a state is caught spying in the physical (as opposed to virtual) world, the result is normally a tit-for-tat expulsion of diplomats and intelligence officers, nothing more.

More could be done to develop equivalent protocols for cyber espionage. One tactic employed by the US and its allies over the last five years has been to work together to publicly name individual perpetrators of cyber attacks. In some cases, the US has also indicted them, effectively barring them from travelling to relevant jurisdictions, with an eye to deterring similar conduct in future. These remedies demonstrate the ability of democratic governments not only to detect and attribute attacks, but also to operate in close alliance, with extensive sharing of cyber intelligence and, in some cases, integrated capabilities.[11] China, Iran, North Korea and Russia have nothing equivalent.

Internationally agreed protocols are also useful. One of the original 11 cyber norms of behaviour agreed under the auspices of the United Nations in 2015 encourages states to consider all relevant information, including the wider context and the nature and extent of the consequence of any cyber intrusion, before reacting.[12] The same norm, however, implies that it is difficult to attribute cyber operations, which might encourage some states to execute operations in the belief that they can avoid blame. Such a rationale seriously misconceives the nature of attribution.[13] Cyber-capable states have for some time been able to confidently identify perpetrators of attacks, though they have often hesitated to make those attributions public due to worries about protecting sensitive intelligence sources and methods. As cyber-security ecosystems have matured, particularly in terms of private-sector intelligence gathering and cooperation between governments and companies, the public attribution of cyber operations has become more commonplace. SolarWinds is a case in point, clearly signalling that, once detected, state cyber operations are likely to be firmly attributed.

Of course, the 11 original cyber norms of behaviour agreed in 2015, and those added subsequently by the Global Commission on the Stability of Cyberspace and other bodies, are voluntary and non-binding, and include various national-security exceptions. They are honoured more in the breach than in the observance, and are not enforceable. For example, one of the original 11 holds that states should take responsible steps to ensure the integrity of the supply chain for information- and communication-technology (ICT) products by seeking to prevent the proliferation of malicious ICT tools and

techniques, and the use of 'hidden functions'. The NotPetya and SolarWinds hacks, as well as the US espionage operations exposed by Snowden and the Shadow Brokers, clearly contravene this guideline. Another norm advises that states should not intentionally damage or impair the use and operation of critical infrastructure, which the Russians did with NotPetya though not, it would seem, with SolarWinds.

Such guidelines need to be more tightly and realistically framed. For example, states will inevitably consider a potential adversary's critical networks a legitimate wartime target, and need to gain a technical presence on such networks during peacetime to prepare for that eventuality. There is little point in pretending that they won't try to do so. Also, the term 'critical national infrastructure' is too open to interpretation. Accordingly, it would be useful to establish a norm of behaviour that specifically identifies those networks that no nation should consider sensible to target for reconnaissance, espionage or attack in war or peace. Examples include hospitals, emergency services and nuclear command-and-control systems. Rather than unrealistically attempting to exclude an array of other aspects of 'critical infrastructure', an overarching norm of behaviour could broadly define as unacceptable the reckless use of indiscriminate techniques likely to undermine the day-to-day use of the internet by unintended victims. Given the potentially dangerous nature of their effects, the careless protection and reckless use of such capabilities would then deserve the same sort of international opprobrium given to carpet bombing, cluster munitions and chemical weapons. In the wake of the SolarWinds hack, President Joseph Biden has specifically highlighted the 'recklessness' of Russian behaviour and made cyber diplomacy and international cyber norms foreign-policy priorities. It would also help if the US community ceased labelling the SolarWinds hack 'sophisticated' – it is technically far more challenging to be surgical than to be indiscriminate – and instead reserved that description for attacks that so qualify.

Legal and diplomatic clarifications are required to give such voluntary norms sufficient teeth. In particular, states should be pressed to acknowledge that existing international law applies to cyber operations, emphasising that it is the effect rather than the specific means of a hostile operation that

matters from a legal standpoint. In turn, states could agree on penalties that could be imposed on states caught behaving recklessly and imperilling the general safety of populations during peacetime, making clear that mere indignation over an operation's technical audacity and success – à la SolarWinds – would not trigger such penalties. These could range from exclusions from international forums to diplomatic expulsions to economic reprisals. Of note, work is under way at the International Committee of the Red Cross to better define the responsible use of cyber capabilities, including how international humanitarian law applies to cyber operations.

