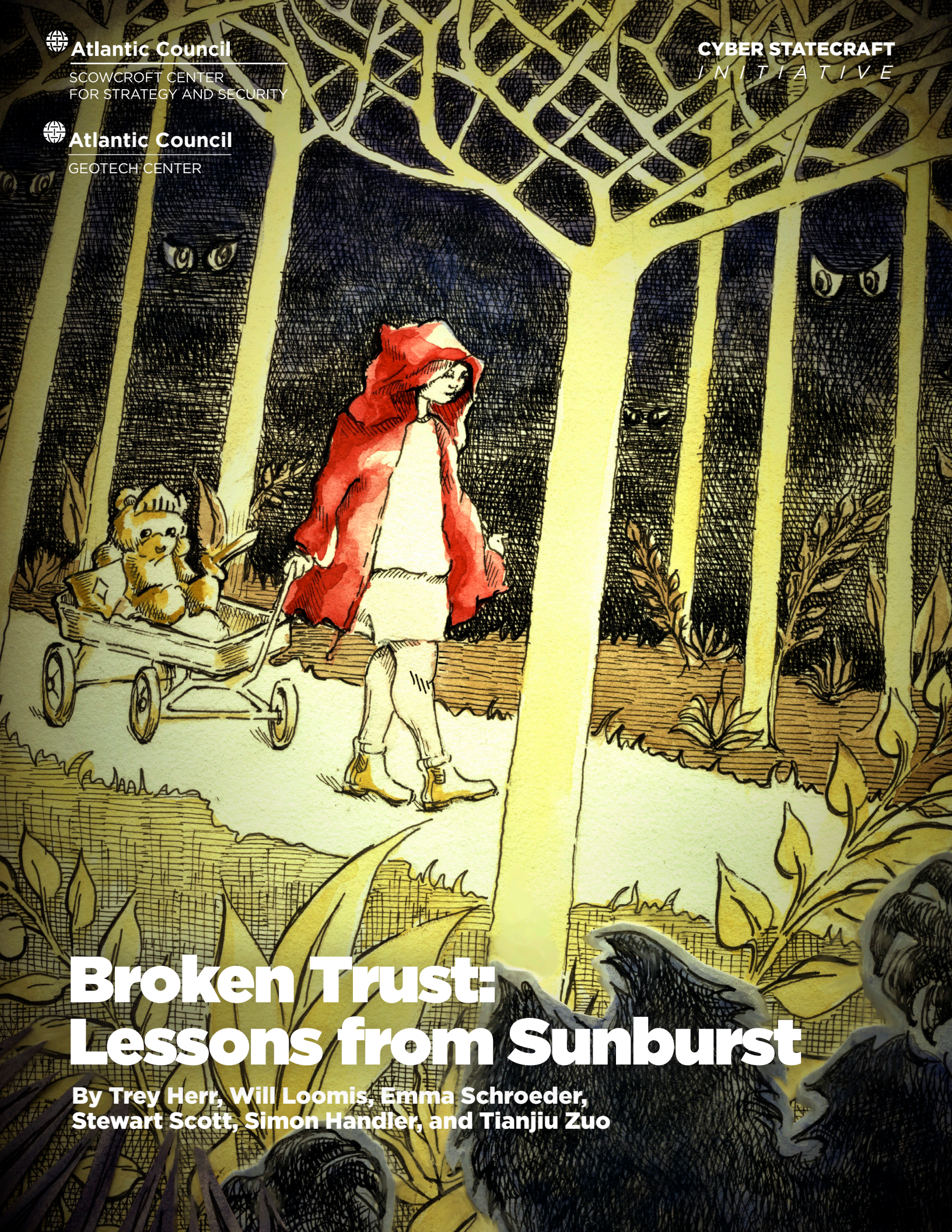
Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

Atlantic Council
GEOTECH CENTER

CYBER STATECRAFT
INITIATIVE



Broken Trust: Lessons from Sunburst

By Trey Herr, Will Loomis, Emma Schroeder, Stewart Scott, Simon Handler, and Tianjiu Zuo

Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

Atlantic Council
GEOTECH CENTER

CYBER STATECRAFT
INITIATIVE

The Scowcroft Center for Strategy and Security works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

The Cyber Statecraft Initiative works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

The GeoTech Center is one of the newest centers within the Atlantic Council, and its mission is to champion positive paths that nations, economies, and societies can pursue to ensure new tech and data empower people while securing prosperity and peace. The GeoTech Center was founded with the recognition that the Atlantic Council's mission of "shaping the future together" must now address the outsized role that data and technology will play in molding that future and whether it results in a better, more peaceful world. As a result, the GeoTech Center has a broad mandate to explore the geopolitical implications of data and technology including technology for good, non-traditional geopolitical actors, and US technology policy.

Cover: A vintage style of children's book illustration brings to life new threats, while reminding us that the story of trust is as old as time. The cover art and signets were designed by Ivana Troselj who is studying a cybersecurity-related field in Australia. She has a background in fine arts and illustration.

For more on software supply-chain security, visit the Cyber Statecraft Initiative's Breaking Trust project:
https://www.atlanticcouncil.org/programs/scowcroft-center-for-strategy-and-security/cyber-statecraft-initiative/breaking-trust/

Atlantic Council
1030 15th Street NW, 12th Floor
Washington, DC 20005

For more information, please visit
www.AtlanticCouncil.org.

ISBN-13: 978-1-61977-168-0
March 2021

This report was designed by Donald Partyka.

Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

Atlantic Council
GEOTECH CENTER

Broken Trust: Lessons from Sunburst

Trey Herr, Will Loomis,[a] Emma Schroeder,[a] Stewart Scott,[b] Simon Handler,[a] and Tianjiu Zuo[c]

a Atlantic Council's Cyber Statecraft Initiative in the Scowcroft Center for Security and Strategy
b Atlantic Council's GeoTech Center
c Duke University

EXECUTIVE SUMMARY

The Sunburst crisis was a failure of strategy more than it was the product of an information-technology (IT) problem or a mythical adversary. Overlooking that question of strategy invites crises larger and more frequent than those the United States is battling today. The US government and industry should embrace the idea of "persistent flow" to address this strategic shortfall; emphasizing that effective cybersecurity is more about speed, balance, and concentrated action. Both the public and private sectors must work together to ruthlessly prioritize risk, make linchpin systems in the cloud more defensible, and make federal cyber-risk management more self-adaptive.

The story of trust is an old one, but the Sunburst cyber-espionage campaign was a startling reminder of the United States' collective cyber insecurity and the inadequacy of current US strategy to compete in a dynamic intelligence contest in cyberspace. The compromise of SolarWinds, part of the wider Sunburst campaign, has had enormous consequences, but, as supply-chain attacks go, it was not unprecedented, as demonstrated by seven other events from the last decade.[1]

Sunburst was also a significant moment for cloud computing security. The adversary inflicted the campaign's most dramatic harm by silently moving through Microsoft's identity software products, including those supporting Office 365 and Azure cloud services, and vacuuming up emails and files from dozens of organizations. The campaign raises concerns about the existing threat model that major cloud service providers Amazon, Microsoft, and Google, utilize for their linchpin services, and the ease with which users can manage and defend these products. For cloud's "shared responsibility" to work, cloud providers must build technology users can actually defend.

Studying the Sunburst campaign, three overarching lessons become clear. First, states have compromised sensitive software supply chains before. The role of cloud computing as a target is what takes Sunburst from another in a string of supply-chain compromises to a significant intelligence-gathering coup. Second, the United States could have done more to limit the harm of this event, especially by better prioritizing risk in federal technology systems, by making the targeted cloud services more easily defensible and capable by default, and by giving federal cybersecurity leaders better tools to adapt and govern their shared enterprise.

Third, Sunburst was a failure of strategy much more than it was just an IT risk-management foul-up or the success of a clever adversary. The United States government continues to labor under a regulatory model for software security that does not match the ways in which software are built, bought, or deployed. Adding vague new secure development standards to an already overbuilt system of unmet controls and overlapping committees is not a recipe for success. Meanwhile, industry is struggling to architect its services to simultaneously and effectively defend against the latest threats, account for overlapping government requirements, and remain competitive—especially in the market for cloud services.

Observers should recognize Sunburst as part of a disturbing trend: an ongoing intelligence contest between the United States and its adversaries in which the United States is giving up leverage due to technical insecurity, deficient policy response, and a shortfall in strategy. The response to Sunburst must lead to meaningful action from both industry and the policymaking community to improve the defensibility of the technology ecosystem and position the United States and its allies to compete more effectively in this intelligence contest.

The Sunburst crisis can be a catalyst for change and, while near-term reforms are practicable, change must extend beyond shifting how the United States buys technology or takes retribution against an adversary. The United States and its allies must acknowledge that this is a fight for that leverage. In an intelligence contest, tactical and operational information about an adversary—such as insight on forthcoming sanctions or the shape of a vulnerable network—is strategic leverage. The policymaking community must work with industry to assist defenders in becoming faster, more balanced, and better synchronized with offensive activities to ensure cyberspace remains a useful domain—one that advances national security objectives.

1 Trey Herr, William Loomis, June Lee, and Stewart Scott, Breaking Trust: Shades of Crisis across an Insecure Software Supply Chain, Atlantic Council, July 27, 2020, https://www.atlanticcouncil.org/in-depth-research-reports/report/breaking-trust-shades-of-crisis-across-an-insecure-software-supply-chain.

DECEMBER 14, 2020

"US HOMELAND SECURITY, THOUSANDS OF BUSINESSES SCRAMBLE AFTER SUSPECTED RUSSIAN HACK"
— REUTERS

"MICROSOFT'S ROLE IN SOLARWINDS BREACH COMES UNDER SCRUTINY"
— CRN

DECEMBER 15, 2020

DECEMBER 20, 2020

"BIDEN CHIEF OF STAFF SAYS HACK RESPONSE WILL GO BEYOND 'JUST SANCTIONS'"
— REUTERS

"SOLARWINDS BREACH 'MUCH WORSE' THAN FEARED"
— SDXCENTRAL

JANUARY 4, 2021

JANUARY 14, 2021

"SOLARWINDS HACK FORCES RECKONING WITH SUPPLY-CHAIN SECURITY"
— THE WALL STREET JOURNAL

"BIDEN ORDER US INTELLIGENCE REVIEW OF SOLARWINDS HACK"
— CYBERSCOOP

JANUARY 21, 2021

FEBRUARY 18, 2021

"SOLARWINDS ATTACK HIT 100 COMPANIES AND TOOK MONTHS OF PLANNING, SAYS WHITE HOUSE"
— ZDNET

"US GOVERNMENT TO RESPOND TO SOLARWINDS HACKERS IN WEEKS: SENIOR OFFICIAL"
— REUTERS

MARCH 12, 2021

MARCH 17, 2021

"OFFICIALS URGE BIDEN TO APPOINT CYBER LEADERS AFTER SOLARWINDS, MICROSOFT HACKS"
— THE HILL

INTRODUCTION

Now more than ever, society depends on software. Whether it is the cloud computing behind an email service, a new fifth-generation (5G) telecommunications deployment, or the system used to monitor a remote oil rig, software has become an essential and pervasive facet of modern society. As one commentator put it, "software is eating the world."[2] Unlike physical systems, software is always a work in progress. It relies on continual revisions from patches and updates to address security flaws and vulnerabilities, and to make functional improvements. This ongoing maintenance leaves software supply chains long, messy, and in continuous flux, resulting in significant and underappreciated aggregated risk for organizations across the world. Despite warnings from key members of the security community and increased attention to supply-chain security more generally, software has largely taken a backseat to hardware—especially 5G—in policy debates over supply-chain security.[3]

Cyberspace is a domain of persistent low-grade engagement below the threshold of war. Software supply chains have become a key vector for adversaries—especially those contesting for valuable intelligence. The logic of the intelligence contest argues that cyber operations are principally focused on the acquisition of information from or denial of the same to an adversary. States can use this information to identify and seize leverage over an opponent. The emailed deliberations of diplomatic activity within a coalition, a government agency's coordination with industry during a standards body's meeting, contracts for an upcoming naval flotilla's port of call—all of these are nuggets of useful information that an adversary can use to shape its behavior, moving toward gaps in attention and recognizing points of vulnerability subject to influence. All of this information contributes to adversaries' search for strategic leverage over one another and helps create opportunities to exert that leverage toward national security objectives.

In the fall of 2019, the Atlantic Council's Cyber Statecraft Initiative launched the Breaking Trust project to catalog software supply-chain intrusions over the past decade and identify major trends in their execution. Released in July 2020, the first report from this project, and its accompanying dataset, found that operations exploiting the software supply chain have become more frequent and more impactful over the last ten years as their targets have become even more diverse.[4] This report updates the dataset to include one hundred and thirty-eight incidents and, now, one of the most consequential cybersecurity crises of a young decade: Sunburst.

Beginning sometime in 2019 and carrying throughout 2020, an adversary group infiltrated more than one hundred organizations ranging from the US Departments of Homeland Security and the Treasury to Intel and Microsoft, along with seven other government agencies in the United States and nearly one hundred private companies. The adversary targeted email accounts and other productivity tools. In nearly every case, the adversary moved across victim networks by abusing several widely used Microsoft identity and access management (IAM) products, and leveraging this abuse to gain access to customer Office 365 environments in the cloud.[5] As many as 70 percent of these victims were initially compromised by a software supply-chain attack on Texas-based vendor SolarWinds, from which the incident originally received its moniker.

This report uses the label "Sunburst" for this ongoing campaign. While public reporting initially focused on SolarWinds, and the compromise of this vendor's Orion software was significant, it was just one of multiple vectors used to gain access to targeted organizations and compromise both on-premises and cloud services.[6] As a supply-chain compromise, Sunburst is not unique; it shares common traits with, and reflects lessons unlearned from, at least seven other major software supply-chain attacks from the last decade. According to an estimate by the Cybersecurity and Infrastructure Security Agency (CISA), as many as 30 percent of these compromises occurred without

2 Marc Andreessen, "Why Software Is Eating the World," Wall Street Journal, August 20, 2011, https://www.wsj.com/articles/SB10001424053111903480904576512250915629460.

3 "Remediation and Hardening Strategies for Microsoft 365 to Defend Against UNC2452, Version 1," Mandiant, January 19, 2021, https://www.fireeye.com/content/dam/collateral/en/wp-m-unc2452.pdf.

4 Ibid.

5 Ibid.

6 "Alert (AA20-352A)," Cybersecurity and Infrastructure Security Agency, December 17, 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-352a.

any involvement by SolarWinds software, with acting Director of CISA Brandon Wales making clear, "It is absolutely correct that this campaign should not be thought of as the SolarWinds campaign."[7] The Sunburst malware was one of several malicious tools that the adversary used to move across targeted networks, including hopping into dozens of Office 365 environments. It is this lateral movement into the cloud, and the effective abuse of Microsoft's identity services, that distinguishes an otherwise large software supply chain attack from a widespread intelligence coup.

Sunburst was neither a military strike nor an indiscriminate act of harm; it was a slow and considered development of access to sensitive government, industry, and nonprofit targets, much more like a human-intelligence operation than a kinetic strike. The campaign is visible evidence of the persistent intelligence contest that is ongoing in, and through, cyberspace. How the adversary will use information obtained during the Sunburst campaign to exert leverage over the United States, facilitate sabotage, or carry out some later outright attack, is yet unrealized.[8]

This report develops the first significant, contextualized public analysis of Sunburst, and extracts lessons for both policymakers and industry. The goal of this analysis is to understand key phases of the Sunburst campaign in the framework of an intelligence contest, examine critical similarities with seven other recent campaigns, identify both technical and policy shortfalls that precipitated the crisis, and develop recommendations to renew US cybersecurity strategy.

Section I explores the Sunburst campaign and works to understand the interplay between the software supply-chain compromise and the abuse of cloud and on-premises identity services.

Section II focuses on the familiarity of the Sunburst campaign in light of previous software supply-chain attacks by providing in-depth analysis of seven likely state-backed examples from 2012 to 2020. The section maps all incidents onto a notional outline of the software supply chain and development lifecycle used in the Atlantic Council's previous reporting on supply chain risk management and draws out commonalities among them. The similarities—in execution, intent, and outcome—guide two critical discussions in the subsequent sections: the intelligence context in which software supply chain attacks occur and the failure of current policies and industry priorities to better prevent, identify, mitigate, and respond to them. Supply chain attacks like Sunburst have happened before, and understanding why and how the United States has adapted (or failed to adapt) previously will inform a more effective cybersecurity strategy going forward.

Section III analyzes some of the causal factors behind Sunburst's scope and success. It delves into the shortcomings of US cybersecurity strategy and posture along three key lanes: deficiencies in risk management, reliance on hard-to-defend linchpin technologies, and limited speed alongside poor adaptability. Sunburst uniquely brings attention to the many concurrent weaknesses throughout the US cybersecurity risk-management architecture. The section pays particular attention to the cloud-enabled and cloud-adjacent features of the campaign, which differentiate Sunburst from previous widespread software supply-chain compromises. Even within existing policy regimes, better mitigation and more rapid responses to compromise, in line with stated program goals, could have curbed Sunburst's impact. Identifying these shortcomings is key to an informed and holistic policy shift. This both primes understanding and repairing the system and creates an urgent call to action for reform.

Section IV looks at the systemic misalignment between US strategy and cybersecurity outcomes. It includes acknowledgement of underappreciated but successful (or potentially so) policy programs before developing three clusters of recommendations to renew US cybersecurity strategy. The recommendations aim to drive ruthless prioritization of risk across federal cybersecurity, to improve the defensibility of linchpin cloud services, and to develop a more adaptive federal cyber risk-management system. Together, these twelve recommendations argue for concentrating effort at points of maximum value to defenders, while improving interconnectivity between offense and defense, and maximizing the speed and

7 Robert McMillan, et al., "Suspected Russian Hack Extends Far Beyond SolarWinds Software, Investigators Say," Wall Street Journal, January 29, 2021, https://www.wsj.com/articles/suspected-russian-hack-extends-far-beyond-solarwinds-software-investigators-say-11611921601.

8 This report and related content use the terms "attack" and "target" both for rhetorical clarity and to match the language of the technical and operational reporting on which much of this analysis is based. SolarWinds and the Sunburst incident do not rise to the level of an armed attack, nor the threshold of war, but the authors will leave it to others to parse the ongoing (and perhaps never-ending) debate over terminology and classification of this contest.

adaptability of policymaking in partnership with key industry stakeholders. Taken together, the recommendations can help create a more responsive, better aligned US cybersecurity strategy.

The Sunburst campaign was not a triumph of some mythical adversary, nor simply the product of IT failures. It was the result of a strategic shortfall in how the United States organizes itself to fight for leverage in cyberspace. Overcoming this shortfall requires examining the technical and policy pathways of the Sunburst campaign as much as its strategic intent. Policymakers' response to the campaign should take heed of the continuity between Sunburst and past events to recognize that this is surely not the last such crisis with which the United States will have to contend.

Acknowledgements

Thank you to the many staff and researchers who have supported the Breaking Trust project since its inception, including Madison Lockett, June Lee, Ben Schatz, and Lily Liu. Thank you to Nancy Messiah for data visualization and web interactivity and to Donald Partyka for graphic and document design. The authors are indebted to Ivana Troselj for her work to create the cover and chapter signets. For their peer review of the cloud security discussion and role of cloud in the Sunburst campaign, the authors thank Dirk-jan Mollema, Rich Mogull, Marc Rogers, and several other reviewers who wish to remain anonymous. Thank you to the attendees of seven roundtables and workshops over the past year for feedback on this effort. Finally, thank you to Joyce Corell, Dan Geer, Allan Friedman, Wendy Nather, Chris Wysopal, and Joshua Rovner for their guidance and insight.

"THE SUNBURST CAMPAIGN WAS NOT A TRIUMPH OF SOME MYTHICAL ADVERSARY, NOR SIMPLY THE PRODUCT OF IT FAILURES. IT WAS THE RESULT OF A STRATEGIC SHORTFALL IN HOW THE UNITED STATES ORGANIZES ITSELF TO FIGHT FOR LEVERAGE IN CYBERSPACE."

I — SUNBURST EXPLAINED

The incident response to the Sunburst crisis is ongoing, and more details about the campaign's scope will become known in time. SolarWinds was one of several companies compromised as the adversary's means of gaining access to more than one hundred actively exploited targets. The adversary's ultimate goal in every publicly discussed case was organizational email accounts, along with their associated calendars and files.[9] To facilitate this access, the intruders persistently and effectively abused features of several Microsoft IAM products to move throughout organizations, pilfering inboxes in ways that proved difficult to track and trace. Indeed, the varied flavors of Microsoft's IAM services are as central, if not more so, to the Sunburst campaign than SolarWinds. For instance, Malwarebytes, a security firm, disclosed a compromise through which Sunburst actors targeted the company's systems by "abusing applications with privileged access to Microsoft Office 365 and Azure environments" to access emails, despite the firm not using SolarWinds Orion.[10] Other examples include a failed attempt by the intruders to breach the security firm CrowdStrike through a Microsoft reseller's Azure account to access the company's email servers, and reports from Mimecast, an email security management provider, that explained how in January a malicious actor had compromised one of the certificates used to "guard connections between its products and Microsoft's cloud server."[11] Although Mimecast stated that up to 3,600 of its customers could have been affected, it believes that only

9 Damien Cash, et al., "Dark Halo Leverages SolarWinds Compromise to Breach Organizations," Volexity, December 14, 2020, https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations; White House, "02/17/21: Press Briefing by Press Secretary and Deputy National Security Advisor," YouTube, February 17, 2021, https://www.youtube.com/watch?v=Ta_vatZ24Cs.

10 Dan Goodin, "Security Firm Malwarebytes Was Infected by Same Hackers Who Hit SolarWinds," Ars Technica, January 20, 2021, https://arstechnica.com/information-technology/2021/01/security-firm-malwarebytes-was-infected-by-same-hackers-who-hit-solarwinds/; Marcin Kleczynski, "Malwarebytes Targeted by Nation State Actor Implicated in SolarWinds Breach. Evidence Suggests Abuse of Privileged Access to Microsoft Office 365 and Azure Environments," Malwarebytes Labs, January 28, 2021, https://blog.malwarebytes.com/malwarebytes-news/2021/01/malwarebytes-targeted-by-nation-state-actor-implicated-in-solarwinds-breach-evidence-suggests-abuse-of-privileged-access-to-microsoft-office-365-and-azure-environments.

11 Shannon Vavra, "Microsoft Alerts CrowdStrike of Hackers' Attempted Break-in," CyberScoop, December 24, 2020, https://www.cyberscoop.com/crowdstrike-solarwinds-targeted-microsoft; "Email Security Firm Mimecast Says Hackers Hijacked Its Products to Spy on Customers," Reuters, January 12, 2021, https://www.reuters.com/article/us-global-cyber-mimecast/email-security-firm-mimecast-says-hackers-hijacked-its-products-to-spy-on-customers-idUSKBN29H22K.