## Implications for cyber security

Perhaps most importantly, the SolarWinds hack should focus attention on what adjustments are needed to the internal cyber-security strategies and capabilities of the US and its allies. This has been the central concern of expert testimony to the US Congress, which has called for increasing the powers of and funding for the US Cybersecurity and Infrastructure Security Agency (CISA); improving coordination between the US government and the corporate sector; grants to state and local government to enhance their cyber security; and accelerating IT modernisation across the federal government. Notably, most experts are not suggesting that all networks can be technically shielded from all attacks, or advocating that increased investment should be reserved solely for more and bigger technical solutions.

To be sure, protecting networks remains crucial for preventing the vast majority of attacks, especially those conducted by cyber criminals. The rapid growth in the criminal use of ransomware – whereby an organisation's data is encrypted and held to ransom – is arguably more strategically damaging than state cyber-spying. Ransomware attacks increased by approximately 40% during 2020 compared with 2019, as perpetrators took advantage of the COVID-19 pandemic, with the average payout more than doubling.[14] Criminals have also shifted towards soft targets, prioritising poorly defended sectors such as education, health and local government, as well as smaller companies. Even before the recent hike in ransomware attacks, the overall global loss to financially motivated cyber crime has been assessed to be 1–2% of global GDP.[15]

It would therefore be a mistake to let concerns about a complex state attack like the SolarWinds hack obfuscate the need for a concerted effort across all sectors to improve basic cyber hygiene.[16] The majority of cyber-criminal capabilities are not as sophisticated as those available to cyber-capable states, and do not involve the level of ingenuity employed in the SolarWinds hack. Instead, they rely on lapses in fundamental protections, as indeed do most state attacks. Many exploit human weakness: poor password discipline, poor awareness and training (particularly against phishing), failure to keep the routine patching of software up to date and failure to audit. Reinforcing basic cyber hygiene with new laws establishing disincentives to pay ransoms to cyber criminals – it is currently too convenient for companies simply to use their insurance to pay up – and stronger incentives for companies to report all breaches would make sense. Organisations that implement basic cyber hygiene can stop 90% of potential breaches.

Good cyber hygiene is part of a 'whole of society' approach to cyber security. This is, appropriately, the declared aim of cyber-capable democracies and requires central government to facilitate close public–private collaboration, develop appropriate upskilling and educational schemes, and heighten public awareness. For the US and some of its key allies, this approach is underpinned by a burgeoning cyber-security industrial sector, capable of detecting, attributing and preventing sophisticated hacks. In liberal democracies, where for good reason there are extensive restrictions on the ability of the intelligence community to monitor private networks (including those providing the cloud services that appeared to feature in the SolarWinds hack), this young industry has become a fundamental element of the overall cyber-security ecosystem. Russia and China have nothing of an equivalent scale, and therefore often try to copy Western technical cyber-security solutions. Notwithstanding SolarWinds, it would be a mistake to lose confidence in the cyber-security industry and the suppliers of secure IT solutions in general (including cloud providers), and certainly nobody would advocate increasing the government's internal surveillance powers. The fact that the US private sector detected and disrupted a complex Russian espionage operation is evidence that the liberal-democratic cyber-security model works.

That said, the US model was not nearly efficient or effective enough, given the time it seems to have taken to uncover the Russian hack. Having advised their clients repeatedly about the 'supply-chain' threat, cyber-security and IT companies should recognise that they themselves are prize targets for potential supply-chain operations and therefore need to rigorously follow their own security advice. This should include applying extra protections to their most valuable data which, for cyber-security companies, includes their own red-team hacking tools and stored threat intelligence. More generally, cyber-security experts in governments and companies are advocating the development of a 'zero-trust architecture' approach to security. This includes the requirement that users, devices and services be continuously authorised and authenticated once they are inside the network, not just when joining it.[17] There have also been calls in congressional testimony for major IT companies to modernise some of their key security-related processes, including authentication systems. Furthermore, debate has intensified over how the storage of critical data should be spread between the cloud and 'on-premise' solutions. The recently uncovered Chinese hacking of Microsoft email servers intensifies these concerns.

*The psychology of security needs to change*

Regardless of how much the security of cyber-security and IT services can be improved through regulation or corporate initiatives, their customers cannot afford to be complacent. It is still their data, the compromise of which is their reputational, legal and financial risk. They should therefore hold those selling them services closer to account for the security provided. How many of SolarWinds' many clients asked the company to provide proof of a recent, externally validated audit of SolarWinds' own security practices? The psychology of security in most companies still needs to change. In major companies, junior officials report security issues to boards primarily concerned with the implications for the company's legal compliance. Instead, the boards themselves should include a mandatory, permanent, full-time executive in charge of security, which should be treated on a par with legal and financial risk.

A further weakness in the cyber-security ecosystem is that a good deal of security consulting is done by the same companies that sell the services and technology. Objective appraisal may clash with sales goals, which raises a potential conflict of interest. Of course, some independent advice is already available through government organisations such as the National Institute of Standards and Technology and CISA in the US, and the National Cyber Security Centre in the UK. Nevertheless, the development of a stronger stable of independent private-sector consultancy firms with no technical solutions and only expertise and advice to sell, approved by government, would strengthen the overall system.

All of the aforementioned safeguards might have led to quicker detection or even prevention of the SolarWinds hack, or significantly limited its spread, raising the cost to Russia of successful espionage. But the balance of power would still remain with the capable state attacker. It still only needs to find one way around or through the defences, whereas the defender has to detect and stop every attack. While good cyber hygiene might prevent 90% of attacks, and more sophisticated layers of defence might take that to 95–99%, the most capable actors will still eventually get through. Perhaps the key lesson of SolarWinds for cyber security, and more broadly of ransomware attacks for those who cannot afford the best defence, is that greater priority should be given to improving resilience. Networks should be designed and constructed, and data stored, to lessen the impact of compromise by ensuring that the best protections and redundancy are applied to the most valuable subset of data. This could involve introducing a data-classification system and storing the most valuable data in several independent places, and in some instances even air-gapping its storage from the internet. In addition, processes for crisis management and response and disaster recovery should be regularly exercised, in preparation for the almost inevitable breach.

Finally, it is worth noting that the SolarWinds hack exploited software and equipment supplied by US companies. It had nothing to do with any Russian-owned or -supplied equipment. Neither did the recently discovered Chinese hack of Microsoft email servers involve Chinese equipment. Indeed, this is true of most state cyber-espionage operations, which might otherwise

jeopardise the state's own companies and their exports. In this light, the inclination of the US government to ban Chinese equipment from national networks on account of an espionage risk appears somewhat overblown. The more formidable technological challenge to cyber security will arise with the Internet of Things: household appliances, cars, roads, healthcare systems and even whole cities connected to the internet so as to become 'smart'. This development portends a massive increase in the number of internet-connected devices, and a far wider vulnerability to disruption. Devising a security ecosystem, technical protections and even basic cyber hygiene to protect the Internet of Things involves far more complex tasks. In this instance, foreign ownership of key components inside national networks does present a major risk – not of espionage in peacetime, but rather sabotage in periods of heightened tension or war. Diversifying next-generation mobile networks by using open architectures to integrate equipment from multiple vendors, while placing restrictions on high-risk vendors, looks like one way to manage such risks in the future.

## The implications for offensive cyber

The development and application of offensive cyber doctrine have been under way in the United States for almost as long as the internet it invented has existed.[18] Its notably successful use of sophisticated cyber capabilities between 2008 and 2010 to disrupt Iranian nuclear enrichment occurred only halfway through that short history.

The 2018 US National Cyber Strategy announced a Cyber Deterrence Initiative that aimed to impose 'consequences' on malign cyber actors. While the national strategy makes it clear that there are many ways to do this, the US Department of Defense's 2018 Cyber Strategy sets out the role aggressive US cyber operations are intended to play. The strategy contemplates using cyber operations for an assertive defence of national interests, defending 'forward' (that is, on adversary networks), pre-empting attack and competing daily by way of 'persistent engagement'.[19] As a result of the SolarWinds hack, some are questioning whether such use of cyber operations is working or could ever work, and whether the investment should instead be diverted to national cyber security.