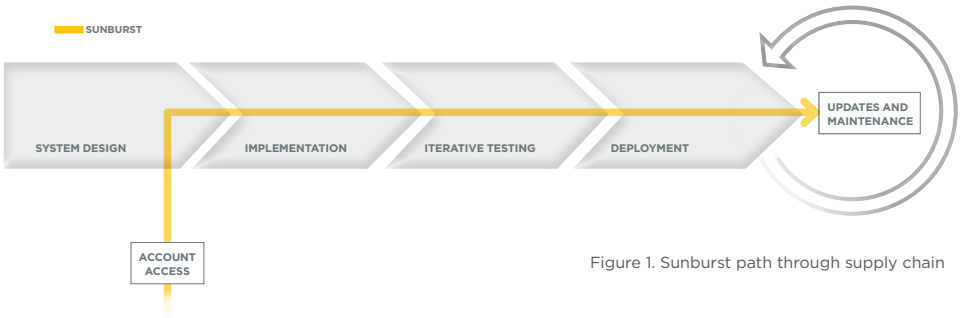


Figure 1. Sunburst path through supply chain

a "low single-digit number" of users were specifically targeted, demonstrating a pattern of deliberation in the Sunburst campaign.[12]

SolarWinds was a significant vector to this wider effort to compromise email and cloud environments.[13] Sometime in 2019, malicious actors compromised SolarWinds, a software developer based in Austin, Texas, and gained access to software-development and build infrastructure for the company's Orion product.[14]

Once inside, the adversary inserted the Sunburst backdoor into a version of Orion via a small, but malicious, change to a dynamic-link library (DLL), which triggered the larger backdoor.[15] SolarWinds would eventually unknowingly digitally sign and distribute this compromised version of Orion as an update to customers.[16]

This compromised update, with its legitimate certificates, allowed Sunburst to slip easily undetected past network security tools and into more than eighteen thousand organizations from February to June 2020.[17] This initial infection included more than four hundred and twenty-five members of the US Fortune 500, systemically important technology vendors like Microsoft and Intel,[18] and nearly a dozen US federal government agencies, including the Departments of the Treasury, Homeland Security, State, and Energy, as well state and local agencies.[19] Orion's popularity, and the software's wide use among system administrators with permissioned access to most or all of victim networks, made it a valuable target.

The adversary further compromised a very small number of these total eighteen thousand targets, using Sunburst to call a series of second-stage malware known as droppers, Teardrop and Raindrop, to download yet more malware that the

12 Tara Seals, "Mimecast Confirms SolarWinds Hack as List of Security Vendor Victims Snowball," Threatpost, January 28, 2021, https://threatpost.com/mimecast-solarwinds-hack-security-vendor-victims/163431.

13 Sudhakar Ramakrishna, "New Findings From Our Investigation of SUNBURST," Orange Matter, January 11, 2021, https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst.

14 "A Timeline of the Solarwinds Hack: What We've Learned," Kiuwan, January 19, 2021, https://www.kiuwan.com/solarwinds-hack-timeline; "SolarStorm Timeline: Details of the Software Supply-Chain Attack," Unit42, December 23, 2020, https://unit42.paloaltonetworks.com/solarstorm-supply-chain-attack-timeline.

15 "Analyzing Solorigate, the Compromised DLL File That Started a Sophisticated Cyberattack, and How Microsoft Defender Helps Protect Customers," Microsoft Security, December 18, 2020, https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect.

16 Snir Ben Shimol, "SolarWinds SUNBURST Backdoor: Inside the Stealthy APT Campaign," Inside Out Security, March 9, 2021, https://www.varonis.com/blog/solarwinds-sunburst-backdoor-inside-the-stealthy-apt-campaign.

17 Chris Hickman, "How X.509 Certificate Were Involved in SolarWinds Attack," Security Boulevard, December 18, 2020, https://securityboulevard.com/2020/12/how-x-509-certificates-were-involved-in-solarwinds-attack-keyfactor; Catalin Cimpanu, "SEC Filings: SolarWinds Says 18,000 Customers Were Impacted by Recent Hack," ZDNet, December 14, 2020, https://www.zdnet.com/article/sec-filings-solarwinds-says-18000-customers-are-impacted-by-recent-hack.

18 Laura Hautala, "Russia Has Allegedly Hit the US with an Unprecedented Malware Attack: Here's What You Need to Know," CNET, February 28, 2021, https://www.cnet.com/news/solarwinds-not-the-only-company-used-to-hack-targets-tech-execs-say-at-hearing; Mitchell Clark, "Big Tech Companies Including Intel, Nvidia, and Cisco Were All Infected During the SolarWinds Hack," Verge, December 21, 2020, https://www.theverge.com/2020/12/21/22194183/intel-nvidia-cisco-government-infected-solarwinds-hack; Kim Zetter, "Someone Asked Me to Provide a Simple Description of What This SolarWinds Hack Is All About So for Anyone Who Is Confused by the Technical Details, Here's a Thread with a Simplified Explanation of What Happened and What It Means," Twitter, December 14, 2020, 2:43 a.m., https://twitter.com/KimZetter/status/1338389130951061504.

19 Sara Wilson, "SolarWinds Recap: All of the Federal Agencies Caught Up in the Orion Breach," FedScoop, December 22, 2020, https://www.fedscoop.com/solarwinds-recap-federal-agencies-caught-orion-breach; Raphael Satter, "U.S. Cyber Agency Says SolarWinds Hackers Are 'Impacting' State, Local Governments," Reuters, December 24, 2020, https://www.reuters.com/article/us-global-cyber-usa-idUSKBN28Y09L; Jack Stubbs, et al., "SolarWinds Hackers Broke into U.S. Cable Firm and Arizona County, Web Records Show," Reuters, December 18, 2020, https://www.reuters.com/article/us-usa-cyber-idUSKBN28S2B9.

intruders would use to move through target networks.[20] Decoupling these second- and later-stage malware from Sunburst helped hide the SolarWinds compromise for as long as possible.[21]

Although more than 80 percent of the affected SolarWinds customers operate in the United States, the breach also affected clients in Canada, Mexico, Belgium, Spain, the United Kingdom, Israel, and the United Arab Emirates.[22] The effort needed to simultaneously and directly compromise even one tenth as many organizations would be enormous, underlining the incredible cost-effectiveness of software supply-chain intrusions.

In the case of Sunburst, a large-scale software supply-chain attack became a full-blown crisis when the adversary successfully abused several Microsoft IAM products. This abuse, sustained by including techniques known to the security community for years, helped the adversary move silently across victim networks. These techniques also enabled the adversary, in a damaging turn of events, to hop from on-premises networks into Office 365 environments.

In nearly every case observed by FireEye, the Sunburst adversary relied on various techniques to abuse Microsoft's IAM products to move laterally within organizations—enabling the most consequential phase of the ongoing incident.[23] Sunburst operators targeted Azure Active Directory, the Microsoft service used to authenticate users of both Office 365 and Azure, to modify access controls and abuse highly privileged accounts to access email accounts across organizations.[24] The adversary also leveraged a previously disclosed technique to steal signing certificates to grant itself access to sensitive resources while bypassing multi-factor authentication safeguards, including dozens of user email inboxes in Office 365.[25]

The US government and multiple security firms have asserted state-sponsored Russian culpability for the campaign, although there is disagreement about which specific group is responsible. Incident response has taken place in stages, and by

20 "SUNSPOT: An Implant in the Build Process," CrowdStrike Blog, January 11, 2021, https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/.

21 The details of the attack are intricate, but—given the many payloads and intrusion stages, as well as the variety of malware strains tailored to specific targets—they are worth reviewing briefly. "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor," FireEye, December 13, 2020, https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html; "SUNSPOT: An Implant in the Build Process," CrowdStrike Intelligence Team, January 11, 2021, https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/. The intruders first infiltrated the network of SolarWinds and implanted the SUNSPOT malware, which, in turn, inserted the SUNBURST malware into Orion during its development. Even at this early phase, the intruders took great care to remain stealthy, running SUNSPOT infrequently and encrypting its log files. "Deep Dive into the Solorigate Second-Stage Activation: From SUNBURST to TEARDROP and Raindrop," Microsoft, January 20, 2021, https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/. Once Sunburst was in target systems via an Orion update, it downloaded another malware called Teardrop onto selected systems. Teardrop is a "dropper" designed to stealthily inject more malware onto a target system. In this case, Teardrop inserted Beacon, a penetration testing suite based on the commercial Cobalt Strike. "Raindrop: New Malware Discovered in SolarWinds Investigation," Symantec Blogs, January 18, 2021, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-raindrop-malware. After Teardrop, the malicious actor installed Raindrop, a similar dropper, onto targeted computers that were not infected by Sunburst. Raindrop also inserted Cobalt Strike Beacon onto targets, though the exact configurations and setups of the two droppers vary. "Malware Analysis Report (AR21-039B)," Cybersecurity and Infrastructure Security Agency, February 8, 2021, https://us-cert.cisa.gov/ncas/analysis-reports/ar21-039b; "Beacon Covert C2 Payload," Cobalt Strike, accessed March 1, 2021, https://www.cobaltstrike.com/help-beacon. By using Teardrop and Raindrop, the intruders protected the Sunburst backdoor from discovery.

22 Catalin Cimpanu, "Microsoft Says It Identified 40 Victims of the SolarWinds Hack," ZDNet, December 18, 2020, https://www.zdnet.com/article/microsoft-says-it-identified-40-victims-of-the-solarwinds-hack.

23 "Microsoft Security Response Center," Microsoft Security Response Center, December 31, 2020, https://msrc-blog.microsoft.com/2020/12/31/microsoft-internal-solorigate-investigation-update.

24 Shain Wray, "SolarWinds Post-Compromise Hunting with Azure Sentinel," Microsoft, December 16, 2020, https://techcommunity.microsoft.com/t5/azure-sentinel/solarwinds-post-compromise-hunting-with-azure-sentinel/ba-p/1995095. "Remediation and Hardening Strategies for Microsoft 365 to Defend Against UNC2452, Version 1"; Michael Sentonas, "CrowdStrike Launches Free Tool to Identify & Mitigate Risks in Azure Active Directory," CrowdStrike, January 12, 2021, https://www.crowdstrike.com/blog/crowdstrike-launches-free-tool-to-identify-and-help-mitigate-risks-in-azure-active-directory.

25 Mathew J. Schwartz and Ron Ross, "US Treasury Suffered 'Significant' SolarWinds Breach," Bank Information Security, https://www.bankinfosecurity.com/us-treasury-suffers-significant-solarwinds-breach-a-15641;

Alex Weinert, "Understanding Solorigate's Identity IOCs—for Identity Vendors and Their Customers," Microsoft, February 1, 2021, https://techcommunity.microsoft.com/t5/azure-active-directory-identity/understanding-quot-solorigate-quot-s-identity-iocs-for-identity/ba-p/2007610.

independent investigations using both private and public data where attribution was not the first priority. On December 14, 2020, The Washington Post, citing anonymous sources, blamed the campaign on APT29 (Cozy Bear), which Dutch intelligence agencies have linked to Russia's Foreign Intelligence Service (SVR).[26] The Russian attribution seemed to be informally confirmed the next day, when a member of the US Congress publicly identified Russia after receiving a classified briefing.[27] Indeed, this attribution to Russia was strengthened when a joint statement by the Federal Bureau of Investigation (FBI), CISA, the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA) identified the operation as "likely Russian in origin."[28]

"IMPORTANTLY, MANY OF SUNBURST'S CHARACTERISTICS—OBJECTIVES, METHODS, AND TARGET SELECTION—ECHO PREVIOUS CAMPAIGNS, AND SHOULD PROVIDE LESSONS FOR INDUSTRY PRACTITIONERS AND POLICYMAKERS ALIKE."

Attribution, as ever, remains more than a technical question.[29] From the private sector, both FireEye and the security firm Volexity, in contrast to the reporting by The Washington Post, attributed the operation to an unknown or uncategorized group, called UNC2452 by FireEye on December 13, 2020,[30] and Dark Halo by Volexity the following day.[31] Both FireEye and Volexity have maintained this attribution. Separately, technical evidence published on January 11, 2021, by Kaspersky researchers highlighted similarities between the SolarWinds compromise and past operations by Turla (Venomous Bear),[32] a threat actor that the Estonian Foreign Intelligence Service (EFIS) had previously tied to the Russian Federal Security Service (FSB).[33] This slow and winding attribution process is likely to continue in the coming months.

While the adversary's successful, repeated abuse of Microsoft's identity products helped Sunburst become something more than a notable supply-chain compromise, there are important lessons in the SolarWinds vector. Importantly, many of Sunburst's characteristics—objectives, methods, and target selection—echo previous campaigns, and should provide lessons for industry practitioners and policymakers alike.

26 Ellen Nakashima, et al., "Russian Government Hackers Are behind a Broad Espionage Campaign That Has Compromised U.S. Agencies, including Treasury and Commerce," Washington Post, December 14, 2020, 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.

27 Richard Blumenthal, "Stunning. Today's Classified Briefing on Russia's Cyberattack Left Me Deeply Alarmed, in Fact Downright Scared. Americans Deserve to Know What's Going On. Declassify What's Known & Unknown," Twitter, December 15, 2020, https://twitter.com/SenBlumenthal/status/1338972186535727105?s=20.

28 "ODNI Home," ODNI Office of Strategic Communications, January 5, 2021, https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2021/item/2176-joint-statement-by-the-federal-bureau-of-investigation-fbi-the-cybersecurity-and-infrastructure-security-agency-cisa-the-office-of-the-director-of-national-intelligence-odni-and-the-national-security-agency-nsa; Andrew Olson, et al., "Explainer—Russia's Potent Cyber and Information Warfare Capabilities," Reuters, December 19, 2020, https://www.reuters.com/article/global-cyber-russia/explainer-russias-potent-cyber-and-information-warfare-capabilities-idUSKBN28T0ML.

29 Thomas Rid, et al., "Attributing Cyber Attacks," Journal of Strategic Studies 38: 1–2, 4–37, https://www.tandfonline.com/doi/abs/10.1080/01402390.2014.977382.

30 Kevin Mandia, "Global Intrusion Campaign Leverages Software Supply Chain Compromise," FireEye, December 13, 2020, https://www.fireeye.com/blog/products-and-services/2020/12/global-intrusion-campaign-leverages-software-supply-chain-compromise.html.

31 Cash, et al., "Dark Halo Leverages SolarWinds Compromise to Breach Organizations."

32 Georgy Raiu, et al., "Sunburst Backdoor—Code Overlaps with Kazuar," Securelist, January 11, 2021, https://securelist.com/sunburst-backdoor-kazuar/99981.

33 "The Domestic Political Situation in Russia," Estonian Foreign Intelligence Service, 2018, https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf; Andy Greenburg, "SolarWinds Hackers Shared Tricks with Known Russian Cyberspies," Wired, January 11, 2021, https://www.wired.com/story/solarwinds-russia-hackers-turla-malware.

II —THE HISTORICAL ROOTS OF SUNBURST

Sunburst offers rare public insight into the intense contest for information taking place in and through cyberspace, as well as the insecurity of critical technology supply chains. Sunburst may be one of the most consequential espionage campaigns of a generation. But, as a software supply-chain intrusion, it has ample precedent.

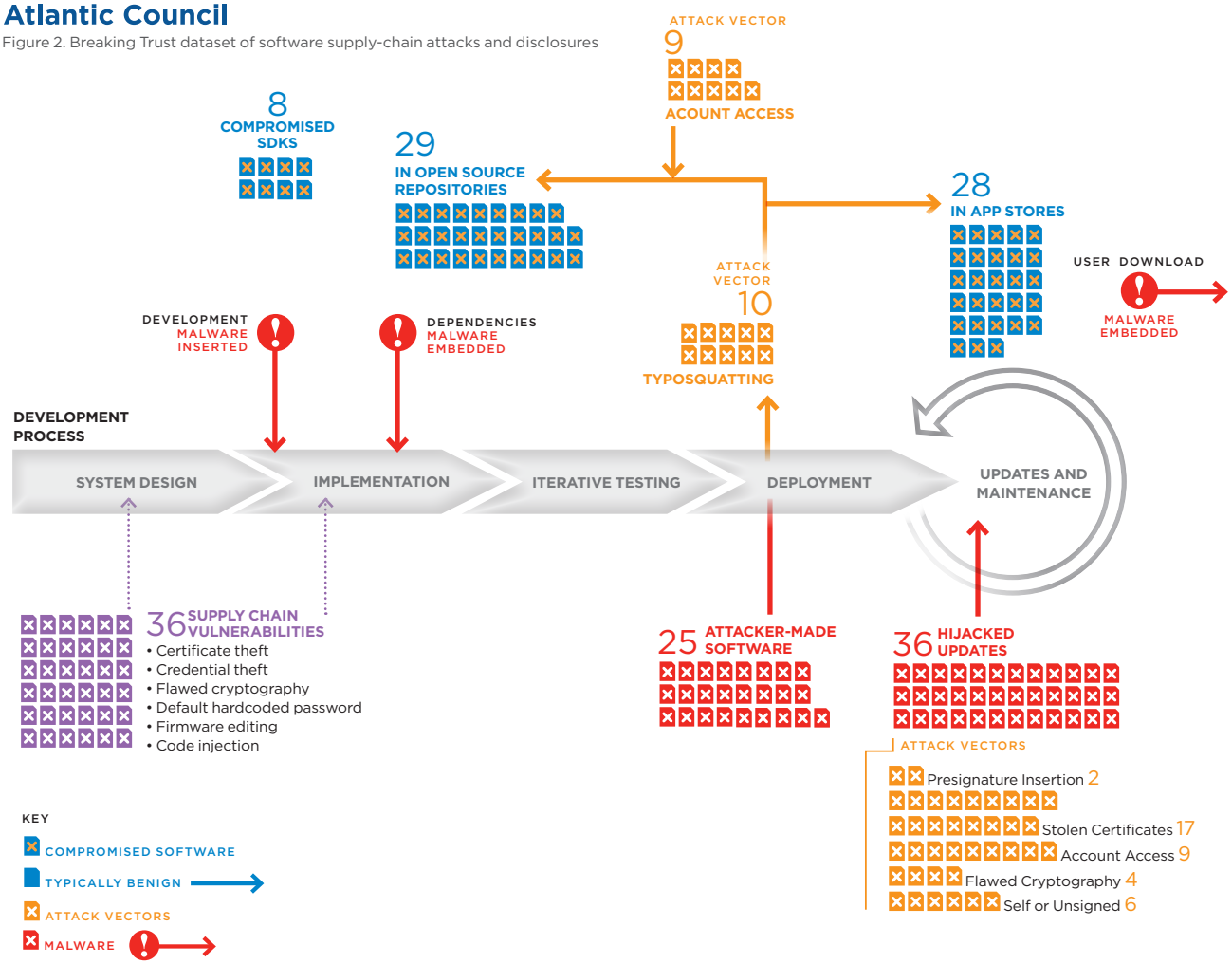
A significant vector in the Sunburst incident was the adversary's compromise of SolarWinds' Orion software-development infrastructure, allowing intruders to place malware in thousands of potential targets. As Figure 2 illustrates, since 2010, there have been thirty-six other cases of intruders likewise successfully targeting software updates out of one hundred and thirty-eight total recorded supply-chain attacks and vulnerability disclosures. The authors laid out each of these incidents along a notional model of software development to show their distribution across the software supply chain.[34]

In the Sunburst case, intruders were able to access SolarWinds' build infrastructure, rather than just tacking malware onto a pending update. Of these thirty-six total cases, approximately fifteen included similar access to build or update infrastructure, and, of those, nearly half have state attribution. Rather than adding their malware alongside the Orion software just before they sent it to customers, like attaching to a motorcycle a sidecar with a bomb inside, the intruders went further and compromised the company's build infrastructure. The result was like secreting a bomb into the cylinders of the motorcycle's engine before it sold—far more deeply embedded in the resulting device, and thus harder to detect or remove.

34 There is no good way to concisely represent all of software development, and this graphic is not intended to capture the many intricacies of the process. This representation of a waterfall-style model matches with much of the software captured in the study. For more on this dataset, see: Herr et al., Breaking Trust.

Atlantic Council

Figure 2. Breaking Trust dataset of software supply-chain attacks and disclosures



Many of these states are locked in a persistent contest for information in which they "compete to steal information from one another, protect what they have acquired, and corrupt the other side's data and communications."[35] Software supply-chain intrusions are well suited to this intelligence contest. They deliver stealthy espionage capabilities, including data collection, data alteration, and the opportunity to position for follow-on activities. This kind of access, and the information it offers, can produce the type of operational leverage states seek to achieve in cyberspace in support of more strategic ends beyond the one domain. Though not leveraged directly, information's aggregation and distillation allow parties to recognize opportunities for action, and to anticipate or respond to efforts against their valuable targets. This leverage could come, for example, in the form of valuable intellectual property that can invigorate a key industry or as information on planned sanction targets and timelines to enable the resilience of the affected areas. Recognizing the logic of this intelligence contest, and the real value of this leverage, should help inform a more effective defense.

This section reviews seven campaigns that share common traits with Sunburst: CCleaner, Kingslayer, Flame, Able Desktop, VeraPort, SignSight, and Juniper. The report covers these seven cases as similarly meaningful examples of state-backed software supply-chain intrusions as well as to cover a range of dates, from 2012 to more recent incidents from 2020.

CCleaner

Over the course of 2017, a version of the ubiquitous administrative tool CCleaner, now owned by Avast, was compromised and distributed to several hundred thousand customers, and then used to infiltrate a

35 Robert Chesney et al., "Policy Roundtable: Cyber Conflict as an Intelligence Contest," Texas National Security Review, December 18, 2020, https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest.

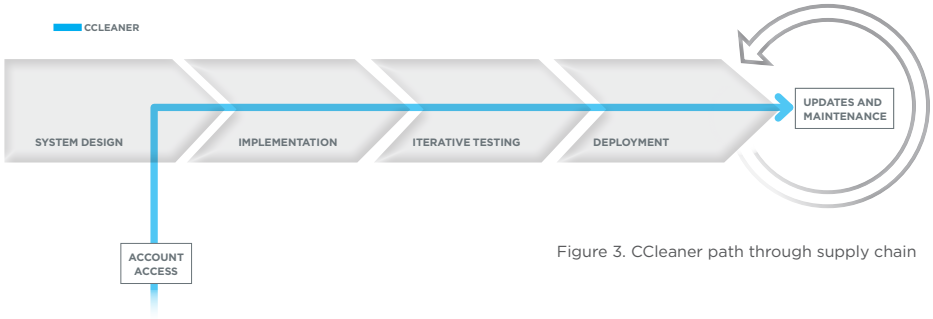


Figure 3. CCleaner path through supply chain

small set of technology and telecommunications companies from within the initial target group.[36]

Intruders initially gained access to the software while it was still owned and operated by Piriform, through a developer workstation reached using credentials stolen from an administrative collaborative tool called TeamViewer.[37]

Once inside, the intruders began to move laterally within Piriform's network during off hours to avoid detection and, in less than a month, installed a modified version of the ShadowPad malware to gain wider access to Piriform's build and deployment systems. Beginning in August 2017, after Avast's acquisition of the software, intruders began distributing a compromised version of CCleaner to approximately 2.27 million users through the company's update system. As in the case of Sunburst, users had no reason to suspect the authenticity of these software updates. They came cryptographically signed directly from the software vendor. These companies were based in eight different countries, mostly in East and Southeast Asia. This tactic of casting a wide net and then narrowly refining an active target list is common to this type of intrusion. However, with Sunburst, the malware distribution reached more diverse targets, including government agencies and nonprofits. As in the Sunburst case, the CCleaner compromise focused on gathering information, with no evidence that there was any intent to disrupt or deny operation of the affected companies.