If the intent of SolarWinds was espionage and reconnaissance, it should be no surprise that US offensive cyber capabilities did not deter it, as that is manifestly not their purpose. During the Cold War, the threat of retaliatory conventional and nuclear attack was to stop war, not to deter state-on-state espionage, reconnaissance, pre-positioning or even covert action; indeed, it incentivised such activities. We should not view actions taken in cyberspace differently. The United States' defend-forward strategy is intended to deter (and retaliate against) a state whose goal is to use cyber or other means to disrupt, damage or destroy rather than to spy. By contrast, in dealing with cyber espionage, a state's strategy should be to incorporate protective measures that make espionage against it as difficult as possible, and to detect, dissect and disrupt it when it occurs. It should not expect to prevent it completely, especially given that it is an accepted part of international behaviour. Indeed, the only publicly avowed US cyber operations to have taken place against a state actor under the Cyber Deterrence Initiative were conducted by US Cyber Command before the US mid-term elections in 2018 against a Russian group that attempted to disrupt – not merely spy on – the 2016 US presidential election. While there were probably many reasons the Russians did not attempt to disrupt the 2020 presidential election in the same way, the US operation may have contributed. Furthermore, the fact that in 2019 the US considered the use of cyber operations to retaliate against the shooting down of a US drone by the Iranians is a reminder that, ultimately, the development of offensive cyber capabilities is also for when deterrence fails. As the Pentagon's 2018 Cyber Strategy acknowledges, such capabilities are also needed for war.[20] Doctrinally, cyber-capable states recognise that they cannot just build cyber fortresses ('Maginot Lines') but also need to be able to manoeuvre in cyberspace.

Clearly, therefore, the SolarWinds hack does not detract from the need to invest in and develop offensive cyber. But the short history of cyber operations starkly shows how carefully this must be done. As noted, to attack Ukraine, the Russians used a worm in combination with highly sensitive capabilities that the US had developed for espionage, failed to protect and lost. The same leaked US capabilities also played a role in North Korea's

worldwide use of a worm in the WannaCry ransomware attack of 2017 that infected 200,000 computers across 150 countries, and claimed the UK National Health Service as an unintended victim. Even if the US intent behind creating the original capabilities was to use them purely for espionage, and even if the Russian intent behind the SolarWinds hack was the same, the release of such capabilities 'in the wild' opens them up to reuse and repurposing by other states (and non-state actors, for that matter) to destructive effect.

Like their adversaries, though, liberal democracies still need to reconnoitre networks and position capabilities in peacetime to have any chance of success during war. As noted, the risks of miscalculation need to be carefully managed. In this connection, the United States' persistent engagement during peacetime with state adversaries on their networks appears risky. Such skirmishing can be easily justified when conducted to disrupt the state, or state-directed organisations, responsible for hostile cyber attacks. But if used to interfere with, or perceived to interfere with, the more general networks of state adversaries, it could become problematic. An adversary might use it to justify retaliatory interference in internal US networks, including, for example, those relating to the US electoral process. In that case, the intended deterrence would have failed. Defenders of persistent engagement might argue, of course, that operations demonstrating the potential to cause disruption on adversary networks could have precisely the deterrent effect the United States seeks. The point is that these are fine lines, and the history of offensive cyber is too short to support firm conclusions either way.[21]

Generally, there is not enough that is properly understood about the realities of offensive cyber to allow for informed public debate about its utility and the risks entailed. It is salutary that, without so far having had such a debate, some were quick to question the need to invest in offensive cyber at all. Given the US Cyber Deterrence Initiative and, for example, the UK's recent creation of a National Cyber Force, it is all the more urgent to have that informed debate.

* * *

The extent of the SolarWinds hack, and the vulnerabilities it has created, are extremely serious. Nevertheless, given that its intent was probably merely reconnaissance or espionage, direct retaliatory measures may be hard to justify. The priority instead is for the US to review and renew its approach to national cyber security, while at the same time working with allies and partners to redefine the boundaries of responsible cyber behaviour. In particular, the indiscriminate use of widespread IT vulnerabilities should be recognised as beyond the pale for a responsible state. Protocols for retaliatory and de-escalatory measures should be further developed, noting a key lesson from SolarWinds: that some informed US officials and analysts came close to construing Russian cyber espionage as an act of war.

At the same time, the US should not let the SolarWinds hack dislodge the basic tenets of its current strategy, including a 'whole of society' approach, greater attention to cyber hygiene, improving cooperation between government and the private sector, tackling as a priority the use of ransomware, and deterring destructive attacks by states. The US should maintain confidence in the key advantages that liberal democracies have over their adversaries: a strong and innovative private cyber-security sector, and the ability to act in concert with international allies. Companies in the IT-services and cyber-security sectors should still take a more rigorous approach to ensuring their own security; all organisations should plan for maximum resiliency; and perhaps new domestic regulations mandating the notification of breaches and discouraging the payment of ransoms to cyber criminals are needed.

More broadly, there needs to be a better understanding of the purpose of offensive cyber operations in a liberal democracy: when they are intended for deterrence or retaliation; how they are used in actual conflict; how they can be used in peacetime; and how the risks should be managed. The use of such capabilities to compete persistently on the networks of adversary states in peacetime warrants careful review, to weigh intended effects against attendant risks. Most importantly, liberal democracies need to tell the story publicly of how they, in contrast with their adversaries, develop, protect and use cyber capabilities responsibly. In that vein, both the US and UK governments have revealed publicly how they make decisions about releasing any 'zero day' computer-security vulnerabilities they discover,

each announcing a default position to disclose them for patching rather than to retain them for exploitation.[22] This is a good first step, but more is needed.

Ultimately, while the US cannot afford to be complacent, it still needs to keep its assessment of the implications of the SolarWinds hack set in its wider context. Based on the relevant criteria – strategy, governance, cyber security, cyber intelligence, digital industrial capacity and innovation, diplomacy and international alliances, and offensive cyber – the US remains the world's most powerful cyber state by some margin.[23] The SolarWinds hack holds painful lessons for the US, requiring action, but it is unlikely to alter that reality.

## Notes

1 Quoted in Kari Paul et al., 'SolarWinds Hack Was Work of "At Least 1,000 Engineers", Tech Executives Tell Senate', *Guardian*, 24 February 2021, https://www.theguardian.com/technology/2021/feb/23/solarwinds-hack-senate-hearing-microsoft.

2 See, for example, White House, 'Press Briefing by Press Secretary Jen Psaki and Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger', 17 February 2021, https://www.whitehouse.gov/briefing-room/press-briefings/2021/02/17/press-briefing-by-press-secretary-jen-psaki-and-deputy-national-security-advisor-for-cyber-and-emerging-technology-anne-neuberger-february-17-2021/.

3 To add a further complication, there are apparently ongoing FBI investigations into a hack into SolarWinds, suspected to have been perpetrated by the Chinese state, which led to a breach of a federal payroll agency within the US Department of Agriculture. This used a different software flaw and was on a much smaller scale than the Russian operation. See Christopher Bing et al., 'Exclusive: Suspected Chinese Hackers Used SolarWinds Bug to Spy on U.S. Payroll Agency – Sources', Reuters, 2 February 2021, https://www.reuters.com/article/us-cyber-solarwinds-china-exclusive-idUSKBN2A22K8.

4 White House, 'Press Briefing by Press Secretary Jen Psaki and Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger'.

5 See, for example, Yevgeny Vindman, 'Is the SolarWinds Cyberattack an Act of War? It Is, if the United States Says It Is', *Lawfare*, 26 January 2021, https://www.lawfareblog.com/solarwinds-cyberattack-act-war-it-if-united-states-says-it.

6 Quoted in Paul et al., 'SolarWinds Hack Was Work of "At Least 1,000 Engineers", Tech Executives Tell Senate'.

7 See 'Russia's Communications Ministry Plans to Isolate the RuNet by 2020', *Meduza*, 13 May 2016, https://

meduza.io/en/news/2016/05/13/communications-ministry-plans-to-isolate-runet-by-2020; and Justin Sherman, 'Russia's Domestic Internet Is a Threat to the Global Internet', *Slate*, 24 October 2019, https://slate.com/technology/2019/10/russia-runet-disconnection-domestic-internet.html.