Kaspersky Lab and others have linked_CCleaner to the Chinese hacking group APT17 under the umbrella of the Axiom group, which has a history of using software supply-chain incursions as its core tool to uncover and exploit espionage targets. Based on both technical and contextual evidence, this allegation details tactics that strongly resembled those used in intrusions previously attributed to the Axiom group. Focusing on attribution through intent, the specific concentration on these companies strongly suggests that the intruder's intent was to extract intellectual property. China has previously been identified as a prominent practitioner of economic espionage, and others point to the degree of resource intensity of the CCleaner compromise, the apparent technical knowledge of the intruders, and their level of preparation as strongly indicative of a state-affiliated group.[38]

Kingslayer

First disclosed by RSA Security researchers in February 2017, the Kingslayer operation targeted an administrative software package called EvLog—developed by the Canadian software company Altair Technologies—in a concerted software supply-chain intrusion, affecting a significant number of enterprise organizations across the globe.

EvLog served as a valuable target because its users were largely system and domain administrators, allowing intruders a high degree of access to targeted networks once they compromised the tool. In a statement later removed from its website, Altair claimed that its customers included four major telecommunications providers, ten different Western military organizations, twenty-four Fortune 500 companies, five major defense contractors, dozens of Western government

36 Lucian Constantin, "40 Enterprise Computers Infected with Second-Stage CCleaner Malware," Security Boulevard, September 26, 2017, https://securityboulevard.com/2017/09/40-enterprise-computers-infected-second-stage-ccleaner-malware/.

37 Alyssa Foote, "Inside the Unnerving Supply Chain Attack That Corrupted CCleaner," Wired, April 7, 2018, https://www.wired.com/story/inside-the-unnerving-supply-chain-attack-that-corrupted-ccleaner.

38 Michael Mimoso, "Inside the CCleaner Backdoor Attack," Threat Post, October 5, 2017, https://threatpost.com/inside-the-ccleaner-backdoor-attack/128283/; Lucian Constantin, "Researchers Link CCleaner Hack to Cyberespionage Group," Vice, September 21, 2017, https://www.vice.com/en/article/7xkxba/researchers-link-ccleaner-hack-to-cyberespionage-group; Hearing before the Congressional Executive Commission on China, 113th Congress, 1st session, June 25, 2013, https://www.govinfo.gov/content/pkg/CHRG-113hhrg81855/html/CHRG-113hhrg81855.htm; Jay Rosenberg, "Evidence Aurora Operation Still Active Part 2: More Ties Uncovered Between CCleaner Hack & Chinese Hackers," Intezer, October 2, 2017, https://www.intezer.com/blog/research/evidence-aurora-operation-still-active-part-2-more-ties-uncovered-between-ccleaner-hack-chinese-hackers.

organizations, and myriad banks and universities. As with Sunburst, the intruders utilized EvLog's extensive client list and administrative privileges to achieve persistent access to the systems of a wide variety of high-tier clients in the private and public sectors.[39] However, almost five years after the Kingslayer campaign began, it is still not known how many of these customers may have been—and possibly remain—compromised by the operation.

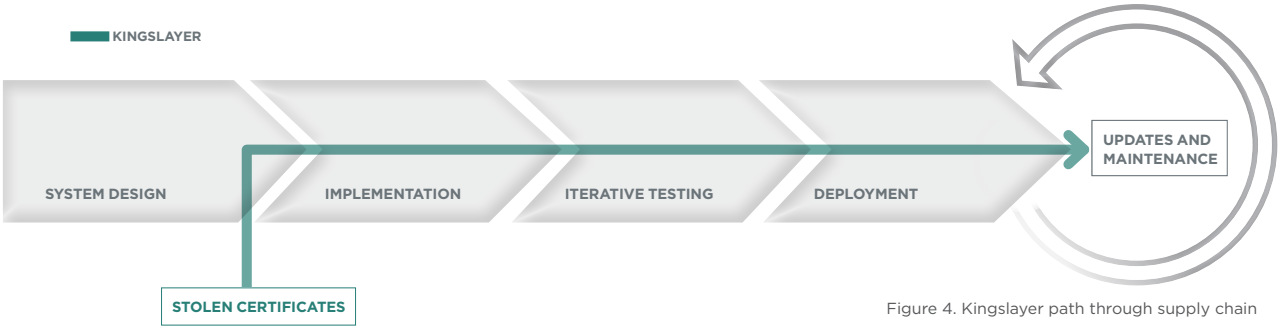


Figure 4. Kingslayer path through supply chain

The primary vector in this incident was Altair's EvLog 3.0, a tool that allowed Windows system administrators to accurately interpret and troubleshoot items in event logs. Intruders initially compromised eventid.net, the website used to host EvLog and provide downloads and updates, and replaced legitimate EvLog 3.0 files with a malicious version of the software. It is not clear how these intruders first gained access to the Altair update system, but they managed to secure Altair's code-signing certificate and authenticate their malicious version. Once this install or update was complete, the malicious package would then attempt to download a secondary payload. The targets of this malware, as in the Sunburst incident, trusted the compromised version of the EvLog software without verification, as it appeared "certified and sent" by Altair Technology.[40]

Like Sunburst, Kingslayer appears to have been an espionage operation, with no evidence that there was any intent to disrupt or deny operations of the affected companies, and the intruders took significant steps to remain covert. Because EvLog is almost exclusively used by system administrators, it also represents an "ideal beachhead and operational staging environment for systematic exploitation of a large enterprise."[41] The malware gave intruders espionage-enabling capabilities such as uploading and downloading files, as well as the ability to execute programs on the affected network. The Kingslayer campaign was attributed with some confidence to the China-based threat group Codoso, also known as APT9 or Nightshade Panda. Researchers were able to identify overlapping domains and Internet Protocol (IP) addresses for command-and-control infrastructure between Kingslayer and past Codoso campaigns. This incident fits the observed trend of Chinese espionage operations, which tend to be large and covert incursions against both private-sector actors and US government entities, including targets whose value may only be realized in operations months or years later.[42]

Flame

In 2012, a technically mature cyber-espionage operation was reportedly linked to the same consortium of agencies as the watershed Stuxnet malware discovered two years earlier.[43] The initial target of this software supply-chain operation was the widely used Microsoft Windows operating system, in which Flame masqueraded as a legitimate software update.

The operators of Flame used a novel variant of a cryptographic collision to take advantage of weaknesses

39 Amy Blackshaw, "Kingslayer—A Supply Chain Attack," RSA, February 13, 2017, https://www.rsa.com/en-us/blog/2017-02/kingslayer-a-supply-chain-attack.

40 Howard Solomon, "Canadian Cyber Firm Confirms It Was the Victim Described in RSA Investigation," IT World Canada, February 23, 2017, https://www.itworldcanada.com/article/canadian-cyber-firm-confirms-it-was-the-victim-described-in-rsa-investigation/390903.

41 "Whitepaper: Kingslayer—A Supply Chain Attack," RSA, February 13, 2017, https://www.rsa.com/en-us/offers/kingslayer-a-supply-chain-attack.

42 Eduard Kovacs, "Serious Breach Linked to Chinese APTs Comes to Light," SecurityWeek, February 22, 2017, https://www.securityweek.com/serious-breach-linked-chinese-apts-comes-light.

43 Kim Zetter, "Report: US and Israel Behind Flame Espionage Tool," Wired, June 19, 2012, https://www.wired.com/2012/06/us-and-israel-behind-flame.

inherent in the MD5 hashing algorithm within the system design—weaknesses that had been known for more than a decade.[44] The intruders abused the weak hashing algorithm and the code-signing privileges erroneously granted to Terminal Server Licensing Service to forge code-signing certificates that were linked to Microsoft's root certificate authority.[45] These certificates tricked target computers into accepting incoming malware payload deployments as legitimate Windows updates.[46] To improve the likelihood of users accepting the falsified update, and to better disguise its activity, Flame was able to verify the update needs of individual systems. Unlike with Sunburst, intruders did not infiltrate Microsoft's update process per se; rather, they successfully disguised their deployments as legitimate software from the vendor.[47]

Once the Flame malware downloaded and unpacked itself onto target machines, it connected with one of approximately eighty available command-and-control servers to await further instruction. This malware had myriad capabilities, including mapping network traffic, taking screenshots, making audio recordings, and tracking keystrokes.[48] The Flame infection—first detected in 2010—likely began much earlier and infected machines worldwide, though its activity was concentrated in the Middle East.[49] The systems infected represented a wide diversity of target types, ranging from individuals to private companies to educational institutions to government organizations. The Flame malware, like Sunburst, showed impressive diversity in design and target typing.

Flame served as an effective espionage tool, gathering a wide range of information and allowing the intruders to both collect and alter data on the target systems. As with Sunburst, there is no evidence that the Flame malware was intended to cause destruction, only to gather and exfiltrate information. The Flame designers appear to have prioritized stealth and operational longevity in creating Flame, forgoing svelte malware for a large and multi-featured platform with sophisticated tricks to remove most traces of its presence from targeted computers.[50] According to a former high-ranking US intelligence official, the reported intelligence gathering surrounding the Iranian nuclear program was executed as part of a larger program intended to slow Iran's nuclear-enrichment program, and served as cyber prepositioning for further efforts to that end.

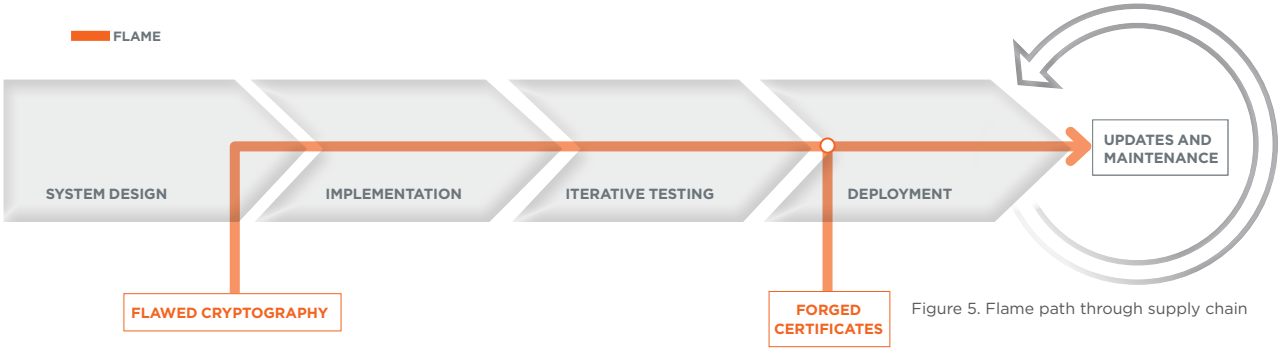


Figure 5. Flame path through supply chain

44 "CWI Cryptanalyst Discovers New Cryptographic Attack Variant in Flame Spy Malware," CWI, July 6, 2012, https://www.cwi.nl/news/2012/cwi-cryptanalist-discovers-new-cryptographic-attack-variant-in-flame-spy-malware; Robert Lemos, "Flame Exploited Long-Known Flaw in MD5 Certificate Algorithm," EWEEK, February 2, 2021, https://www.eweek.com/security/flame-exploited-long-known-flaw-in-md5-certificate-algorithm.

45 Alex Sotirov, "Analyzing the MD5 Collision in Flame," Trail of Bits, http://www.kormanyablak.org/it_security/2012-07-17/Alex_Sotirov_Flame_MD5-collision.pdf.

46 Gregg Keizer, "Researcher Reveal How Flame Fakes Windows Update," Computerworld, June 5, 2012, https://www.computerworld.com/article/2503916/researchers-reveal-how-flame-fakes-windows-update.html.

47 Zetter, "Report: US and Israel Behind Flame Espionage Tool"; Kim Zetter, "Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers," Wired, May 28, 2012, https://www.wired.com/2012/05/flame/.

48 Dave Lee, "Flame: Massive Cyber-attack Discovered, Researchers Say," BBC News, May 28, 2012, https://www.bbc.com/news/technology-18238326.

49 Alexander Gostev, et al., "The Flame: Questions and Answers," Securelist English Global, May 28, 2012, https://securelist.com/the-flame-questions-and-answers/34344.

50 Brian Prince, "Newly Discovered 'Flame' Cyber Weapon On Par With Stuxnet, Duqu," SecurityWeek, May 28, 2012, https://www.securityweek.com/newly-discovered-flame-cyber-weapon-par-stuxnet-duqu.

[51]Initial analysis of the size, complexity, and geographic scope of Flame suggested state involvement. As in the case of Sunburst, the developer would have needed to invest significant resources and technical expertise to execute the operation, especially to calculate the hash collision that allowed access to the Windows update process. After initial wide speculation as to attribution, The Washington Post reported that the United States and Israel were responsible for the creation of the Flame malware.[52] This attribution followed the discovery of evidence informing the behavior of the intruder, and the connection made that Flame contained some of the same code as the Stuxnet malware. This attribution, though not confirmed, also fits with the apparent intentions and targets of the malware—the Iranian nuclear-enrichment program—as well as with the intrusion's level of sophistication.[53]

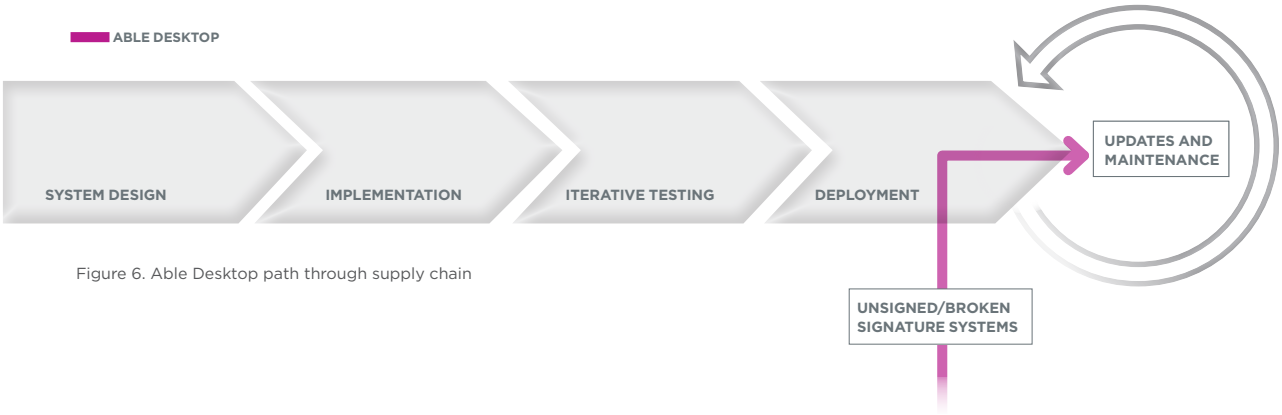


Figure 6. Able Desktop path through supply chain

Able Desktop

First disclosed by the Slovak security firm ESET in December 2020, Able Software's Able Desktop application was compromised through its software supply chain using hijacked updates, affecting private-sector and government users across Mongolia.

The primary vector for this compromise was Able Desktop, an application that supports instant messaging as an add-on to the company's main product, a human-resources management program. Initial access to Able Software's corporate network came through targeted phishing campaigns. Once inside, the intruders were able to move laterally and compromise Able Software's update-deployment infrastructure. The intruders used this compromise to upload two well-known malware strains, HyperBro and Tmanger, to the company's update server. Whenever prompted to update their desktop application, Able Software's customers received this malicious code instead.[54] Unlike Sunburst and CCleaner, the intruders did not need to steal or forge an update signature because Able's updates were unsigned—even when they were legitimate and did not include malicious code.

As with Sunburst, it is unclear when initial access began, or how long the operation was under way—intruders could have been hiding unobserved in systems for months, or even years. One report suggests that the intruders' interest in the Able Software networks stretched as far back as May 2018. Able Software was a valuable target due to its widespread use by the Mongolian federal government. More than four hundred and thirty different agencies, including the Office of the President, the Ministry of Justice, and various state and law-enforcements bodies used Able's

51 Greg Miller, et al., "U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say," Washington Post, June 19, 2012, https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html.

52 Ibid.

53 Alexander Gostev, et al., "Full Analysis of Flame's Command & Control servers," Securelist English Global Securelistcom, September 17, 2012, https://securelist.com/full-analysis-of-flames-command-control-servers/34216/; Gostev, "The Flame: Questions and Answers"; Prince, "Newly Discovered 'Flame' Cyber Weapon On Par With Stuxnet, Duqu"; Kim Zetter, "Coders Behind the Flame Malware Left Incriminating Clues on Control Servers," Wired, September 17, 2012, https://www.wired.com/2012/09/flame-coders-left-fingerprints.

54 "Operation StealthyTrident: Corporate Software under Attack," WeLiveSecurity, December 21, 2020, https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop.

software suite every day, giving intruders a deep, wide view into government operations.[55] This focus on government targets, along with the uploaded malware's capabilities, strongly suggests that intruders aimed to exfiltrate large quantities of sensitive, and potentially valuable, intelligence from government agencies.

There is extensive contextual and technical evidence that this operation was part of a larger espionage campaign against the Mongolian government. The Able Software update system had been targeted by at least two other attempts using tactics similar to the 2020 operation. Although researchers loosely attributed this operation to the Chinese APT group LuckyMouse by analyzing the tools used, those tools have also been utilized elsewhere by other actors—not all of them Chinese.[56] ESET believes this lack of clarity could be because these groups, mostly state-sponsored Chinese ones, collaborate to use the same tools, or are smaller entities acting as "part of a larger threat actor that controls their operations and targeting." This incident is part of a recurring pattern of digital espionage operations against Mongolian targets attributed by various entities to Chinese sources,[57] suggesting a long-running effort to support China's broader aims of geopolitical influence and regional, as well as social, stability, with intermittent attempts by the Mongolian government to assert leverage of its own.[58]

WIZVERA VeraPort

In November 2020, ESET disclosed that a widely required South Korean security tool, WIZVERA VeraPort, had been compromised, affecting an unknown number of organizations across the country.

WIZVERA VeraPort, the main vector for the intrusion, is a program used by South Korean banking and government websites to manage the download and use of mandated security plug-ins to verify the identity of users. Users are often blocked from using these sites unless they have WIZVERA VeraPort installed on their devices. In this operation, intruders took advantage of the requirement, stole code-signing certificates from two South Korean security companies, and used them to sign and then deploy malware through compromised websites.[59] Like with the Orion software in Sunburst, VeraPort's software trusted these certificates to certify new code as authentic, and so did not seek to validate downloads more intensely.

Figure 7. VeraPort path through supply chain

Similar to the Able Desktop intrusion, spear phishing was likely used to gain initial access to these websites and position these signed malware for download.

55 Catalin Cimpanu, "Chinese APT Suspected of Supply Chain Attack on Mongolian Government Agencies," ZDNet, December 10, 2020. https://www.zdnet.com/article/chinese-apt-suspected-of-supply-chain-attack-on-mongolian-government-agencies.

56 Luigino Camastra, et al., "APT Group Targeting Governmental Agencies in East Asia," Avast Threat Labs, December 18, 2020, https://decoded.avast.io/luigicamastra/apt-group-targeting-governmental-agencies-in-east-asia/.

57 "Khaan Quest: Chinese Cyber Espionage Targeting Mongolia: ThreatConnect: Risk-Threat-Response," ThreatConnect, October 7, 2013, https://threatconnect.com/blog/khaan-quest-chinese-cyber-espionage-targeting-mongolia.

58 Cimpanu, "Chinese APT Suspected of Supply Chain Attack on Mongolian Government Agencies"; Anthony Cuthbertson, "Mongolia Arrests 800 Chinese Nationals in Cyber Crime Raids," Independent, October 31, 2019, https://www.independent.co.uk/life-style/gadgets-and-tech/news/mongolia-china-cyber-crime-arrest-raids-a9179471.html.

59 "Lazarus Supply-Chain Attack in South Korea," WeLiveSecurity, January 1, 2021, https://www.welivesecurity.com/2020/11/16/lazarus-supply-chain-attack-south-korea; Charlie Osborne, "Lazarus Malware Strikes South Korean Supply Chains," ZDNet, November 16, 2020, https://www.zdnet.com/article/lazarus-malware-strikes-south-korean-supply-chains.

Once on users' systems, the intruders deployed added payloads to gather information and open a backdoor.[60] As with Sunburst, it is hard to determine how long intruders actively exploited VeraPort as they took great pains to disguise themselves—including varying filenames and using legitimate-looking icons.

Because the intrusion exclusively targeted users of VeraPort-supported websites, not much is known about the intended targets of the operation, other than their South Korean citizenship. This type of intrusion explicitly exploits the trust relationship between government, vendor, and citizen by utilizing mandated software as its distribution vector. The WIZVERA VeraPort compromise has been strongly attributed to Lazarus—also known as Hidden Cobra—an umbrella term used to describe groups likely tied to the North Korean government. Best remembered as the actor behind the 2014 Sony Hack, Lazarus is also known for consistently targeting South Korean citizens.[61] As with Sunburst, VeraPort provided another avenue for intelligence collection across a long-running geopolitical rivalry.

Operation SignSight

In the summer of 2020, the Vietnamese Government Certificate Authority (VGCA) was the primary vector of a software supply-chain intrusion targeting a wide range of public and private entities that used its digital-signature software, which provides both certificates of validation and software suites for handling digital document signatures. The software is widely used throughout the country, and is mandated in some cases.[62]

This software, like that targeted through Sunburst, was a trusted administrative tool distributed widely and at the nexus of many public-private interactions. The intruders infiltrated the VGCA website and redirected download links for two different pieces of software to instead deploy malware-laced versions from at least July 23 to August 16, 2020.[63] When run, the compromised software opened the legitimate VGCA program, while also writing the malware onto the target's computer. As the first step in a multi-part intrusion, the program created a backdoor on the victim machine called Smanager or PhantomNet, communicating basic information to a command-and-control server, and enabling the download and execution of additional malicious packages. The uncompromised versions of the installers had faulty signatures, so the malicious versions—whose digital signatures also failed to verify their integrity—appeared as authentic as the originals.

The SignSight incident derived its potency from the trust users placed in the compromised vendor—the VGCA—and the service oligopoly it had. The VGCA is one of only a handful of entities in Vietnam authorized to issue digital certificates, a crucial component in the cryptography of digital signatures that ensures the identity of the signer, meaning the authorities that issue them must be trustworthy. In fact, the VGCA was

Figure 8. SignSight path through supply chain

60 "Lazarus Supply-Chain Attack in South Korea."

61 Ibid.; Osborne, "Lazarus Malware Strikes South Korean Supply Chains."

62 "Electronic Signature Laws & Regulations—Vietnam," Adobe Help Center, September 22, 2020, https://helpx.adobe.com/sign/using/legality-vietnam.html; "Operation SignSight: Supply-Chain Attack against a Certification Authority in Southeast Asia," WeLiveSecurity, December 29, 2020, https://www.welivesecurity.com/2020/12/17/operation-signsight-supply-chain-attack-southeast-asia.

63 "Operation SignSight: SupplyChain Attack against a Certification Authority in Southeast Asia."

so trusted that its own incorrectly signed legitimate software failed to raise any red flags.[64] As the government provider of software for navigating digital signatures, the VGCA, much like the vectors involved in the Sunburst case, distributes to a large number of public- and private-sector clients. This gave the intrusion a wide blast radius, particularly centered on entities interacting directly with the Vietnamese government. SignSight also resembles the Sunburst intrusion in its targeting and speculated intent—espionage.

Where Operation SignSight differs from the Sunburst intrusion is in its sophistication. Though some errant instances of Smanager detected in the Philippines might imply a broader intrusion that utilized more vectors than currently understood, Operation SignSight lacks the global reach of Sunburst. Additionally, although the malicious versions of this software used deceptive names for malware files and communicated through encrypted web connections, SignSight lacks the more elaborate deception efforts seen in Sunburst. Even within the relatively niche slice of software supply-chain intrusions that target government-associated IT administrative software for intelligence gathering, there is a wide spectrum of complexity.

Some researchers attribute the intrusion to a China-backed group, due to artifacts left in the malware and to the similarities between Smanager and another backdoor, Tmanger, which is attributed to TA428, a group linked to China that has targeted East Asian countries like Mongolia, Russia, and Vietnam for intelligence-gathering purposes. Moreover, TA428 tends to target government IT entities, as did the perpetrators of Operation SignSight, with an eye toward extracting intelligence. As with Able Desktop, cooperation and sharing of malicious tools and infrastructure between Chinese groups complicates precise attribution.[65] A Chinese cyber intrusion into Vietnam would provide continued visibility into the decision-making of a burgeoning regional player whose security relationships with Chinese rivals in the Indo-Pacific, including the United States, continue to grow.

Juniper

Juniper Networks, an industry leader in networking products based in Sunnyvale, California, publicly announced a serious flaw in its NetScreen line of products in December 2015. Hackers infiltrated Juniper's software-development process and compromised the algorithm used to encrypt classified communications, allowing them to intercept data from multinational corporations and US government agencies.[66]

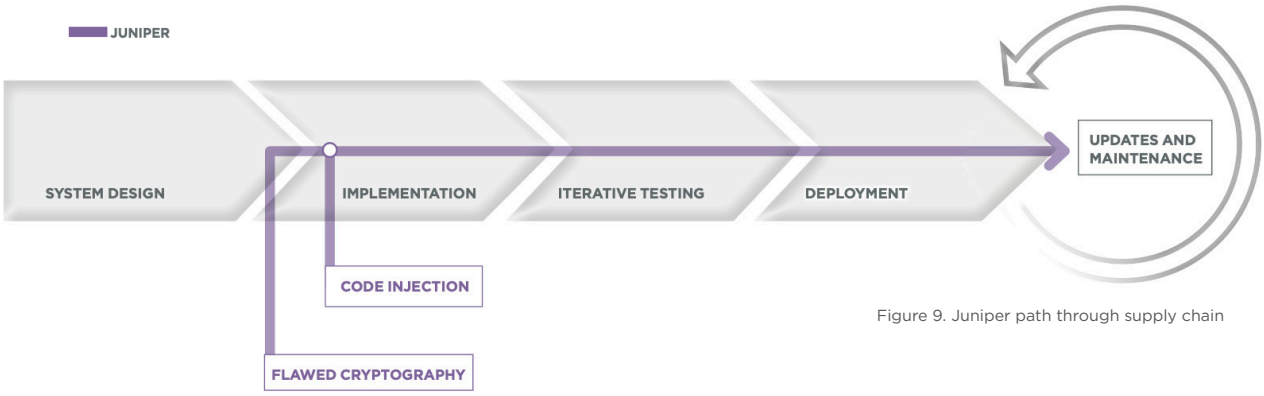


Figure 9. Juniper path through supply chain

NetScreen manufactures high-performance, commercial-grade security systems that are designed to provide firewall, virtual private network (VPN), and network traffic-management capabilities to large organizations. ScreenOS is the operating system powering NetScreen devices, through which authorized users transmit classified data using the built-in

64 Ha Thi Dung, "Digital Signature in Vietnam," Lexology, August 24, 2020, https://www.lexology.com/library/detail.aspx?g=3ef35305-e1f6-4dcf-82ad-bf1dcd8c0fd1.

65 "[RE018-2] Analyzing New Malware of China Panda Hacker Group Used to Attack Supply Chain against Vietnam Government Certification Authority—Part 2," VinCSS Blog, December 25, 2020, https://blog.vincss.net/2020/12/re018-2-analyzing-new-malware-of-china-panda-hacker-group-used-to-attack-supply-chain-against-vietnam-government-certification-authority.html?m=1; "Operation StealthyTrident: Corporate Software under Attack."; "Threat Group Cards: A Threat Actor Encyclopedia," TA428—Threat Group Cards: A Threat Actor Encyclopedia, https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=TA428&n=1.

66 Evan Perez and Shimon Prokupecz, "Newly Discovered Hack Has U.S. Fearing Foreign Infiltration," CNN, December 19, 2015, https://www.cnn.com/2015/12/18/politics/juniper-networks-us-government-security-hack; Emily Price, "Juniper Networks Security Flaw May Have Exposed US Government Data," *Guardian*, December 22, 2015, https://www.theguardian.com/technology/2015/dec/22/juniper-networks-flaw-vpn-government-data.

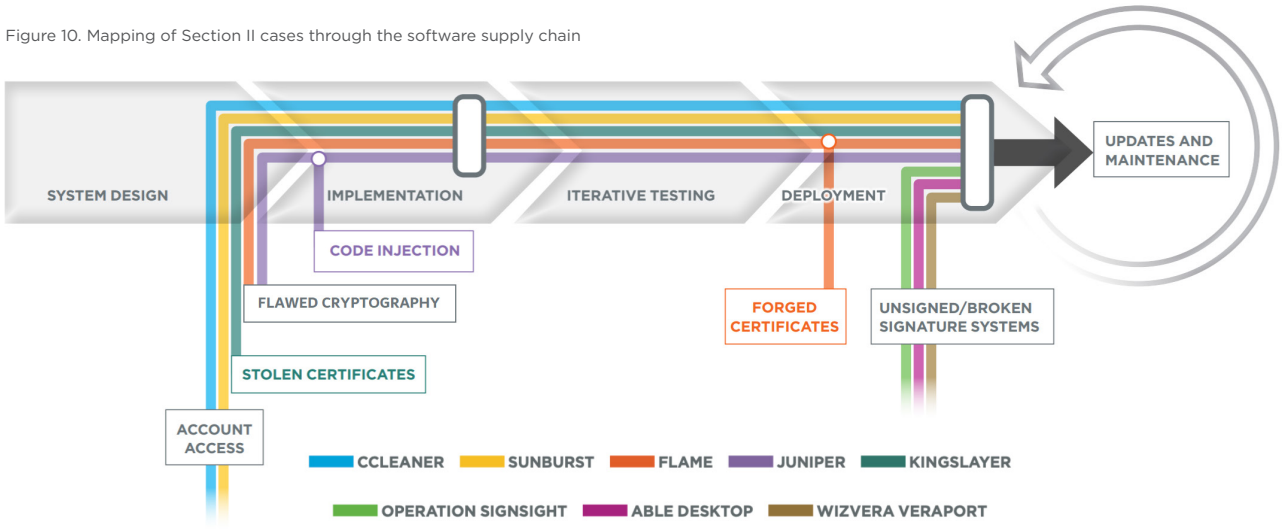
VPN. In 2006, the National Institute of Standards and Technology (NIST) released standards on an encryption algorithm developed by the NSA, called the Dual Elliptic Curve Deterministic Random Bit Generator (or Dual_EC).[67] This algorithm relies on a static value, known as "Q," to encrypt data. Juniper, under the assumption that Dual_EC_DRBG was safe, began to ship its products using a Juniper-specific "Q" value sometime between 2008 and 2009.[68]

Originally, Juniper planned to use the Dual_EC_DRBG algorithm alongside another encryption algorithm to ensure product security. But, for some unknown reason, the second encryption algorithm was not included in the software, so Juniper products relied solely and by default on Dual_EC_DRBG for encryption. In 2012, unbeknownst to Juniper, malicious actors infiltrated Juniper's software-development process and changed the aforementioned "Q" static value to one they knew. This alteration allowed them to intercept and eavesdrop on sensitive communications by organizations using Juniper VPNs shipped after August 2012. At the time, Juniper's clients for this product included the Department of Defense, Department of Justice, the Federal Bureau of Investigation, and the Department of the Treasury. It is unclear how much, if any, data was exfiltrated using this exploit. However, honeypots created after the vulnerability's discovery indicated that the attackers were active. The exploit's discovery in December 2015 meant that the attackers were able to eavesdrop on "VPN-protected" communications for three years.[69]

According to leaked materials, the NSA was well aware of this "Q" static value backdoor in the Dual_EC_DRBG encryption algorithm and may have intentionally left it there for its own signals-intelligence purposes. The Juniper networking equipment is used in many target countries—such as Pakistan, Yemen, and China—making the backdoor highly valuable to

Atlantic Council

Figure 10. Mapping of Section II cases through the software supply chain



67 Elaine Barker and John Kelsey, "Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised), NIST Special Publication 800-90," National Institute of Standards and Technology, March 2007, https://projectbullrun.org/dual-ec/documents/SP800-90revised_March2007.pdf.

68 "'Backdoor' Computer Hack May Have Put Government Data at Risk," CBS News, December 19, 2015, https://www.cbsnews.com/news/juniper-technologies-computer-hack-could-put-government-data-at-risk/; "TechLibrary," Juniper Networks, https://www.juniper.net/documentation/en_US/release-independent/screenos/information-products/pathway-pages/netscreen-series/product/; Sen. Ron Wyden, et al., "Letter to The Honorable General Paul M. Nakasone," United States Congress, January 28, 2021, https://www.wyden.senate.gov/imo/media/doc/012921%20Wyden%20Booker%20Letter%20to%20NSA%20RE%20SolarWinds%20Juniper%20Hacks.pdf; Kim Zetter, "Researchers Solve Juniper Backdoor Mystery; Signs Point To NSA," *Wired*, December 12, 2015, https://www.wired.com/2015/12/researchers-solve-the-juniper-mystery-and-they-say-its-partially-the-nsas-fault/.

69 Justin Katz, "Lawmakers Press NSA for Answers about Juniper Hack from 2015," *FCW*, January 31, 2021, https://fcw.com/articles/2021/01/31/juniper-hack-algo-nsa-letter.aspx; Evan Kovacs, "Backdoors Not Patched in Many Juniper Firewalls," *Security Week*, January 6, 2016, https://www.securityweek.com/backdoors-not-patched-many-juniper-firewalls; Perez and Prokupecz, "Newly Discovered Hack Has US Fearing Foreign Infiltration"; Zetter, "Researchers Solve Juniper Backdoor Mystery' Signs Point to NSA."

Western intelligence agencies.[70] The Juniper hack clearly demonstrates the benefits and risks of purposefully creating backdoors in software used by US government agencies, as they may be more easily leveraged by adversaries. In the aftermath of the Sunburst campaign, senators sent a letter in February 2021 to the NSA questioning why extra software supply-chain safeguards were not put into place after the 2015 Juniper hack. Attribution for this attack is still unknown.[71]

Trendlines Leading to Sunburst

Taken together, these cases convey trends in state-backed software-supply compromises: the identification and extraction of valuable information from adversaries; the undermining of key technical mechanisms of trust to gain access and preserve operational secrecy; and the targeting of deeply privileged programs or those deployed widely across governments and industry—usually at the seams of assurance, with less-than-adequate protection. Far from an unprecedented bolt-from-the-blue attack, Sunburst echoed many of these trends as a supply-chain compromise while adding a highly effective focus on the seams of security in cloud deployments and on-premises identity systems. Unfortunately for the organizations targeted, these supply-chain lessons went largely unheeded, and much of what might have been done to limit the harm of these cloud-focused techniques happened late, or not at all.

The following analysis synthesizes, for each case the types of software targeted, the respective adversary's tactics and intent, and the immediate implications of the incident, without presenting an exhaustive dissection of each. In Figure 10, this report overlaid each intrusion to directly compare them to each other, and Sunburst, along the same notional model of the software supply chain and development lifecycle.

The Contest for Information

Over the past decade, there have been at least one hundred and thirty-eight software supply-chain attacks or vulnerability disclosures. Thirty of these are tied to states—four, including Sunburst, are linked to Russia, versus eight to China.[72]

The Flame, VeraPort, CCleaner, and Able Desktop operations all provided their operators with stealthy means to infiltrate sensitive networks and access systems without detection for months, if not years.[73] The Flame malware was able to control infected machines' internal microphones to record conversations, siphon contact information via nearby Bluetooth devices, record screenshots, and manipulate network devices to collect usernames and passwords.

The Sunburst designers included some similar capabilities, such as transferring and executing files on affected systems, which gave them the ability to exfiltrate large amounts of information from targets over the course of months.[74] Intruders appear to have accessed SolarWinds' corporate networks and infiltrated the company's build infrastructure as early as September 2019, through still-unconfirmed means.

A key aspect of the intelligence contest is not only the acquisition of information, but a combination of data collection, data denial, and securing access to target networks that allows actors to more effectively maneuver around adversary defenses, in and outside of cyberspace, and preposition capabilities for future use. Triton, not mentioned above, serves as a good example of prepositioning. Intruders in the Triton case first gained access to the plant's networks through a poorly secured engineering workstation, before then moving to a computer that controlled a number of physical safety systems using a previously unknown

70 "Assessment of Intelligence Opportunity—Juniper," Intercept DocumentCloud, February 3, 2011, https://beta.documentcloud.org/documents/2653542-Juniper-Opportunity-Assessment-03FEB11-Redacted; Ryan Gallagher and Glenn Greenwald, "NSA Helped British Spies Find Security Holes In Juniper Firewalls," *Intercept*, December 23, 2015, https://theintercept.com/2015/12/23/juniper-firewalls-successfully-targeted-by-nsa-and-gchq; Nicole Perlroth, Jeff Larson, and Scott Shane, "N.S.A. Able to Foil Basic Safeguards of Privacy on Web," *New York Times*, September 5, 2013, https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all&_r=1.

71 Wyden, et al., "Letter to The Honorable General Paul M. Nakasone."

72 Herr, et al., *Breaking Trust*, https://www.atlanticcouncil.org/resources/breaking-trust-the-dataset.

73 Zetter, "Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers"; Ravie Lakshmanan, "Trojanized Security Software Hits South Korea Users in Supply-Chain Attack," *Hacker News*, November 16, 2020, https://thehackernews.com/2020/11/trojanized-security-software-hits-south.html; Martin Brinkmann, "CCleaner Malware Second Payload Discovered," *GHacks Technology News*, September 21, 2017, https://www.ghacks.net/2017/09/21/ccleaner-malware-second-payload-discovered; Cimpanu, "Chinese APT Suspected of Supply Chain Attack on Mongolian Government Agencies."

74 "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor," FireEye, December 13, 2020, https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html.

software vulnerability, or zero-day.[75] This vulnerability enabled the malware to alter the system design by accessing supervisor privileges to inject the malware payload into the firmware, as well as modify a piece of administrative software running on the computer. This software, called Trixonex, linked the computer to a number of physical control and safety systems. The malware enabled intruders to read, write, and execute commands inside the safety-control network, which triggered two shutdowns in June and August 2017, leading to the operation's unmasking and obscuring its final stages from discovery.[76]

Despite the lack of final-stage execution, the accessed privileged information about the plant created the possibility for the intruders to create real physical harm. In a worst-case scenario, the access the intruders had before their discovery would have allowed them to trigger explosions causing casualties both at the plant and in surrounding areas.[77] Safety instrumented systems are not unique to petrochemical powerplants in Saudi Arabia; they secure everything from transportation systems to nuclear powerplants. The execution of such an action would fall outside the realm of espionage operations, but the preparation for it demands exquisite information about a target system. These intrusions, once discovered, no longer provided tangible espionage capabilities, but the preparation for such an eventuality constitutes prepositioning. If the intent of Triton was to prove a potential destructive capability, it succeeded.

Tactics: Run Silent, Run Deep

For most of the studied cases, intruders' key point of entry to their targets was the circumvention of code-signing protections to compromise software. From there, intruders moved laterally throughout the networks they could access via the initial infection. Among these eight total cases (including Sunburst), a diversity of techniques was employed to break, evade, or abuse the protections of these signatures. Flame managed to solve the significant mathematical problem of breaking the cryptographic protections of a certificate that granted excessive permissions in order to target individual users. Juniper exploited backdoors in an encryption standard on private networks meant to protect classified government communications. Others opted for more cost-efficient, less demanding techniques, such as stealing legitimate code-signing certificates (VeraPort)[78] or compromising build servers to inject code prior to signing (CCleaner).[79] At the other end of the spectrum, some compromises relied on shortcomings already present in code-integrity protections by targeting unsigned software, programs with signatures that had already failed verification, or systems that did not fully authenticate certificates.

Each of the intruders in these cases used varying methods to remain unobserved, though Flame and Sunburst evidenced particular sophistication in their methods, including operational restraint in where they deployed. The Sunburst operators gained an intelligence foothold in US government agencies and leading technology companies for as long as nine months. To achieve this intelligence objective, Sunburst operators prioritized stealth in their malware design, having its communications masquerade as legitimate network traffic and sent out in sparing intervals.[80]

75 "Triton Malware Is Spreading," Cyber Security Intelligence, March 19, 2019, https://www.cybersecurityintelligence.com/blog/triton-malware-is-spreading-4177.html; Nimrod Stoler, "Anatomy of the Triton Malware Attack," CyberArk, February 8, 2018, https://www.cyberark.com/resources/threat-research-blog/anatomy-of-the-triton-malware-attack; Martin Giles, "Triton Is the World's Most Murderous Malware, and It's Spreading," *MIT Technology Review*, March 5, 2019, https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware.

76 Stoler, "Anatomy of the Triton Malware Attack"; "Triton Malware Is Spreading," Cyber Security Intelligence.

77 Giles, "Triton Is the World's Most Murderous Malware, and It's Spreading"

78 Osborne, "Lazarus Malware Strikes South Korean Supply Chains."

79 Lily Hay Newman, "Inside the Unnerving CCleaner Supply Chain Attack," *Wired*, April 17, 2018, https://www.wired.com/story/inside-the-unnerving-supply-chain-attack-that-corrupted-ccleaner.

80 Eric Byres, "Three Things SolarWinds Supply Chain Attack Can Teach Us," Adolus, December 18, 2020, https://blog.adolus.com/blog/three-things-the-solarwinds-supply-chain-attack-can-teach-us; Sunburst actors used highly sophisticated defense evasion and persistence techniques, such as a twelve- to fourteen-day sleep timer, anti-analysis techniques, and modular and staged approach to infection. See: Tom Kellerman and Greg Foss, "Iron Rain: Understanding Nation-State Motives and APT Groups," VMWare, February 2021, https://www.carbonblack.com/resources/iron-rain-understanding-nation-state-motives-and-apt-groups.

Despite operating over a multitude of targets, the Sunburst intruders maintained significantly high levels of operational security to avoid discovery. The Sunburst malware landed in its prospective targets and waited, patiently, for two weeks before initiating any activity. The intruders went to great lengths to avoid detection, masquerading as legitimate SolarWinds network traffic, hiding in the operations of other software and scheduled tasks, and downloading additional malicious functionality/payloads, like Teardrop, which were never stored on disk. Avoiding detection gave intruders time to choose whom they wished to fully compromise. While none of these techniques is entirely new, they represent significant technical investment and operational patience. The Sunburst intruders also showed serious precision in their targeting. Although the initial infection vectors cast a wide net, follow-on operations appeared deliberate and precise.[81]

Designing stealthy malware is integral to the success of an espionage operation. As Kevin Mandia, CEO of FireEye, said of the actor behind Sunburst in his statement to the US Senate Select Committee on Intelligence, "Everything about this aligned to a threat actor who…was more concerned about operational security than mission accomplished."[82] Remaining hidden allows an intruder the time and space to employ espionage capabilities and fulfill its strategic ends. Most of these operations enjoyed lengthy periods of operation between their initial compromise and discovery.

Bounding the Blast Radius

Many of these cases share a key characteristic—the compromised codebases were widely used, or otherwise required software with significant default permissions; this class of software provided ready access to target networks with massive economies of investment. This efficiency makes software supply chain attacks particularly compelling, and, despite the identified one hundred and thirty-eight events over the last decade, there are doubtless more that have yet to emerge. The Sunburst campaign targeted network-monitoring software widely used across industry and government, while CCleaner leveraged an immensely popular administrative tool. VeraPort managed access to secure websites and authenticating users, and SignSight exploited Vietnamese government-managed cryptographic software employed throughout the country. The necessity or commonality of this software creates points of failure that users of the underlying service cannot avoid, allowing intruders to funnel themselves toward end targets.[83]

Many of these software supply-chain campaigns also targeted administrative and security tools because of their significant permissions and frequent presence on devices not subject to the same security evaluation as standard endpoints. Kingslayer undermined a frequently downloaded log-analysis tool for IT administrators. Triconex, targeted in the Triton campaign, coordinated operations at large industrial facilities.

81 "Deep Dive into the Solorigate Second-Stage Activation: From SUNBURST to TEARDROP and Raindrop," Microsoft, 2021, https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/; Lucian Constantin, "SolarWinds Attack Explained: And Why It Was so Hard to Detect," CSO Online, December 15, 2020, https://www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html. The operations were narrowly tailored at the per-victim and per-host level including "unique Cobalt Strike configurations, file naming conventions, and other artifacts of adversary behaviors." Joe Slowik, "Change in Perspective on the Unity of SUNBURST-related Network Indicators," DOMAINTOOLS, January 22, 2021, https://www.domaintools.com/resources/blog/change-in-perspective-on-the-utility-of-sunburst-related-network-indicators. The intruders also tailored their command-and-control infrastructure, including unique domains and hosting IPs, to further obscure their operations from defenders.

82 US Congress, Senate, Select Committee on Intelligence, "Hearing on the Hack of U.S. Networks by a Foreign Adversary," 117th Congress, February 23, 2021, https://www.intelligence.senate.gov/hearings/open-hearing-hearing-hack-us-networks-foreign-adversary.

83 Herr, et al., *Breaking Trust*; Cimpanu, "SEC Filings: SolarWinds Says 18,000 Customers Were Impacted by Recent Hack"; Alina Bradford, "CCleaner Hack Affects 2.27 Million Computers, Including Yours?" CNET, September 19, 2017, https://www.cnet.com/how-to/ccleaner-was-hacked-heres-what-to-do-next; "Operation StealthyTrident: Corporate Software under Attack"; Osborne, "Lazarus Malware Strikes South Korean Supply Chains"; "Vietnam Targeted in Complex Supply Chain Attack," OODA Loop, December 28, 2020, https://www.oodaloop.com/briefs/2020/12/28/vietnam-targeted-in-complex-supply-chain-attack/; "Electronic Signature Laws & Regulations—Vietnam," Adobe Help Center, September 22, 2020, https://helpx.adobe.com/sign/using/legality-vietnam.html; Ignacio Sanmillan and Matthieu Faou, "Operation SignSight: SupplyChain Attack against a Certification Authority in Southeast Asia," WeLiveSecurity, December 17, 2020, https://www.welivesecurity.com/2020/12/17/operation-signsight-supply-chain-attack-southeast-asia.

Hijacked updates already enjoy the ability to reach deep into systems, and many of the software programs targeted in other cases had even greater proximity to sensitive functions in their host networks.

Some incursions also leveraged, or attempted to leverage, multiple points of entry to reach their desired targets. In cyberspace, as in any open system, the principle of equifinality applies, meaning that a given end state is attainable through a multitude of paths. The choice to identify and exploit several vectors increases the chance for the discovery of an operation. Both strong and weak actors often use multiple vectors not to compensate for a lack of ability, but to multiply existing ability. The actors responsible for Sunburst did not build their strategy around the weaknesses of SolarWinds, but targeted that software due to its wide connections with technology companies and government entities. In the majority of cases, the focus of these intruders appears instead to have been organization's email and productivity tools, including Microsoft's SaaS suite—Office 365.[84] SolarWinds served as an important vector—one of several—to that end.

"MANY OF THESE SOFTWARE SUPPLY-CHAIN CAMPAIGNS ALSO TARGETED ADMINISTRATIVE AND SECURITY TOOLS BECAUSE OF THEIR SIGNIFICANT PERMISSIONS AND FREQUENT PRESENCE ON DEVICES NOT SUBJECT TO THE SAME SECURITY EVALUATION AS STANDARD ENDPOINTS."

84 "Modernizing the Federal Civilian Approach to Cybersecurity," hearing before the House Appropriations Committee, Subcommittee on Homeland Security, 117th Congress, March 10, 2021, testimony of Brandon Wales, acting director of the Cybersecurity and Infrastructure Security Agency, YouTube, 24:10, https://youtu.be/ccEAuemkgdY?t=1450.

III — CONTRIBUTING FACTORS TO SUNBURST

At its heart, Sunburst was an expansive intelligence-gathering campaign, characterized by long-running reconnaissance and preparation, persistent compromise of a variety of systems and victims, and stealthy operation throughout. Though mature organizations assume a compromise is inevitable, especially in the face of better resourced and skilled adversaries, more could have been done to discover and mitigate the Sunburst campaign. The issue is not that the adversary got through, but that it roamed so freely, so far, and for so long.

This section analyzes the defining characteristics of Sunburst with themes from the previous cases to understand the operations' success against key points of failure in government and industry: a lack of effective risk prioritization, shortfalls in the defensibility of linchpin cloud infrastructure, ineffective operational collaboration, and a brittle federal cyber risk-management apparatus. None of these failures is existential, and all offer opportunities for reform by policymakers and industry.

In evaluating Sunburst, problems emerge in (at least) three areas.

1. DEFICIENCIES IN RISK MANAGEMENT

Federal enterprise risk management leans more heavily toward "management" than risk. The .gov and .mil environments are unusually challenging environments to secure. They are wildly uneven landscapes of technology versions, use cases, governance structures, and resources. What standards are present are often poorly implemented, and the programs underachieving. Better risk prioritization will account for this challenge, but it must be ruthless.

2. HARD-TO-DEFEND LINCHPIN CLOUD TECHNOLOGIES

Many in industry failed to adequately share responsibility for the security of their products. For vendors like SolarWinds, and in most of the other cases surveyed for this report, especially Kingslayer and SignSight, this will require better securing development environments as well as improving the security of software deployments. The major cloud providers—Microsoft in this instance, but also Amazon and Google—can work to make linchpin technologies like IAM services more defensible, in line with changing adversary behavior.

3. LIMITED SPEED AND POOR ADAPTABILITY

Federal supply-chain security policies change too slowly to keep up with the landscape of supply-chain risk, especially in software. The federal government must reform itself to better adapt supply-chain security policies without the need for significant shifts in authorities or wholesale new programs.

Deficiencies in Risk Management

Having a robust system for identifying High Value Assets (HVAs) and the tools needed to protect them is a critical start to minimizing future risk and assessing what data and systems comprise the HVAs that already exist in federal agencies. In 2016, the Office of Management and Budget (OMB) put out a memorandum defining HVAs as federal information systems and data for which unauthorized access could cause a significant impact to US national security, among other characteristics. CISA has circulated further guidance to government agencies and private-sector organizations alike to consider interconnectivity and dependencies in assessments of what constitutes an HVA.[85]

The Department of Homeland Security (DHS), through CISA's Continuous Diagnostics and Mitigation Program (CDM), was supposed to provide an incisive look into the security posture of all federal agencies, but, as Sunburst illustrated, it somewhat unsurprisingly failed to meet expectations. Since 2012, CDM has sought to standardize security procedures and frameworks across federal civilian agencies.[86] Despite the relatively long program duration, several of its key metrics went unmet, severely limiting what CISA could have known and, therefore, done. Continuous monitoring of network behavior relies on assessing which metrics provide valuable checks on network integrity, and the practice can play a key role in compromise detection and mitigation. In the case of SolarWinds, continuous monitoring applied thoroughly could have detected mismatches in login and authentication requests in Azure Active Directories or picked up on the creation of new trust entities, alerting targets to attacker behavior—if the metric was correctly identified. Information about agency implementation is sparse.[87]

Federal agencies have instructions to maintain awareness of the value of systems not just from their own perspectives, but also from the perspectives of malicious actors. OMB outlined a framework for agencies to identify and prioritize HVAs based on risk factors such as adversary intent. Orion's pervasiveness across government agencies, depth of access, and proximity to valuable information make the software the archetype of this type of system. The CISA page in support of OMB specifically gives the example that "if the authentication solution for an HVA is the organization's centralized Active Directory solution then the Active Directory solution may also be considered an HVA due to critical dependency."[88]

CDM's Asset Management and Network Security Management programs are supposed to track each agency's security-management configurations and supply-chain risk-management programs. This promise has yet to be fully realized. For example, on the hardware side, because of numerous miscommunications with contractors, individual agencies faced difficulty in registering devices with the CDM system. Without proper device registration, CDM is unable to get the full picture of an agency's network (and, subsequently, the federal government's network), leaving gaps for adversaries to exploit. CISA was aware of this failure in March 2019, but, as late as August 2020, the hardware issue was still without a resolution.[89]

On the software side, CDM's software asset-management tools caused the Small Business Administration's

85 Shaun Donavan, "Memorandum for Heads of Executive Departments and Agencies: Management of Federal High Value Assets, M-17-09," Executive Office of the President, Office of Management and Budget, December 9, 2016, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-09.pdf; "CISA Insights: Secure High Value Assets (HVAs)," US Department of Homeland Security, Cyber and Infrastructure Security Agency, accessed March 1, 2021, https://www.cisa.gov/sites/default/files/publications/CISAInsights-Cyber-SecureHighValueAssets_S508C.pdf.

86 "Continuous Diagnostics and Mitigation (CDM)," Cybersecurity and Infrastructure Security Agency, accessed March 1, 2021, https://www.cisa.gov/cdm; "CDM Program Overview," Department of Homeland Security, Cyber and Infrastructure Security Agency, accessed March 1, 2021, https://www.cisa.gov/sites/default/files/publications/2020%2009%2003_CDM%20Program%20Overview_Fact%20Sheet_1.pdf.

87 "Sygnia Advisory: Detection of Golden SAML Attacks," Sygnia, December 2020, https://www.sygnia.co/golden-saml-advisory.

88 "Secure High Value Assets," Cybersecurity and Infrastructure Security Agency, accessed March 1, 2021, https://www.cisa.gov/publication/secure-high-value-assets.

89 Dave Nyczepir, "No Agency Has Implemented Every Key CDM Requirement, Seven Years Later," *FedScoop*, August 19, 2020, https://www.fedscoop.com/agency-cdm-requirement-implementation/; "Cybersecurity: DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program, GAO-20-598," US Government Accountability Office, 2020, 70, https://www.gao.gov/assets/710/708885.pdf.

devices to crash frequently, requiring the agency to abandon the monitoring program entirely.[90] Operating systems and software not documented by CDM were simply left unsecured and viewed as a low priority, although threat vectors could very well infiltrate through those devices. And, even though the CDM system presents a helpful dashboard populated with agency-specific threat information and security priorities, agency officials reported that the quality of information was poor.[91] A potentially useful program to detect and mitigate Sunburst was insufficient for the task.

CISA's EINSTEIN program does monitor inbound and outbound traffic to federal-agency networks. Though it was circumvented in the SolarWinds incident, the program could be significantly improved and updated toward a more allow-list-oriented screening process and in-network auditing.[92] Nonetheless, any delay and cost it imposed by forcing the adversary to circumvent it can be viewed as moderate successes.

Importantly, when it comes to better risk prioritization, continuous-monitoring regimes are no panacea. Continuous monitoring is used somewhat interchangeably to describe a set of objects all under a broad approach to security—monitoring of compliance, monitoring of risk assessment and security posture, monitoring network behavior, and monitoring dependencies—all of which deserve discussion. Though requiring different tools and applied at different levels by different entities, each of these aims is critical to effective supply-chain risk management. Compliance monitoring can be jointly undertaken by agencies requiring compliance, auditors ensuring it, and vendors maintaining it. The Federal Risk and Authorization Management Program (FedRAMP), Federal Information Security Modernization Act (FISMA), Cybersecurity Maturity Model Certification (CMMC), etc., are moving toward, or have implemented, continuous monitoring as a supplement to periodic review.

Risk-assessment monitoring occurs within agencies and vendors analyzing their exposure to known vulnerabilities and threats. NIST guidelines emphasize continuous monitoring, even providing a dedicated special publication for the topic (SP 800-137), aimed at federal organizations and information systems and dating back to at least 2011.[93] It focuses on the practice of assessing "security control effectiveness and of organizational security states," though federal integration of its processes is incomplete and unclear. The 2018 Annual FISMA Report to Congress indicated that seventeen of twenty-three primary federal civilian agencies had implemented such practices.[94] In either case, the practice was likely a victim of vague guidelines and subjective self-assessment. Agencies, especially those capable of more automation, should more extensively implement the NIST guidelines.

Even more broadly, agency-wide ICT supply-chain risk-management practices could have created a faster and more comprehensive incident response, but—at least within the federal government—they are chronically underdeveloped. A recent General Accounting Office (GAO) report, 21-171, found that just five of twenty-three examined federal civilian agencies had fully or partially established agency-wide ICT supply-chain risk-assessment processes in compliance with seven identified foundational best practices.[95]

Existing certification and authorization regimes also lag behind the use of their considered software. In SolarWinds' case, Orion is on the Department of Defense Information Networks (DoDIN) Approved Products List (APL), along with many other certifications and approvals for both the product and its vendor.[96] Placement on the APL is a laborious, months-long process, which, in theory, reviews major updates

90 "Cybersecurity: DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program."

91 Ibid.

92 Justin Katz, "Does Einstein Need a Post-SolarWinds Makeover?" *FCW*, February 1, 2021, https://fcw.com/articles/2021/02/01/einstein-rethink-supply-chain-hack.aspx; "The EINSTEIN Program," Cybersecurity and Infrastructure Security Agency, accessed March 1, 2021, https://www.cisa.gov/publication/einstein-program.

93 "NIST Publishes Final Guidelines for Protecting Sensitive Government Information Held by Contractors," National Institute of Standards and Technology, January 8, 2018, https://www.nist.gov/news-events/news/2015/06/nist-publishes-final-guidelines-protecting-sensitive-government-information.

94 "Federal Information Security Modernization Act Fiscal Year 2018 Annual Report to Congress," Executive Office of the President of the United States, Office of Management and Budget, 2018, https://www.whitehouse.gov/wp-content/uploads/2019/08/FISMA-2018-Report-FINAL-to-post.pdf.

95 "Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks, GAO-21-171," US Government Accountability Office, 2020, https://www.gao.gov/assets/gao-21-171.pdf.

96 "SolarWinds Orion Suite V3.0 Added to DoDIN APL: SolarWinds," SolarWinds Government, accessed March 1, 2021, https://www.solarwinds.com/federal-government/solution/dodin-apl.

to deployed systems. However, the disconnect between a vendor's intent for an update and an attacker's ability to exploit it means that "minor" releases can conceal major compromises. Throughout government schema for protecting acquired software, the review of updates and the periodic nature of certification audits mean that security cannot keep pace with threats, even as various programs strive for more frequent checks. An increase in the frequency and depth of these evaluations, in turn, could have improved government reaction to Sunburst, and would require that agencies know better what software requires scrutiny by the nature of its use and its proximity to valuable information.

These shortcomings in risk prioritization and supply-chain risk management, the slow and encumbered bureaucratic response in the face of a patient and persistent adversary, and failures in basic, important security tools are not new—nor is the adversary's targeting of widely used software with significant permissions on victim networks. Federal practices could have stymied the spread of Sunburst more quickly and more thoroughly. Lateral movement could have been reduced, post-compromise information disseminated among agencies quicker, and individual agencies could have detected, aggregated information about, and acted on aberrant behavior faster. Should Orion have been classified as a high-priority program, its network traffic may have been monitored better and updates checked more rigorously—even SolarWinds, the vendor itself, may have been subjected to better cyber-hygiene requirements that would have alerted government clients to issues such as its much-publicized insecure update server.[97] With better knowledge about its critical assets, and a better organizational framework for assessing related security postures, the government will also be better situated to widen the aperture of its authorizations.

Hard-to-Defend Linchpin Cloud Technologies

With the widening adoption of cloud computing, major providers have become uniform in their evangelism of the "shared responsibility" model. Users must play a role in securing even the most hands-off cloud technologies by determining factors like user roles and the classification of data, which the provider's technology can then enforce.

Shared responsibility is a useful model, but it comes with three important caveats. First, shared responsibility masks the uneven maturity of organizations and technologies on the user side of that shared line, producing much more of a zigzag than a clean line of responsibility. Second, all cloud deployments rely on certain linchpin technologies on which every other security program or critical resource depends. As cloud computing becomes ever more widely used, the potential harm for such a failure in a linchpin system like IAM, secrets management, or host virtualization grows. These services cannot fail; and in the rare instances where they do, they must fail with uncommon grace. Cloud providers must be conscious of weaknesses in the assumptions they make about their architecture and its relationship with users. Exploitable flaws or soft spots in design and concept will not always present themselves as categorizable vulnerabilities.

Cloud service providers take on the obligation to secure these linchpins, but the threats they envision, and thus design against, must keep pace with real-world adversary behaviors—including some low-probability, high-consequence events, which may demand costly and inconvenient choices.[98] Third, because providers build the products and services for which users are obligated to share responsibility, providers must make those systems straightforward to both use and defend. Otherwise, responsibility is abdicated more than shared, and the model breaks.

In the case of Sunburst, a large-scale software supply-chain attack became a full-blown crisis when the adversary successfully abused several Microsoft IAM products. This abuse, which was sustained despite including techniques known to the security community for years, helped the adversary move silently across victim networks. These techniques also enabled the adversary, in a damaging turn of events, to hop from on-premises networks into Office 365 environments.

The Sunburst adversary worked to abuse Microsoft IAM products to move throughout victim organizations in nearly every case catalogued by FireEye.[99]

97 Thomas Claburn, "We're Not Saying This Is How SolarWinds Was Backdoored, but Its FTP Password 'Leaked on GitHub in Plaintext,'" *Register*, December 16, 2020, https://www.theregister.com/2020/12/16/solarwinds_github_password.

98 Dan Patrick, "Is Azure Active Directory Microsoft's Weakest Link?" Build 5 Nines, September 29, 2020, https://build5nines.com/is-azure-active-directory-microsofts-weakest-link/.

99 "Remediation and Hardening Strategies for Microsoft 365 to Defend Against UNC2452."

Microsoft Azure's IAM system is Azure Active Directory (AAD). It authenticates users for Office 365 and Azure, the Software as a Service (SaaS) and Platform/Infrastructure as a Service (PaaS/IaaS) offerings, respectively, of the Redmond giant.[100] AAD is not to be confused with Active Directory (AD), an IAM for on-premises networks that does not authenticate for cloud applications.[101] Often, organizations opt to avoid the administrative hassle of having two sets of credentials separately stored on both AAD and AD for each employee and connect the two using one of several products, including Active Directory Federated Services (ADFS).[102]

The Sunburst operators targeted a variety of these products. With AAD, they modified authentication requirements, rewrote access controls, and abused highly privileged accounts to access resources across organizations. In the case of ADFS, the adversary stole certificates to create its own identities and bypass multi-factor authentication requirements and other safeguards designed to stop the intrusion.[103] While Azure Active Directory Connect has not been directly implicateddirectly implicated, it is reasonable to assume that malicious actors with access to on-premises AD services may have simply moved laterally into the connected Azure cloud environment, a technique previously demonstrated by security researchers.[104] The adversary used the stolen signing certificates to grant itself access to sensitive resources while bypassing multi-factor authentication safeguards, including direct access to dozens of email accounts in Office 365 (and the ability to view thousands more).[105] This kind of targeting of IAM services is not novel to Sunburst, nor new. One of the attacks on ADFS, referred to as Golden SAML, was known at least as far back as 2017.[106] FireEye flagged an increase in compromises against AAD and Office 365 just a few months before

100 For more on the SaaS of cloud computing and some background on these technologies, see: Simon Handler, et al., *Dude, Where's My Cloud? A Guide for Wonks and Users*, *Atlantic Council*, September 28, 2020, https://www.atlanticcouncil.org/in-depth-research-reports/report/dude-wheres-my-cloud-a-guide-for-wonks-and-users.

101 Aymeric Palhière, et al., "Azure AD Introduction for Red Teamers," Synacktiv, April 20, 2020, https://www.synacktiv.com/en/publications/azure-ad-introduction-for-red-teamers.html.

102 "What Is Federation with Azure AD?" Microsoft, https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed; "What's the Difference between AD vs Azure AD?" Compete366, November 20, 2020, https://www.compete366.com/blog-posts/the-difference-between-ad-and-azure-ad-explained/; Danny Murphy, "The Difference Between Windows Active Directory and Azure AD," Lepide Blog: A Guide to IT Security, Compliance and IT Operations, May 14, 2020, https://www.lepide.com/blog/the-difference-between-windows-active-directory-and-azure-ad/; "Deep-Dive to Azure Active Directory Identity Federation," Office365 Blog, June 12, 2019, https://o365blog.com/post/aad-deepdive.

103 Wray, "SolarWinds Post-Compromise Hunting with Azure Sentinel"; Sentonas, "CrowdStrike Launches Free Tool to Identify & Mitigate Risks in Azure Active Directory"; Brad Smith, "Strengthening the Nation's Cybersecurity: Lessons and Steps Forward Following the Attack on SolarWinds," written testimony to the Senate Select Committee on Intelligence, 2021, https://www.intelligence.senate.gov/sites/default/files/documents/os-bsmith-022321.pdf; Weinert, "Understanding Solorigates' Identity IOCs—for Identity Vendors and Their Customers," Microsoft, 2021, https://techcommunity.microsoft.com/t5/azure-active-directory-identity/understanding-quot-solorigate-quot-s-identity-iocs-for-identity/ba-p/2007610. Jai Vijayan, "SolarWinds Campaign Focuses Attention on 'Golden SAML' Attack Vector," Dark Reading, December 22, 2020, https://www.darkreading.com/attacks-breaches/solarwinds-campaign-focuses-attention-on-golden-saml-attack-vector/d/d-id/1339794. In some cases, these certificates were used to forge Security Assertion Markup Language (SAML) tokens, which are digital passports containing a user's identity and permissions. This forgery is called the "Golden SAML" technique. Kurt Mackie, "CrowdStrike Exec Points to Active Director 'Structural Problems' in Senate Solarigate Hearing," Redmond, February 26, 2021, https://redmondmag.com/articles/2021/02/26/crowdstrike-active-directory-structural-problems.aspx. Golden SAML capitalizes on users' inadequate defense of these cryptographic secrets, which appears to have been made far more likely because of poor out-of-the-box configurations. These product limitations also made this abuse difficult to detect. Joseph Menn, "Microsoft Failed to Shore Up Defenses that Could Have Limited SolarWinds Hack: U.S. Senator," Reuters, February 25, 2021, https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AP2XD. Microsoft asserted that it has only observed this Golden SAML technique in 15 percent of incidents, though without specifying the sensitivity of the accounts targeted or the organizations impacted.

104 Tim Anderson, "Malwarebytes Says Its Office 365, Azure Tenancies Invaded by SolarWinds Hackers, Insists Its Tools Are Still Safe to Use," *Register*, January 21, 2021, https://www.theregister.com/2021/01/20/malwarebytes_solarwinds_hack_latest/; Dirk-Jan Mollema, "I'm in Your Cloud, Reading Everyone's Emails," TROOPERS21, March 20, 2019, https://troopers.de/troopers19/agenda/y3nswp/; "Remediation and Hardening Strategies for Microsoft 365 to Defend Against UNC2452"; Eric Saraga, "Azure Skeleton Key: Exploiting Pass-Through Auth to Steal Credentials," Inside Out Security, November 19, 2020, https://www.varonis.com/blog/azure-skeleton-key.

105 Schwartz and Ross, "US Treasury Suffered 'Significant' SolarWinds Breach."; Catalin Cimpanu, "SolarWinds Fallout: DOJ Says Hackers Accessed Its Microsoft O365 Email Server," *ZDNet*, January 6, 2021, https://www.zdnet.com/article/solarwinds-fallout-doj-says-hackers-accessed-its-microsoft-o365-email-server/.

106 Shaked Reiner, "Golden SAML: Newly Discovered Attack Technique Forges Authentication to Cloud Apps," CyberArk, November 21, 2017, https://www.cyberark.com/resources/threat-research-blog/golden-saml-newly-discovered-attack-technique-forges-authentication-to-cloud-apps.

news of Sunburst broke (and roughly a year after SolarWinds was first compromised).[107] While not used in every compromise, the Golden SAML technique was difficult to detect, and still sufficiently impactful to allow the adversary to bypass multi-factor authentication (MFA) protections and continue to work after a password change.[108]

This GoldenSAML technique was not the only one used to bypass MFA. Within AAD, cloud applications have unique permission profiles, called Application Permissions, which these applications to interface with Office 365 products.[109] If an adversary manages to commandeer a cloud application, then they can take advantage of its equipped permissions. In the Sunburst campaign, the adversary first conducted reconnaissance to determine which applications were bestowed with powerful permissions (e.g., permission to access all emails for backup).[110] Using a compromised account (such as an Application Administrator), the adversary added unauthorized certificates to the identified applications, then impersonated these applications to gather intelligence, avoiding MFA protections entirely.[111]

In Microsoft's response to Sunburst, the company recommended numerous best practices and configurations, some of which could have been implemented by default and possibly have mitigated the eventual breach.[112] Microsoft may also have worsened the situation by limiting baseline security tools to upsell a more capable paid version of Azure Defender, turning it into a profit center and adding a barrier to organizational investment in security by limiting logging tools and features to higher-level licenses than those required for the identity products themselves.[113] This practice has attracted criticism from several members of Congress.[114] CrowdStrike, a security firm (and competitor to the expanding Azure/Office 365/Windows security suite), also criticized Microsoft for inadequately documenting crisis-response procedures for users and making security audits of these products technically challenging.[115]

The abuse of the cloud provider's IAM services, and of the zigzagging line of shared responsibility in mixed on-premises/cloud environments, critically differentiates Sunburst from the other software supply-chain attacks profiled in this report. This raises two important questions about the security of cloud computing services.

- Are cloud service providers doing enough to provide defensible technologies that allow their users to adequately share responsibility for their security?
- Are the threat models against which cloud service providers secure their linchpin technologies, like IAM, sufficient for the current risk landscape?

107 Mike Burns, "Detecting Microsoft 365 and Azure Active Directory Backdoors," FireEye, September 30, 2020, https://www.fireeye.com/blog/threat-research/2020/09/detecting-microsoft-365-azure-active-directory-backdoors.html; Samantha Schwartz, "SolarWinds Initially Hacked in September 2019, 3rd Malware Found," Cybersecurity Dive, January 12, 2021, https://www.cybersecuritydive.com/news/sunspot-malware-sunburst-crowdstrike-solarwinds/593215/.

108 Marcus LaFerrera, "A Golden SAML Journey: SolarWinds Continued," Splunk, January 8, 2021, https://www.splunk.com/en_us/blog/security/a-golden-saml-journey-solarwinds-continued.html; "Remediation and Hardening Strategies for Microsoft 365 to Defend Against UNC2452"; "Sygnia Advisory: Detection of Golden SAML Attacks," Sygnia Advisory: Detection of Golden SAML Attacks, December 2020, https://www.sygnia.co/golden-saml-advisory; Shaked Reiner, "Golden SAML Revisited: The Solorigate Connection," CyberArk, December 29, 2020, https://www.cyberark.com/resources/threat-research-blog/golden-saml-revisited-the-solorigate-connection.

109 "Manage App Registration and API Permission for Microsoft Graph Notifications—Microsoft Graph," Microsoft, https://docs.microsoft.com/en-us/graph/notifications-integration-app-registration.

110 "Remediation and Hardening Strategies for Microsoft 365 to Defend Against UNC2452."

111 Lior Sonntag and Dror Alon, "Behind the Scenes of the SunBurst Attack," New Stack, February 19, 2021, https://thenewstack.io/behind-the-scenes-of-the-sunburst-attack/.

112 "Customer Guidance on Recent Nation-State Cyber Attacks," Microsoft Security Response Center, December 13, 2020, https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/.

113 "Azure Security Center Free vs Azure Defender Enabled," Microsoft, March 8, 2021, https://docs.microsoft.com/en-us/azure/security-center/security-center-pricing.

114 Josephn Menn, Christopher Bing, and Raphael Satter, "Microsoft Could Reap More Than $150 Million in New Cyber Spending, Upsetting Some Lawmakers," Reuters, March 15, 2021, https://www.reuters.com/article/us-usa-cyber-microsoft-exclusive-idUSKBN2B713L; Eric Geller and Martin Matishak, "Capitol Hill Angry over Microsoft's Security Upcharge," Politico, March 15, 2021, https://www.politico.com/newsletters/weekly-cybersecurity/2021/03/15/capitol-hill-angry-over-microsofts-security-upcharge-793983.

115 Michael Novinson, "CrowdStrike Fends Off Attack Attempted By SolarWinds Hackers," CRN, December 24, 2020, https://www.crn.com/news/security/crowdstrike-fends-off-attack-attempted-by-solarwinds-hackers; Michael Sentonas, "CrowdStrike Launches Free Tool to Identify & Mitigate Risks in Azure Active Directory," Crowdstrike, December 23, 2020, https://www.crowdstrike.com/blog/crowdstrike-launches-free-tool-to-identify-and-help-mitigate-risks-in-azure-active-directory/.

Cloud computing is a multi-billion-dollar market and is rapidly growing to become a standard fixture in organizations' networks, often overlapping with on-premises infrastructure. Cloud security is no panacea, however, and organizations bring much of their same risk to these new environments while also being obligated to learn a new vocabulary of product names and functions as they deploy their data into the cloud.[116]

"COMPLICATED AND UNINTUITIVE IAM SERVICES CAN LEAD TO SECURITY MISCONFIGURATIONS AND USER DIFFICULTIES; AS A RESULT, SOME ORGANIZATIONS OPT TO SIMPLY RELY ON INSECURE DEFAULTS."

These cloud deployments rely on certain linchpin security services. For example, all cloud providers have their own IAM services that organizations use to define permissions and authentication requirements for their users, governing what resources and options they may access. As cloud computing matures, these IAM services become more customizable, and increasing customization breeds complexity that can create security and defensibility challenges not well captured by a numbered vulnerability.[117] Complicated and unintuitive IAM services can lead to security misconfigurations and user difficulties; as a result, some organizations opt to simply rely on insecure defaults. Additionally, smaller or less-resourced organizations that lack the expertise to decipher the plethora of IAM choices are more prone to mistakes and stand out as attractive stepping stones to larger targets. Cloud providers need to design IAM services that minimize complexity and maximize ease of use, to ensure consistent security and shore up the proverbial "weakest link."[118]

For instance, Amazon Web Services' (AWS) IAM can also bridge an organization's on-premises identity records and its AWS records, and users are susceptible to similar configuration mistakes.[119] In November 2020, Unit 42 at Palo Alto Networks found that a simple and easily made misconfiguration could easily leave this AWS IAM system open to compromise.[120] A 2019 McAfee report found that the complexity of one AWS storage service (Elastic Block Store) often led to data not being properly encrypted. This issue of technology that was too complex to effectively defend was also tagged as an important culprit in the 2019 Capital One breach, in which an AWS software vulnerability, coupled with Capital One's struggle to properly configure its Amazon IAM service, led to disclosure of tens of millions of user account

116 Dan Geer and Wade Baker, "For Good Measure: Is the Cloud Less Secure than On-Prem?"; Login, 2019, http://geer.tinho.net/fgm/fgm.geer.1909.pdf; "Cloud Computing Market," Markets and Markets, July 2020, https://www.marketsandmarkets.com/Market-Reports/cloud-computing-market-234.html; Handler, et al., *Dude, Where's My Cloud? A Guide for Wonks and Users*.

117 "Detecting Abuse of Authentication Mechanisms," National Security Agency, December 2020, https://media.defense.gov/2020/Dec/17/2002554125/-1/-1/0/AUTHENTICATION_MECHANISMS_CSA_U_OO_198854_20.PDF.

118 Thom Bradley, "The Role of Identity Access Management (IAM) in Raising Issues That Lead to Breaches," Nsc42, October 15, 2020, https://www.nsc42.co.uk/post/iam-role-in-breaches; US Congress, Senate, Hearing, Select Committee on Intelligence, *Hearing on the Hack of US Networks by a Foreign Adversary*, 117th Cong., 2021, https://www.intelligence.senate.gov/hearings/open-hearing-hearing-hack-us-networks-foreign-adversary.

119 Giselle Walker and E. S. Leedham-Green, "Identity Federation in AWS," Amazon, 2010, https://aws.amazon.com/identity/federation/.

120 Michael Vizard, "Palo Alto Networks Surfaces AWS API Vulnerabilities," Security Boulevard, November 23, 2020, https://securityboulevard.com/2020/11/palo-alto-networks-surfaces-aws-api-vulnerabilities/; Walker and Leedham-Green, "Identity." Unit 42 also added that organizations broadly transplanting settings from one AWS account to another may cause systemic risk. And malicious actors, once in the network, may leverage other misconfigurations to elevate their access. "Unit 42 Cloud Threat Report: Identity Security," Palo Alto Networks, 2021, https://www.paloaltonetworks.com/prisma/unit42-cloud-threat-research. Unit 42 also added that organizations broadly transplanting settings from one AWS account to another may cause systemic risk. And malicious actors, once in the network, may leverage other misconfigurations to elevate their access.

records.[121] AWS data leaks due to misconfiguration, even in smaller scale, are not uncommon.[122]

Likewise, Cloud Identity, the Google Cloud Platform (GCP) IAM service, has suffered vulnerabilities from customers' struggles to properly configure and defend their services.[123] Netskope found that even if GCP environments have MFA and hardware-stored or secured-key protections, they are still susceptible to breaches. Making matters worse, detecting such breaches using GCP's logging tools and halting these activities is reportedly difficult, requiring a third-party add-on to parse. Overall, researchers have found secure configurations of GCP's IAM service are not necessarily easy or intuitive to implement. Cloud providers often call on their customers to adopt the "principle of least privilege" when setting up security configurations and settings—only giving network entities access where they strictly need it, and defaulting to refusing access. This is easier said than done. Tweaking configurations for least privilege requires much time, trial, and error, which many organizations cannot afford.[124]

Large cloud vendors are rapidly pushing new products and features to remain competitive. But, swift cycles for innovation also increase configuration complexity, place more security responsibility on customers, and a create a major governance challenge within vendors themselves. It is one thing if a company organizes into dozens of loosely coordinated business units, but the resulting cloud deployment is a single attack surface for the adversary to locate gaps and weaknesses. Reacting to competitors quickly means less attention and fewer resources

121 "Business Home," McAfee, https://www.mcafee.com/enterprise/en-us/forms/gated-form.html?docID=59d987b2-5df5-4fa2-a6b3-f9f7c204140f; Stephen Kuenzli, "Why Are Good AWS Security Policies so Difficult?" K9 Security, September 10, 2020, https://k9security.io/posts/2020/06/why-are-good-aws-security-policies-so-difficult; "The Capital One Data Breach a Year Later: A Look at What Went Wrong and Practical Guidance to Avoid a Breach of Your Own," DivvyCloud, June 5, 2020, https://divvycloud.com/capital-one-data-breach-anniversary; Rob McLean, "A Hacker Gained Access to 100 Million Capital One Credit Card Applications and Accounts," CNN Business, July 30, 2019, https://www.cnn.com/2019/07/29/business/capital-one-data-breach/index.html; "Instance Metadata And User Data," Amazon Web Services, 2021, https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html. AWS servers use a metadata service to provide developers with information about themselves, such as their IP address and their location in the computing fabric. "AWS Security Vulnerabilities And Attack Vectors," Rhino Security Labs, 2016, https://rhinosecuritylabs.com/cloud-security/aws-security-vulnerabilities-perspective/. Crucially, metadata services grant temporary credentials that give AWS assets access to each other (the degree of access is based on an asset's permission configuration). United States of America v. Paige A Thompson (United States District Court for the Western District of Washington at Seattle July 29, 2019), https://www.documentcloud.org/documents/6224689-Capital-One-breach-criminal-complaint.html?_ga=2.161157560.461983242.1614828418-1927355329.1614828418. Because of a firewall misconfiguration, the attacker was freely able to send commands to this privileged metadata service. The attacker first requested the "role name" of the server she accessed. The metadata service complied with this request and returned the string "ISRM-WAF-Role." Hazel Virginia Whitehouse-Grant-Christ, "IAM Roles," Amazon, 2011, https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html. Roles are granular permission settings and labels defining what AWS assets can and cannot do. "A Technical Analysis Of The Capital One Hack," CloudSploit, 2019, https://blog.cloudsploit.com/a-technical-analysis-of-the-capital-one-hack-a9b43d7c8aea. The attacker, utilizing this role designation, sent another command to the metadata service, causing it to reveal the temporary credentials assigned to Capital One's computing cluster (an Amazon Elastic Compute Cloud, EC2). These temporary credentials were used by the attacker to send requests to Capital One's internal network, as if they came from the trusted computing cluster (moving laterally from WAF to EC2). Amol Sarwate, "Preventing a Capital One Cloud Data Breach," CloudPassage, September 4, 2020, https://www.cloudpassage.com/articles/preventing-a-capital-one-cloud-data-breach/. By virtue of the excessive permissions granted to these clusters, the attacker was able to run the ListBuckets command to get information about how the bank's customer data was stored. The S3:Sync command, also granted by the excessive permissions, was then used to copy data from the cloud storage to a local machine. The Capital One breach is, unfortunately, a "perfect" example of cascading security failures caused by cloud misconfiguration.

122 "Misconfigured AWS S3 Bucket Leaks 36,000 Inmate Records," Trend Micro, https://www.trendmicro.com/vinfo/dk/security/news/virtualization-and-cloud/misconfigured-aws-s3-bucket-leaks-36-000-inmate-records; "Unsecured AWS S3 Bucket Found Leaking Data of Over 30K Cannabis Dispensary Customers," Trend Micro, https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/unsecured-aws-s3-bucket-found-leaking-data-of-over-30k-cannabis-dispensary-customers; Shaun Nichols, "Leaky AWS S3 Buckets are so Common, They're Being Found by the Thousands Now—with Lots of Buried Secrets," Register, August 3, 2020, https://www.theregister.com/2020/08/03/leaky_s3_buckets/.

123 "Cloud Identity," Google Cloud, https://cloud.google.com/identity.

124 "IAM Concerned: OAuth Token Hijacking in Google Cloud (GCP)," DEF CON Forums, August 7, 2020, https://forum.defcon.org/node/234712; Rob Soto, "Detecting Google Cloud Platform OAuth Token Abuse Using Splunk," Splunk, October 9, 2020, https://www.splunk.com/en_us/blog/security/detecting-google-cloud-platform-oauth-token-abuse-using-splunk.html; Jani Patokallio and John McGovern, "Don't Get Pwned: Practicing the Principle of Least Privilege," Google, October 3, 2019, https://cloud.google.com/blog/products/identity-security/dont-get-pwned-practicing-the-principle-of-least-privilege; Msmbaldwin, "Azure Security Benchmark V2—Privileged Access," Microsoft, https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access; Sylvia Engdahl and Tracy Pierce, "Blogs," Amazon, August 20, 2020, https://aws.amazon.com/blogs/security/how-to-use-aws-config-to-determine-compliance-of-aws-kms-key-policies-to-your-specifications/.

for detailed architectural planning and comprehensive threat modeling, which can cost users dearly.[125]

Microsoft Azure's development has also exhibited some of these worrying trends. For example, users can pick between Connect, AD Sync, or ADFS to link their on-premises infrastructure to their Azure environments. These three models also have distinct security capabilities, each with trade-offs that require close attention.[126] These different complex mechanisms require comprehensive understanding to configure correctly and prevent attackers from moving laterally between user environments. The pace at which these features are updated makes it burdensome for organizations to adopt best practices in a timely fashion. The increased interface complexity also scales poorly with users' understanding of the cloud.[127]

Unfortunately, as more layers of capability are added, cloud vendors are finding ways to monetize crucial features, especially security tools. To effectively conduct incident response, organizations must be able to retrieve activity logs from their cloud environments. However, both Microsoft and Amazon have adopted schemes in which users must pay to record activity data (e.g., Azure AD Logs and GuardDuty, respectively).[128] Complicated billing structures may also increase the likelihood that organizations overlook essential security features, requiring manual input to turn on. "Secure by default" means readily providing cloud users the tooling to defend themselves. Monetization risks pulling users away from that goal. Cloud service providers can provide more secure linchpin services and defensible products to their users, and these providers will play a crucial role in cybersecurity as the adoption of cloud computing widens.

Brittleness in Federal Cyber Risk Management

Successive federal government cybersecurity leaders have tried run the .gov as a single enterprise without streamlining its ability to buy technologies, develop governance, or enforce policies accordingly. Governance, across the .gov in particular, continues to be fragmented in important ways. The passage of new laws and authorities does little more than pile on new requirements to those unmet previous. Across the federal government, the array of risk-management schemes, authorization programs, certification standards, and guidance for all of the above is staggering. The chart below maps out key existing policy programs and regulatory vehicles, as well as the SOC 2 certification scheme. The horizontal axis captures a highly abstracted flowchart of an information and communications technology (ICT) supply chain. Red entries denote core government responsibilities for implementation, and green for industry. Along the vertical axis are the key points of leverage into these supply chains. The programs noted below span moderating standards, producer practices, products, and deployment. Programs that crossed paths directly with SolarWinds or its Orion program are outlined in gold. Government and independent bodies apply these standards through a complex web of requirements, enforcement policies, certifications, authorizations, and support systems. The complexity of this array defies easy functional categorization and speaks to the dizzying collection of hurdles that stand between a prospective technology vendor and its federal user, let alone between a regulator and reform.

As illustrated graphically above, none of these systems can truly and cleanly fall into a single bucket. FISMA

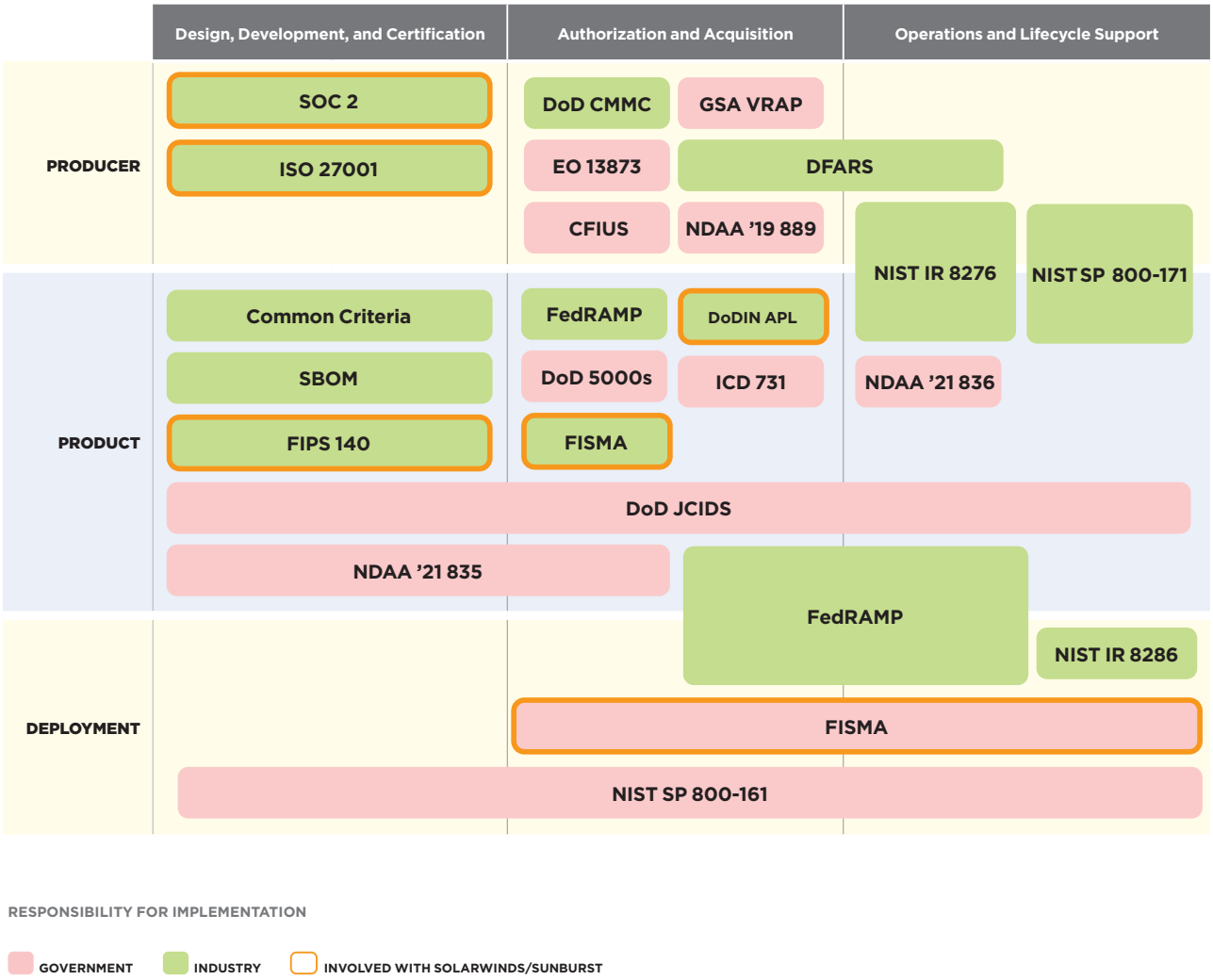
125 David Linthicum, "Cloud Complexity: Why It's Happening-and How to Deal with It," TechBeacon, September 10, 2019, https://techbeacon.com/enterprise-it/cloud-complexity-why-its-happening-how-deal-it#:~:text=Cloud; Patrick Seitz, "Amazon Web Services No Longer Untouchable As Cloud Competition Heats Up," *Investor's Business Daily*, October 29, 2019, https://www.investors.com/news/technology/cloud-computing-competition-will-heat-up-2020-idc-says/.

126 "Synchronizing Users from Azure Active Directory," Cisco, March 16, 2021, https://duo.com/docs/azuresync; "Active Directory Federation Service (ADFS)," Miniorange, 2021, https://docs.miniorange.com/articles/what-is-adfs#:~:text=ADFS%20makes%20use%20of%20claims,token%20by%20the%20identity%20provider; "Securing Microsoft Azure AD Connect," Trimarc, October 26, 2020, https://www.hub.trimarcsecurity.com/post/securing-microsoft-azure-ad-connect; "Active Directory Federation Services," Microsoft, May 31, 2017, https://docs.microsoft.com/en-us/windows-server/identity/active-directory-federation-services; "Active Directory Synchronization or Federation—Which One Should I Choose?" BDO Digital, July 07, 2015, https://www.bdo.com/digital/insights/cloud/active-directory-synchronization-or-federation; "What Is Azure AD Connect and Connect Health," Microsoft, January 8, 2020, https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-azure-ad-connect.

127 "Lateral Movement Explained: What Is Lateral Movement?" CrowdStrike, February 3, 2021, https://www.crowdstrike.com/cybersecurity-101/lateral-movement/; "Regaining ROI by Reducing Cloud Complexity," VentureBeat, February 18, 2021, https://venturebeat.com/2019/11/27/regaining-roi-by-reducing-cloud-complexity/.

128 Dr. Brian Carrier, "How to Investigate User Logins—Intro to Incident Response Triage 2021," Cyber Triage, July 29, 2019, https://www.cybertriage.com/2019/how-to-investigate-user-logins-intro-to-incident-response-triage-2021/; "Azure Active Directory Activity Logs in Azure Monitor," Microsoft, April 9, 2020, https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-activity-logs-azure-monitor; "Amazon GuardDuty User Guide," Amazon Web Services, https://docs.aws.amazon.com/guardduty/latest/ug/guardduty-ug.pdf.

Figure 11. Map of Federal Cyber Supply Chain Risk Management Programs



governs agency practices and deployment as much as it mandates checkboxes to product vendors.[129] The CMMC framework ranks and incorporates vendor practices into product contracts. It is also ambiguous "how" to assess security.[130] Often, the distinctions are too strong. For software, the line between a vendor and its product security is overly simplified. Product integrity cannot be assured if key components of the vendor's build and maintenance infrastructure are vulnerable, as in the case of Sunburst. When the government acquires an off-the-shelf product, it also buys maintenance practices over the product's lifecycle (and even the planned lifecycle itself). Security regimes must reflect that. Likewise, the security needs of a product must not only be determined by its function, but also by its placement and access in the network. FIPS 199, NIST 800-60, and FIPS 200 work under FISMA and requirements from NIST 800-53 to map information types, requisite security categories, and resultant security baselines for federal information systems.[131] However, they focus on classifying the risks from the compromise of information—specifically its confidentiality, integrity, and availability—rather than on the

129 "Federal Information Security Modernization Act," Cybersecurity and Infrastructure Security Agency CISA, https://www.cisa.gov/federal-information-security-modernization-act.

130 "Cybersecurity Maturity Model Certification (CMMC)," Office of the Under Secretary of Defense for Acquisition & Sustainment, December 10, 2020, https://www.acq.osd.mil/cmmc/.

131 "Standards for Security Categorization of Federal Information and Information Systems," National Institute of Standards and Technology, February 1, 2004, https://csrc.nist.gov/publications/detail/fips/199/final; Kevin Stine, et al., "Guide for Mapping Types of Information and Information Systems to Security Categories," National Institute of Standards and Technology, August 1, 2008, https://csrc.nist.gov/publications/detail/sp/800-60/vol-1-rev-1/final; National Institute of Standards and Technology, "Minimum Security Requirements for Federal Information and Information Systems," National Institute of Standards and Technology, March 1, 2006, https://csrc.nist.gov/publications/detail/fips/200/final.

potential blast radius of compromise and the resulting threat to an underlying network.

At the standards level, the FIPS 140 series of certifications maintain standards for cryptographic modules used by the government. NIST and associated labs review source code and any subsequent changes before validating a product, the certification of which lasts for about five years or until a vulnerability is discovered. FIPS 140-2 is being phased out for FIPS 140-3 over a few years, updating to a more diversified hardware, software, firmware, and hybrid modeling framework.[132] Many products have FIPS-inside modes, meaning they use or can be configured to use FIPS-validated modules. The Common Criteria, or International Organization for Standardization (ISO) 15408, is an international standard for mapping a product to evaluation criteria for security assurances. It maps around sixty requirements over several evaluation levels and is widely used in industry and required in federal agencies, essentially creating a common language for evaluations. Its compliance is assessed by NIST-approved labs. The timeline for Common Criteria certification can be long—in some cases, years.[133] The Defense Department's Joint Capabilities Integration and Development System (JCIDS) governs the capabilities-development portion of its acquisition process, enabling iteration of desired product capabilities from design to deployment, moving the process toward a more agile disposition, and incorporating a maturation and risk-reduction phase.[134]

Several different regimes and bodies deal with the security posture of vendors and producers. SOC 2 Type II reports detail compliance with American Institute of Certified Public Accountants (AICPA) requirements over a predetermined timeframe in accordance with CPA or other accountant-entity audits.[135] DFARS is the Department of Defense (DoD) supplement to the Federal Acquisition Regulation (FAR).[136] It contains specific cybersecurity provisions requiring vendor compliance with security controls sourced from NIST 800-171. Compliance can be determined by federal assessment, third-party audit, or self-assessment, with each method providing different degrees of accreditation. The requirements map to ISO 27001 as well, and defense contracts can be revoked without compliance.

The DoD's new CMMC program tiers and assesses vendor cybersecurity practices on a five-level range. It is incorporated into contracts and designed to operate with other existing standards, such as DFARS requirements and FedRAMP (both of which are aligning with CMMC level 3). It builds a C3PAO audit onto the existing DFARS requirements and is expected to provide a useful resource across the federal government.[137] The General Services Administration's (GSA) nascent Vendor Risk Assessment Program (VRAP)—though only in the draft proposal phase—will eventually make use of unclassified and classified information to vet vendor risk in the supply chain of federal contracts.[138] Treasury's Committee on Foreign Investment in the United States (CFIUS) reviews and acts on national security concerns arising from foreign investments and transactions in US domestic companies with authorities to order divestment, mitigate exposure, and even nix deals.[139] EO 13873 grants acquisition oversight powers to DHS under CISA's National Risk Management Center (NRMC) and elaborates on the Department of Commerce Interim Rule Response to define foreign adversaries, deconflict roles with

132 "Security Requirements for Cryptographic Modules," National Institute of Standards and Technology, December 3, 2002, https://csrc.nist.gov/publications/detail/fips/140/2/final; "Announcing Approval and Issuance of FIPS 140-3, Security Requirements for Cryptographic Modules," National Institute of Standards and Technology, May 22, 2019, https://www.nist.gov/news-events/news/2019/05/announcing-approval-and-issuance-fips-140-3-security-requirements.

133 Nancy Mead, "The Common Criteria," Cybersecurity and Infrastructure Security Agency, August 10, 2006, https://us-cert.cisa.gov/bsi/articles/best-practices/requirements-engineering/the-common-criteria; Katie Moss Jefcoat, "What Is Common Criteria Certification, and Why Is It Important?" BTG English, December 11, 2017, https://www.blancco.com/blog-what-is-common-criteria-certification-why-is-it-important/.

134 "JCIDS Process Overview," AcqNotes, February 2, 2021, https://acqnotes.com/acqnote/acquisitions/jcids-overview.

135 "What Is SOC 2: Guide to SOC 2 Compliance & Certification: Imperva," Imperva Learning Center, December 30, 2019, https://www.imperva.com/learn/data-security/soc-2-compliance/.

136 "DPC: Defense Acquisition Regulations System: DFARS/PGI," DPC Defense Acquisition Regulations System, DFARS/PGI, https://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html; "FAR," Federal Acquisition Regulation, https://www.acquisition.gov/browse/index/far.

137 "CMMC FAQs," Office of the Under Secretary of Defense for Acquisition & Sustainment, Cybersecurity Maturity Model Certification (CMMC), December 10, 2020, https://www.acq.osd.mil/cmmc/faq.html.

138 "Polaris GWAC Draft Request for Proposals," General Services Administration, https://beta.sam.gov/api/prod/opps/v3/opportunities/resources/files/ff814e347fbf4d47b3bcf351957bc205/download?api_key=null&token=.

139 "Committee on Foreign Investments in the United States," US Department of the Treasury, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius.

CFIUS, focusing on risk assessment against national security needs.[140] Last, and most granular, NDAA Sec. 889 updates FAR implementation to prohibit government procurement from several prominent Chinese Telecoms corporations.[141] In addition, NIST IR 8276 creates a SCRM overlay based on industry knowledge that provides guidance on vendor best practices for cyber supply-chain risk-management.[142]

At the product level, FISMA enforces the security of federal agency information systems and non-government organizations dealing in governmental CUI (Controlled Unclassified Information). It assigns responsibility to individual agencies for compliance with implementing risk-based security controls for their information systems, sourced from NIST 800-53, and the same for non-governmental organizations dealing with federal information, sourced from NIST 800-171. Overseen by the OMB, FISMA requires yearly reports to Congress by agencies, and incorporates several other standards and frameworks. The National Telecommunications and Information Administration (NTIA) SBoM program proposes a required product deliverable to track software and system dependencies, and has demonstrated successful pilot implementations in the healthcare sector. FedRAMP is a GSA program that implements a "do once use many" structure for the provision of cloud services to federal agencies.[143]

Vendors and their products are vetted by certified third-party auditing organizations for use by any federal civilian agency against a range of impact-severity levels, and held to several NIST standards, including guidance on continuous monitoring. It controls overlap with add-ons to FISMA compliance requirements. DoDIN's APL serves as a centralized list for DoD-acquired products that have achieved interoperability and cybersecurity authorization against a variety of standards and defense requirements.[144] Items can be pulled from the list, and reviews can occur after patches, though they may not need to take place. In parallel, the DoD's Adaptive Acquisition Framework lays out several pathways for vendors to sell products to the DoD, sorted by the type of capability being addressed and all under a blanket requirement of cybersecurity.[145] The specific software pathway focuses on more agile requirement development and iteration processes and more comprehensive lifecycle planning, and a full review is required after three years, barring a three-year extension approval. NDAA Sec. 835 requires the development of software security criteria in bid solicitation, code-review procedure, and coordination with DoD acquisition reform.[146]

Currently, the federal civilian cybersecurity doctrine leans too heavily on individual agencies. They are often expected to determine how to assess producers and product risk and make choices on how to manage that risk. A customized solution for each agency is infeasible. As a result, civilian federal agencies systemically fail at implementing recommended practices.[147] Fourteen of twenty-three federal civilian agencies failed to sufficiently implement a single foundational practice aggregated by the GAO from NIST 800-161, -37, -53, -30, and -39. Those practices are executive oversight of ICT SCRM, agency-wide ICT SCRM strategy development, identification and documentation of agency-specific ICT supply chains, the establishment of procedural ICT supply-risk assessment, the establishment of SCRM review of potential suppliers, organizational SCRM requirements for ICT suppliers, and pre-deployment compromise detection.

The GAO report cited above aggregates several agency-reported reasons for this systemic failure: insufficient federal guidance to implement one or more practices; awaiting guidance from the Federal Acquisition Security Council (FASC); federated organizational structures creating an unmanageable diversity of risk

140 "Executive Order 13873 of May 17, 2019, Securing the Information Communications Technology and Services Supply Chain," Code of Federal Regulations, https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain; "National Risk Management Center (NRMC)," Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/nrmc.

141 "FAR."

142 Jon Boyens, et al., "Key Practices in Cyber Supply Chain Risk Management: Observations from Industry," National Institute of Standards and Technology, February 11, 2021, https://csrc.nist.gov/publications/detail/nistir/8276/final.

143 "Federal Information Security Modernization Act," Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/federal-information-security-modernization-act; "Software Bill of Materials," National Telecommunications and Information Administration, https://www.ntia.gov/SBOM; "Frequently Asked Questions," FedRAMP, https://www.fedramp.gov/faqs.

144 "APLITS," DISA APLITS, https://aplits.disa.mil/#faqs.

145 "Operation of the Adaptive Acquisition Framework, DoD Instruction 5000.02," US Department of Defense, January 23, 2020, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500002p.pdf?ver=2020-01-23-144114-093.

146 "National Defense Authorization Act for Fiscal Year 2021," HR 6395, 116th Congress, introduced March 26, 2020, became law, January 1, 2021, https://www.congress.gov/bill/116th-congress/house-bill/6395/text.

147 "Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks."

tolerances within an agency, or delegating the task to internal bureaus; insufficient need for an ICT SCRM program to justify the resources required; general complexity of the undertaking; and agency preference for ad hoc management of supply-chain risk assessment. Without help in implementing agency SCRM plans, incident response and coordination by the federal government will continue to suffer.

The plethora of information-sharing forums in existence deserves mention, despite not fitting into Figure 10. CISA's Critical Infrastructure and Key Resource (CIKR) Cyber Information Sharing and Collaboration Program (CISCP) strives to aggregate unclassified threat data between industry and government, generally focusing on critical-infrastructure industry partners.[148] Within the government, NTIA's Communication Supply Chain Risk Information Partnership (C-SCRIP) is designed to coordinate incident response and threat intelligence between the ODNI, DHS, the FBI, and the Federal Communications Commission (FCC), and output it to smaller communications providers, but it is still developing.[149] CISA's National Cybersecurity and Communications Integration Center (NCCIC) is designed to coordinate within government, and is also refining its practices among six internal entities.[150]

Most notable, though, is the conspicuous lack of a single clearinghouse for crucial threat information, a common point of concern for industry, which has set up several substitutes, including the Information Technology-Information Sharing and Analysis Center (IT-ISAC), the National Defense Information Sharing and Analysis Center (ND ISAC), and others.[151] While centralizing responsibilities within government would likely prove too onerous and leave gaps in specialized knowledge, information is better situated to benefit from aggregation and standardization.

More important than reactive information, however, is proactive intelligence that anticipates threats and helps to shape the behavior of both offensive and defensive players. The outcome from more proactive, permissioned, and frequent working-level collaboration between offensive and defensive entities, as well as between public and private stakeholders, is crucial to driving a more responsive and defensible technology ecosystem. When FireEye began disclosing the Sunburst campaign elements it had uncovered to government, Chief Executive Officer (CEO) Kevin Mandia, in testimony to House and Senate committees, said, "My reaction was that I didn't see surprise…A lot of folks…had various products that had little blips on the radar, and we had to connect the dots from many different vectors."[152] These common but unconnected concerns, observed once all stakeholders were in the same room, indicate a clear improvement—striving to convene and share regularly and proactively, rather than just in response to an observed incident. In Mandia's words, "If you centralize the intel, it can only improve the speed at which that picture and vision will come together."[153]

Most broadly, this overemphasis on prevention and reaction, rather than mitigation and rapid discovery, forces the government to fight an unwinnable battle. Compromise is inevitable and ongoing. Creating new programs from scratch will not remedy cybersecurity shortcomings, and risks complicating an already crowded regulatory picture. The goal of at least one avenue of reform should be to condense, clarify, and coordinate between existing programs—empowering more rapid adaptation by the executive branch and a recurring trimming back of programs not fit to purpose, or too slow to match the technologies for which they purport to manage risk. Many of the building blocks for these changes are in place, but they require iterative and diligent improvement. The final section of this report discusses how to move these policies, and the larger US cybersecurity strategy, toward a more secure, defensible, and competitive posture.

148 "CIKR Cyber Information Sharing and Collaboration Program," US Department of Homeland Security, https://csrc.nist.gov/CSRC/media/Events/ISPAB-JUNE-2013-MEETING/documents/ispab_june2013_menna_ciscp_one_pager.pdf.

149 "Notice of Establishment of the Communications Supply Chain Risk Information Partnership," National Telecommunications and Information Administration, https://www.ntia.doc.gov/federal-register-notice/2020/notice-establishment-communications-supply-chain-risk-information.

150 Ibid.; US Department of Homeland Security, National Cybersecurity & Communications Integration Center (NCCIC).

151 "ISAC About Us," IT-ISAC, https://www.it-isac.org/about; "About ND-ISAC," National Defense ISAC, June 12, 2020, https://ndisac.org/about-ndisac/.

152 "Weathering the Storm: The Role of Private Tech in the SolarWinds Breach and Ongoing Campaign," US Congress, House, Committee on Oversight and Reform, 117th Congress, February 26, 2021.

153 Ibid.

IV — TOWARD A MORE COMPETITIVE CYBERSECURITY STRATEGY

Despite their sophistication and constancy, state-backed campaigns like Sunburst hold lessons for government and industry to move toward a more competitive US cybersecurity strategy. Between catastrophic inaction and the impossibility of total prevention of harm, there are several existing programs and standing guidelines that can be tweaked, as well as simple new directives built on existing authorities—all of which can help to better contain, and more quickly identify, the next such incident.

For too long, US cybersecurity policy has bifurcated offensive and defensive activities and ignored the realities of the conflict environment in which defensive responses shape the future of an offense that preys on incremental shortcomings. Every change is part of the ongoing search for an advantageous position. And while defenders play with homefield advantage, they must contend with ever more complex networks and a byzantine array of overlapping requirements.

Change is vital to reform the US cybersecurity strategy to match the dynamism and speed of the cyber conflict environment. Both government and industry must take part. Successful participation in an intelligence contest demands just that—good intelligence. Information sharing between government and industry is critical for identifying and addressing similar cyber incidents, and—as often noted in congressional hearings held in the wake of the Sunburst campaign—the current state of such collaboration is inadequate.[154] One group found that the greatest impediment to information sharing from the private sector was its fear of liability, which was not fully covered under the Cybersecurity Information Sharing Act of 2015 (or 2002).[155] Concerns voiced in congressional testimony by Microsoft, FireEye, and others about the difficulty of notifying government echo the findings, and contractual restrictions on notification from one vendor to multiple agencies further compound the issues and delay response.[156] Throwing funding at promising and/or new initiatives before fully grasping the failures

154 "Weathering the Storm: The Role of Private Tech in the SolarWinds Breach and Ongoing Campaign."

155 "Information and Communications Technology Supply Chain Risk Management Task Force Year 2 Report," Cybersecurity and Infrastructure Security Agency, December 2002, https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force_year-two-report_508.pdf.

156 "Weathering the Storm: The Role of Private Tech in the SolarWinds Breach and Ongoing Campaign."; "Information and Communications Technology Supply Chain Risk Management Task Force Year 2 Report," US Department of Homeland Security, Cyber and Infrastructure Security Agency, December 2020, https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force_year-two-report_508.pdf.

(and successes) of existing networks and programs is a recipe for similar results.

The remainder of this section discusses the strategy of "flow," highlights several successful or promising programs in federal cyber risk management and offers three clusters of recommendations to build on these programs in aspirational reform toward a US cybersecurity strategy of "flow."

Seeking Flow

The United States should work to adopt a strategy of persistent "flow," acknowledging that the persistent engagement of cyberspace requires balance and agility in the search for leverage over an opponent—something akin to a continuous boxing match. It is not enough for a US cybersecurity strategy to focus on engagement. The United States must attempt to maintain balance between these operations, and across defenders, while anticipating adversary moves and seeking its own points of leverage to exercise strategic effects. Adversaries contribute to creating this flow. Opponents seek intelligence not just as a means to drive action or to position in anticipation of conflict, but to create leverage.[157] That means leverage through positioning in the classical, mechanical sense, as well as in the compression of time—degrading opponents' ability to identify and respond to new information, while speeding up one's own adaptive cycle or deployment of force against the adversary.[158]

Engagement in the cyber domain is not staggered by periods of war and peace, but remains a constant flow of activity.[159] The Defend Forward strategy, formalized in the DoD's 2018 Cyber Strategy, recognizes the breakdown of the offense-defense binary. The strategy of defending forward will be a part of engaging in persistent flow, but it cannot overshadow the other constituent parts of the strategy. One of the targets of the intelligence contest is the adversary's ability to conduct successful intelligence operations of its own.[160] A key metric of success in intelligence collection is the comparative success of the intelligence collected on an adversary versus the intelligence collected by that adversary.[161] These operations have many forms: intelligence collection, exploitation, sabotage of adversary capabilities, and asset prepositioning. The leverage that emerges from an intelligence operation, therefore, could range from the fait accompli of exploited intelligence to strategic or operational repositioning because of improved situational awareness.

Flow describes a steady state of decision-making, informed by the kind of information yielded from this intelligence contest and continually applied in a cycle of persistent engagement with the adversary.[162] Persistent engagement can be improved on to better encompass not just the moment two adversaries are engaged, but the sequence of moves before and after, including adjustments to take advantage of any leverage gained through action. This continual back and forth—searching for leverage and adapting to an opponent's moves, while keeping balanced and capable in both defense and offense—resembles the flow found in combat sports like a boxer's balanced strikes and parries, looking for a decisive opening, or a wrestler's grappling, hunting for seams and working to end the match.

Nonetheless, strategic outcomes are still possible as the cyber domain has expanded the sources of strategic power that can now be touched by adversaries.[163] Once identified, points of weakness can be exploited through action in any domain. This creates a tension between allowing enough time for the collection and

157 Michael Warner, "The Character of Cyber Conflict," in "Policy Roundtable: Cyber Conflict as an Intelligence Contest," *Texas National Security Review*, 2020, https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/#essay2.

158 This concept of flow owes much to the OODA loop as developed by John Boyd, previous comparisons of offensive cybersecurity activity to the various fighting arts, including the sweet science, and to discussions with AJ, JD Work, and Michael Martelle.

159 Richard J. Harknett, et al., "Deterrence Is Not a Credible Strategy for Cyberspace," Orbis; 61, 3, 2017, 381–393, https://www.sciencedirect.com/science/article/abs/pii/S0030438717300431?via%3Dihub.

160 Joshua Rovner, "What Is an Intelligence Contest?" in "Policy Roundtable: Cyber Conflict as an Intelligence Contest," *Texas National Security Review*, 2020, https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/#essay1.

161 This comparison, by the very nature of the intelligence operations, cannot be evaluated in full, but stands as the key fulcrum in the contest.

162 This model is by no means novel—it echoes many of the same themes found in evolving US counterterrorism strategy in the mid- to late 2000s—collocating intelligence and direct-action elements to more effectively target adversary networks and sustain a high operational tempo. "Summary: 2018 Department of Defense Cyber Strategy," US Department of Defense, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

163 Chesney, et al., "Policy Roundtable: Cyber Conflict as an Intelligence Contest."

analysis of intelligence and ensuring its timely deployment during the fleeting window of information dominance. Recognizing this window and having the structural agility to converge on points of leverage are key to the strategy of persistent flow as an offensive player.

Pulling this same information back to defenders strengthens the foundation from which offensive activities will spring and around which they must maneuver. This makes the interplay between defensive state and offensive initiative important to each. Defensive value, within a persistent flow, is the result of identifying one's weaknesses and dependencies, especially where those points align with areas of significant utility to adversaries. No system can detect and deny every assault, but heightened awareness of these junctures will improve security and resilience.[164]

These junctures, like other points of leverage, are fleeting. Steps within the cyber domain to either take advantage of or protect points of leverage do more than alter the position of each actor involved—they also alter the cyber environment itself. Cyberspace is a manmade domain to a unique degree. Hardware constitutes the continental geography—the mountains, oceans, and plains of cyberspace.[165] Atop this foundation, both cooperative and adversarial efforts have created highways, cities, and homes of firmware and software with varying levels of malleability. In this environment, each weakness found, exploited, and patched alters the terrain incrementally.[166]

Successfully recognizing and moving to the rhythm of the persistent flow will require speed, balance, and agility. In this vein, the report's recommendations focus on building toward a strategy that emphasizes the speed of change and adaptation to current threats by building on existing programs and policies wherever possible, in lieu of creating anew.

Build Better on What Works (Or Could)

While the federal cyber policy landscape, focusing on risk management and authorization programs impacting industry, is brittle and complex, this report acknowledges a number of programs that demonstrate local success or potential for the same. The common NIST frameworks, for example, begin the critical work of centralization while maintaining customizability between agencies and network types. The NIST controls are not a panacea, but they create some continuity between a wide variety of agency and department needs, while still allowing tailoring through specific control requirements and thresholds.

The Agile Acquisitions Framework supports some coordination between overlapping DoD and federal civilian agency processes (CMMC, FISMA, and FedRAMP), and its clear linkages to the NIST SP 800-171 common library are useful, with an implementation framework available. In general, the long-overdue embrace of agile capability requirement and development is a good start. The CMMC's notional assessment of vendor cybersecurity likewise begins to widen the aperture of acquisition to a more realistic set of considerations. Even limited trust-network practices to limit lateral movement may have helped at least reduce the scale of SolarWinds' compromise within the DoD compared to federal civilian agencies.[167]

There are other programs with great promise. While the core assessment program fails to match the pace of technology deployment by providers (or demand by users), FedRAMP's "do once use many" model is a valuable approach.[168] The program can help coordinate among agencies with common needs and vendors with limited resources, and it has important nods to the dynamic nature of software, which is especially important for cloud services. NTIA's Software Bill of Materials (SBOM) can play a valuable role in informing vendors and agencies in kind of their practical and measured exposure to vulnerabilities, serving as

164 Adam Segal, "The Code Not Taken: China, the United States, and the Future of Cyber Espionage," *Bulletin of the Atomic Scientists* 69, 5, September 2013, 38–45, https://doi.org/10.1177/0096340213501344.

165 Chris McGuffin, et al., "On Domains: Cyber and the Practice of Warfare," *International Journal: Canada's Journal of Global Policy Analysis* 69, 3, September 2014, 394–412, https://doi.org/10.1177/0020702014540618.

166 Martin C. Libicki, "Cyberspace Is Not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society* 8, 2, 2012, 321–336.

167 Jackson Barnett, "DOD Has a Leg up in Mitigating Potential SolarWinds Breach, Former Officials Say," *FedScoop*, December 17, 2020, https://www.fedscoop.com/dod-solarwinds-military-pentagon-breach-cybersecurity/; "NIST SP 800-171: DoD Assessment Methodology, Version 1.2.1," National Institute of Standards and Technology, 2020, https://www.acq.osd.mil/dpap/pdi/cyber/docs/NIST%20SP%20800-171%20Assessment%20Methodology%20Version%201.2.1%20%206.24.2020.pdf.

168 Michael Mclaughlin, "Reforming FedRAMP: A Guide to Improving the Federal Procurement and Risk Management of Cloud Services," Information Technology and Innovation Foundation, June 2020, https://itif.org/sites/default/files/2020-fedramp.pdf.

a proxy for indicating system knowledge. GSA's proposed VRAP has the potential to drastically improve information sharing within government, particularly between classified and unclassified networks, and the overlying Polaris program could help make the entire acquisition process more manageable for smaller enterprises.

CISA has undertaken several initiatives that demonstrate that the agency is also looking at many of the right critical areas. Most noteworthy is the CDM program discussed in sections II and III, which aspires to track cloud configurations, software and hardware assets, and security posture, and provide common security services across federal civilian agencies. Hard questions need asking to determine whether CDM is a program capable of success under its current service-delivery model, contractor-supported technology base, and the management and available budget of DHS. Fully realized, however, CDM could fill several of the gaps identified in this report on its own.

The private sector has a major role to play in this period of reform. Microsoft's role in the core incident response to Sunburst cannot be understated because of its intricate knowledge of dependencies and its rapid mobilization of dedicated teams in response. Yet, this expertise was not effectively leveraged to prevent the intrusion. This duality deserves mention. FireEye and Microsoft were first to warn the federal government of the existence and widening scope of the Sunburst incident, faster than highly funded intelligence and cyber agencies (at least publicly). Incident-response teams from both companies have since begun to investigate and remediate compromises for private-sector and federal-agency networks. Some of Microsoft's best and brightest in security engineering, threat intelligence, and consulting incident response have worked for months after the initial discoveries at a ferocious pace. These worthy efforts, and the individuals delivering them, deserve to have their work included and valued in the discussion of cybersecurity policy reforms.

The scale of the lateral movement in the Sunburst incident raises fears that cloud service providers (notably Microsoft in this instance, but not to ignore Amazon, Google, or VMware) continue to underinvest in countering low-probability, high-consequence events not well captured by a common vulnerabilities and exposures (CVE) score.[169] The problem is not only one vendor. The compromise of various on-premises and cloud software in the Sunburst campaign also underlines the challenges of the shared-responsibility model. Where products and services are unnavigable in their complexity or poorly designed against a known class of intrusions, the provider has failed to provide the user with adequately defensible technology.

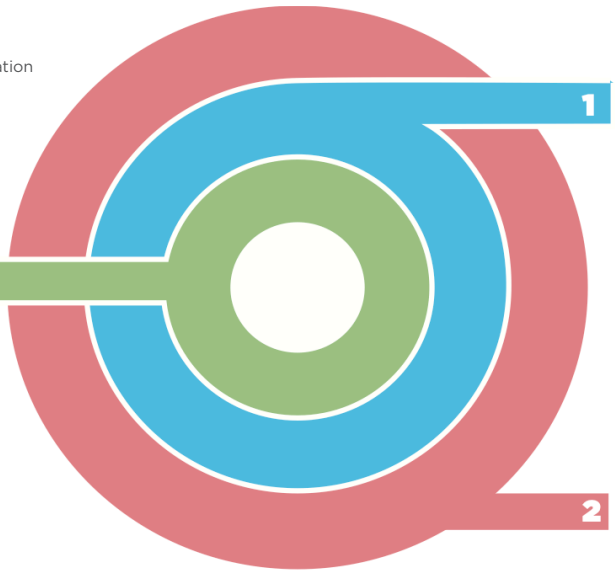
Recommendations

To maintain an advantage in this fight, the United States must emphasize policy reforms and shifts in industry practices that explicitly work to reduce complexity and produce greater speed and agility (capacity to adapt). This report organizes these within three clusters: risk management, defensibility, and adaptability. First, to make the most efficient use of its resources, the government, in partnership with industry, must prioritize those programs and assets at critical junctures of its networks, aligning its response with a ruthlessly risk-based assessment of its exposure to harden these nodes. Second, within those hardened points, and throughout all its networks, the government must work with industry and the open-source community to make linchpin technologies more defensible. Third, any shifts in policy must seek to leave a more adaptive system behind—one with the capacity to iterate on imperfect programs instead of reverting to a complete overhaul at every significant failure. This adaptability is built around and through each of the other pillars.

169 "Russian State-Sponsored Actors Exploiting Vulnerabilities in VMware Workspace ONE Access Using Compromised Credentials," NSA Cybersecurity Directorate, December 2020, https://media.defense.gov/2020/Dec/07/2002547071/-1/-1/0/CSA_VMWARE%20ACCESS_U_OO_195076_20.PDF;
"Microsoft Security Response Center," Microsoft Security Response Center, February 18, 2021, https://msrc-blog.microsoft.com/2021/02/18/microsoft-internal-solorigate-investigation-final-update/. Disclosure about the exposure of sensitive source code from Microsoft's own corporate networks to these same adversaries can hardly slake these fears, if only for contemplating what else might have been compromised. As was later disclosed, this access allowed the adversary to download some source code for Microsoft's email server, Exchange, mobile-device management service, InTune, and some Azure cloud services including "security [and] identity…"

Atlantic Council

Figure 12. Summary of Broken Trust recommendations by ease of implementation



Ready for Work 0

These recommendations build on existing authorities, functions, or programs but may require new funding.

1. **Hunt for Blast Radius**
2. **FASC Sets the Process**
4. **Shift the Landscape for Adversaries**
6. **Give SBOM a Glide Path to Success**
8. **Do Not Leave Open Source Behind**
10. **Create a Trusted Traveler Program for FedRAMP**
11. **Evolve and Default to Secure**

1 Some assembly required

These ideas pair an action with an outcome or actor but may have a critical dependency that keeps them from being shovel ready.

5. **Develop a Lifecycle Security Overlay**
7. **Apply the Overlay**
12. **Govern Through the Cloud**

2 Step Carefully

Ideas to push outside the box a bit farther while still being rooted in critical needs

3. **Breach Response Hunger Games**
9. **Change an Architecture, Change the World**

These recommendations do not try to prevent badness from reaching federal networks; leaning on prevention is a fool's errand. Rather, they seek to increase the speed of detection and responses, decrease the severity of a breach, and move toward a continuous, rather than an iterative, measurement of performance and compliance. There is no recommendation of scorecards or new governance metadata below. In time these may be useful, but part of the challenge the federal government must confront is that, at present, it has too many programs seeking, and failing, to achieve too much. The grades being handed out are already poor, and the answer is not to switch to a new test.

The goal of this report, and thus these recommendations, is to improve US competitiveness in this intelligence contest and better secure users. The response must prioritize incremental improvements, rather than a search for silver bullets. The twelve recommendations fall into three categories based on maturity and complexity.

"TO MAINTAIN AN ADVANTAGE IN THIS FIGHT, THE UNITED STATES MUST EMPHASIZE POLICY REFORMS AND SHIFTS IN INDUSTRY PRACTICES THAT EXPLICITLY WORK TO REDUCE COMPLEXITY AND PRODUCE GREATER SPEED AND AGILITY."

Ruthlessly Prioritize Risk

The argument to minimize blast radius is a form of triage, to bring to bear the most rigorous assessment and code integrity-management methodologies against the most potentially damaging products and services already present on federal networks. Assessing blast radius also treats .gov and .mil as the wider enterprise networks they are evolving to be, rather than a disparate collection of agency silos.

Resources are limited, and cybersecurity resources in government especially so. Whatever can be done to grow those capabilities must be supported by increasing the efficiency of applying what is already there. These recommendations start from the assumption that much of the federal cyber risk-management apparatus is struggling to keep up with the volume of attack surface and pace of threat sophistication; that Sunburst is not a one-off success by the adversary, but rather the product of systemic inadequacies that could quickly reveal themselves again in the future if not addressed. These recommendations prioritize speed and concentration of defender's response, taking a limited and realistic perspective—both in assessing risk and developing policies to manage it.

Table 1 - Annotation Key: **The recommendations below have been annotated with anonymized comments and feedback from five different cybersecurity stakeholder communities collected prior to publication.**

Category	Description
ICT Vendors	Vendors building software and hardware products and services. May sell security products as well.
Security Vendors	Companies selling security tools, services, and information to customers especially focused on defense.
Standards/ Civil Society	Organizations focused on technology standards, software developments, and research or organizing about policy across industry and toward government.
Executive Branch	Staff from executive branch agencies (e.g., DoD and DHS).
Legislative Branch	Staff from committee and personal offices across the US Congress.

ICT VENDORS

» Every piece of tech we adopt has an impact on other systems and affects everything around it if it blows up. We must study this effect and consider it when we design systems. Environments should be considered hostile by default. Need security in design- know how many systems are sandboxed and allow interoperability only when necessary and to the lowest possible level. Blast radius is more easily contained if we consider everything to be a bomb. We need to create a world where there are no default credentials and give trust in small amounts.

» There is going to be time in between, hybrid scenarios. There is implicit trust baked into systems and we need to fix that. Junctions between old and new technology is weak because of this.

» We need to set hard goals and we'll start to see the gradual improvement. We should whittle away at the old stuff. When you start getting the momentum, getting the vendors to play, gets easier to start adapting. Baby steps that will snowball into big transformation.

» Where is the talent in the US government? We need more expertise, get the ideas in the right place, for broad transformation.

» 'Large tech company' has a small group to come up with risk measures and evaluate adherence to them. This is necessary to have centralized accountability, there must be someone at the top who is looking at it holistically and observing the measurement. This is a culture and leadership style, but Federal government means different leadership styles every four years. There is no real ability to set a 20-year coherent policy because every four years it might get disrupted.

» It is going to be extremely culturally hard to break down the prevalence of agency silos, where each organization is siloed and verticized in their approach in where we handle risk. This is probably on the government to build more trust to break down those silos.

» To make these assessments, the concerned body needs to look at the process that was used to make the software, not just the product itself at a single point in time. What kind of standards do they use, do they do architectural analysis, spot check artifacts, where is the threat model for this piece of the software.

» NIST controls are implementable, but a lack of useful case studies of the practical dynamics of this, beyond the check the box approach, of true risk management. Such case studies would be really useful for small to medium businesses.

» Every organization in the USG produces a report on their compliance with the NIST standards. The history of these shows that there is rarely full compliance with regulation. So what is the USG going to do about it? Are we uninstall the software? If there are no consequences for not following guidelines, then there is really no point.

SECURITY VENDORS

» The NIST guidance is unimplementable. It doesn't work, it requires a massive budget, and even then you can't keep up. Just madness trying to do this over and over again. Giving NIST more responsibility that can't be implemented is just wrong. All been trying to follow NIST guidance and just doesn't work. Private sectors have an easier time, but we have to start looking at different ways of looking at this problem. We need more automation, thoughtfully, and hard follow-up. I think there is no stick right now. Will we throw a ton of money at the problem and just be back here again in a few years?

1. Hunt for Blast Radius: *The .gov and .mil environments each need a single agency to hunt for software with the largest potential blast radius, should it be compromised and coordinate proactive and rigorous security assessment of those products and vendors.*

The US government should implement blast-radius assessment programs, headed by one agency each for .gov and .mil. The .gov environment serves as a convenient example.[170] CISA would be empowered to undertake three concurrent initiatives. First, it would realize CDM's goal of collecting real-time asset and product use information from all federal-agency networks. Second, it would develop blast-radius assessment criteria with regular input from FASC, NIST, private-sector threat-intelligence partners, and the federal intelligence and law-enforcement communities. This assessment would judge the potential impact of a product's compromise to the whole of the .gov, not in single agency silos—the blast radius.[171] The criteria to assess blast radius should include a variety of measures, including the frequency of the product's use across .gov, the diversity of vendors for that product, and updated information on adversary targeting and tactics.

Last, these assessments would inform a list of product-vendor entries, ranked by their blast radius and

170 "CDM Program Overview"; "DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program," US Government Accountability Office, 2020, https://www.gao.gov/assets/gao-20-598.pdf. With regard to CISA's CDM, blast radius may well be already sought by the program. However, even if so, the current state of the program is insufficient. Blast-radius assessment is a critical function, and one that should be at the top of any CDM reform process. The resulting program should look like the below, as a way to prioritize the management of risk of products across the federal enterprise, in addition to addressing risk within particular agency networks. The potential overlap of this program with CDM should be seen in context with CDM's struggles to mature and continue rapid expansion. Assessing blast radius and working to manage risk from the most widely used and impactful products in the federal environment aligns with the nominal focus of the HVA program. Pulling this work out and highlighting it in its own program could be an important way forward.

171 There are products that will be difficult to separate from broader technology programs or systems, including myriad cloud services. These may involve broader assessments than just the single product, but the federal government also purchases myriad appliances and standalone devices and software. As discussed above, the goal is not a comprehensive risk-management program, but to minimize harm from the most potentially harmful products.

spread across three to five tiers. The top level, limited to the order of tens of entries, would be subject to exceptional scrutiny and testing, even up to one year after end of use. This top tier would be subject to an evolving set of product-integrity and vendor-security hygiene assessments. This could include measures like introducing the use of reproducible builds, unannounced penetration testing, prohibiting use of certain dependencies or vendors, and more. Lower tiers, increasing in size by orders of magnitude, would be flagged to agency security teams and other elements in CISA for their assessment. This tiered blast-radius list should be available to any federal cybersecurity official or defensive organization.

This blast-radius approach is an important part of managing software supply-chain risk on the demand side. As the cases in Section II showed, it is low-profile software used in critical parts of a network or given high-level permissions that present valuable targets. Identifying a handful of administrative tools as "critical" software beforehand would be difficult without this context of where they are deployed and how they are used. Software like Orion may well be assessed as high risk in one organization, but not another depending on its use and resulting impact on real-world risk. CISA's assessment methodologies should be made public and reviewed annually with industry and researcher input. The costs of assessment and inspections will be borne by CISA, while the added cost of any new program requirements (like reproducible builds) will be borne by the company. Companies receiving scrutiny in this top tier should be highlighted to federal ICT procurement entities for possible preferential procurement. All blast-radius assessment information and products should also be made available to major federal security-authorization programs, including the DoD APL and FedRAMP.[172]

2. FASC Sets the Process: *Federal agencies and departments should be able to leverage common risk-assessment processes to judge ICT supply chains and vendors; the FASC should be responsible for developing these processes, rather than individual organizations.*

Agencies should not be obligated to develop their own processes (code for methodology and standard procedure) to assess the risk of their ICT supply chains and evaluate vendor security maturity. Many are simply not developing them, and .gov and .mil see little benefit from a dozen variations on the same best practices.[173] One of the key issues flagged by the SolarWinds vector to Sunburst is the inconsistent application of existing policies and risk-management approaches. Consistent operating procedures to assess and manage software supply-chain risk are an important governance tool for the Federal CISO, CISA, and others to manage the federal cyber environments (.gov and .mil). The FASC, supported by NIST, CISA, and NSA-CD, should develop appropriate processes to analyze agency ICT supply chains, assess risk across those chains, and evaluate vendor security maturity and risk. In assessing vendor maturity and risk, FASC should look to leverage existing programs like GSA's VRAP wherever possible. FASC's outputs should be adopted as standard and default by all federal agencies procuring ICT, absent specific waiver from the office of the federal CISO.

3. Breach Response Hunger Games: *Rather than trying to implement a one-size-fits-all measure to best contain blast radius in .gov and .mil, CISA should organize and iterate on this competition model to surface the best organizational strategies and reward innovation.*

Identifying blast radius is tantamount to containing it. The logic of "treat everything like a bomb" speaks to the realistic limits any technology purchasing and using organization can have in designing or selecting the risk out of a product or service. To complement these .gov and .mil efforts to triage existing blast radius, this recommendation works to surface the best practices, highest-functioning teams, and best organizational models across the federal government to contain blast radius.

CISA should, at least twice a year, organize a breach

ICT VENDORS

» What size should the blast radius be? One vendor suggested cutting the network into one-hour containment blocksWe need to measure effectiveness of containment, so the cleanup is much faster. We can start to clean up some of this risk/reduce loss tolerance. We shouldn't think about success criteria as one big jump, but as milestones along the road.We need the right measurements that measure the blast radius itself. How many of your systems are trusted by another system? How easy is lateral movement? How much is sandboxed? How many paths are there? Are there automated systems to prevent mistakes? We need to think about the targets and how we administer and operate these networks.

172 After an initial triage phase, this blast-radius assessment could be inverted. Rather than agencies working with CISA and the .mil equivalent to identify high-value assets, then working with vendors to implement assessment for these Tier 1 products, those vendors could be required to submit their products to those assessments if a potential deployment reaches a suitable size of *prospective* blast radius.

173 "Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks."

response competition. The event could be modeled on the already-successful President's Cup, in this case pitting agencies and departments against each other.[174] The event should measure entrants' time to remediate a simulated breach within their own networks. The technical "breach" element of each competition should be organized by a new host party, much like the rotating creators of popular "capture the flag" competitions. The federal CISO should be empowered to mandate participation at the office's discretion.

Whichever competing organization achieves the shortest time to identity and contain the simulated breach should receive recognition by CISA and a 10-percent bump in baseline IT sustainment or security-related funding from their specific appropriating committee in their subsequent fiscal year. CISA will be responsible for capturing a concise lesson learned from each event, and for adapting the agency's guidance to others across the .gov accordingly.

Improve the Defensibility of Linchpin Software

Core technology companies and platform vendors have the unique opportunity to take information about adversary behavior and proactively change the technical landscape in front of these adversaries. This includes changes in design, and even architecture, of a product, as well as improvements to how straightforward it is to configure and defend those products. Technology vendors have an obligation to keep pace with the risk landscape, especially once low-probability high-consequence failures become more common. Where products and services are unnavigable in their complexity, buggy, or just poorly designed against a known class of intrusions, the provider has failed to provide the user any real opportunity to share the responsibility for their own security and defend themselves.

This need for defensibility is particularly keen in linchpin systems on which large networks and modern cloud deployments rely, like IAM systems. Underinvesting in the defensibility of these linchpin technologies, at the source and at certification, has produced exploitable seams for adversaries. Industry plays a role in securing software supply chains by building mature and defensible software, as well as by effectively defending its own networks and internal processes. More effectively defensible, and secure, technology creates space for offensive activity while denying the same to adversaries.[175]

Information about adversary trends and intentions should inform defensive investments, vendors' architectural choices, updates to existing technologies—including appropriate default configurations—and tools for users to hunt for and evict adversaries. Neither the private sector nor the public has a monopoly on this information, and few vendors or code maintainers can alter their product without impacting others in the ecosystem. This current crisis is an opportunity for the policy community and industry to reinvigorate moribund public-private coordination vehicles, at DHS and elsewhere, to drive common reforms to support responsive industry-led security innovation under clear guardrails determined by the policy community. This collaboration is critical to scale defensive activities in line with the growing complexity of enterprise IT systems and commercial/government cloud deployments.

While the adversary responsible for Sunburst demonstrated significant creativity, competence, and patience, little of what it did was truly unprecedented (or undetectable). Most of the other software supply-chain attacks surveyed for this report shared basic security failings to allow adversaries access to development and deployment infrastructure. Improvements to the security of linchpin systems and a more robust approach to secure software deployment will help address these vectors, including malign account access, flawed cryptography, and broken signature systems. The goal of these recommendations is to push the development of more secure and defensible technologies, especially at the linchpin of major cloud deployments and create greater room for maneuver by offensive entities in support of national security objectives.

174 "President's Cup Cybersecurity Competition," Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/presidentscup.

175 "Building a Defensible Cyberspace," Columbia School of International and Public Affairs, September 28, 2017, https://www.sipa.columbia.edu/ideas-lab/techpolicy/building-defensible-cyberspace . The importance of defensible technology and the benefits it can accrue to defenders in leverage over their technology was well developed previously in the 2017 New York Cyber Task Force report. This report is indebted to this 2017 effort for their articulation of leverage and its impacts.

4. Shift the Landscape for Adversaries: *CISA's new JCPO should coordinate information sharing between appropriate private and public intelligence entities, and core technology and platform vendors, to drive technical changes to disrupt adversaries.*

CISA's Joint Cyber Planning Office (JCPO) should take as a core mission the effort to encourage collaboration between core technology and platform vendors to drive technical changes in their products and services to purposefully disrupt adversary operations. Relying particularly on technical expertise from NSA-CD, JCPO should facilitate working groups between credible private threat-intelligence firms, federal civilian and military intelligence agencies, and core technology and platform vendors.

JCPO should host these working groups as a trusted convener, encouraging their use as a forum to coordinate action or technical changes between private or public entities. Represented vendors should include any commercial technology or infrastructure vendor (including telecommunications) currently included in the Enduring Security Framework. These working groups should also include all major cloud service providers in the United States, any systemically significant device, service, or component, vendors such as Cisco, Intel, Nvidia, Apple, and Broadcom, and any other parties as determined by JCPO or a majority of any working group's membership.

Actionable information sharing of this kind appears most effective in smaller trusted groups, so JCPO may set