8 See, for example, International Telecommunications Union, 'Global Cybersecurity Index 2018', p. 62, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

9 See Tarah Wheeler, 'The Danger in Calling the SolarWinds Breach an "Act of War"', Brookings Institution, 4 March 2021, https://www.brookings.edu/techstream/the-danger-in-calling-the-solarwinds-breach-an-act-of-war/.

10 See Henrik Breitenbauch and Niels Byrjalsen, 'Subversion, Statecraft and Liberal Democracy', *Survival*, vol. 61, no. 4, August–September 2019, pp. 31–41.

11 This dispensation was enshrined in the United States' 2018 National Cyber Strategy as the Cyber Deterrence Initiative: 'The United States will work with like-minded states to coordinate and support each other's responses to significant malicious cyber incidents, including through intelligence sharing, buttressing of attribution claims, public statements of support for responsive actions taken, and joint imposition of consequences against malign actors.' See White House, 'National Cyber Strategy of the United States of America', September 2018, p. 21, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

12 See UN General Assembly, 'Report of the Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', A/70/174, 22 July 2015, https://undocs.org/pdf?symbol=en/A/70/174. A further eight norms are set out in Global Commission on the Stability of Cyberspace, 'Advancing Cyber Stability: Final Report', November 2019, https://cyberstability.org/report/.

13 See David Blagden, 'Deterring Cyber Coercion: The Exaggerated Problem of Attribution', *Survival*, vol. 62, no. 1, February–March 2020, pp. 131–48.

14 See 'Former US Cybersecurity Chief Calls for Military to Attack Hackers', *Financial Times*, 5 February 2021, https://www.ft.com/content/27c09769-ceb5-46dd-824f-40b684d681ae.

15 See, for instance, Sarah Coble, 'Cybercrime Costs World Economy Over 1% of Global GDP', *Infosecurity Magazine*, 7 December 2020, https://www.infosecurity-magazine.com/news/cybercrime-costs-1trillion/; and Zhanna Malekos Smith and Eugenia Lostri, 'The Hidden Costs of Cybercrime', McAfee, December 2020, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf.

16 The Global Commission on the Stability of Cyberspace's 'Advancing Cyber Stability' contains a discussion of 'Basic Cyber Hygiene as Foundational Defence'.

17 This requirement is advocated by, for example, the UK National Cyber Security Centre. See National Cyber Security Centre, 'Zero Trust Architecture Design Principles', 20 November 2019, https://www.

ncsc.gov.uk/blog-post/zero-trust-architecture-design-principles. Companies such as Microsoft and CrowdStrike also support it.

18 The term 'offensive cyber' here covers the full range of active cyber operations – from those designed to influence or for disruptive effect in peacetime, to those designed for destructive effect in war, and all variations in between – regardless of whether the operations are run by civilians or the military, or whether their intended purpose is military or non-military. The definition includes all the various conventional terms, including computer-network attack, computer-network operations, cyber effects, online covert action and cyber-enabled information operations and warfare.

19 See US Department of Defense, 'Summary of US Department of Defence Cyber Strategy', September 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

20 *Ibid*., p. 4.

21 The use of offensive cyber operations for disruptive or destructive effect in peacetime is less controversial against non-state actors, such as terrorists and organised criminals, who are more difficult to deter than states. Nevertheless, such operations still need to avoid the indiscriminate exploitation of widespread IT vulnerabilities.

22 See White House, 'Vulnerabilities Equities Policy and Process for the United States Government', 15 November 2017, https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF; and GCHQ, 'The Equities Process', 29 November 2018, https://www.gchq.gov.uk/information/equities-process. A norm of behaviour set out in the Global Commission on the Stability of Cyberspace's 'Advancing Cyber Stability' is as follows: 'States should create procedurally transparent frameworks to assess whether and when to disclose not publicly known vulnerabilities or flaws they are aware of in information systems and technologies. The default presumption should be in favour of disclosure.'

23 See Nigel Inkster, 'Measuring Military Cyber Power', *Survival*, vol. 59, no. 4, August–September 2017, pp. 27–34; Marcus Willett, 'Assessing Cyber Power', *Survival*, vol. 51, no. 1, February–March 2019, pp. 85–90; and Julia Voo et al., 'National Cyber Power Index 2020: Methodology and Analytical Considerations', China Cyber Policy Initiative, Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2020, pp. 11–12, https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf.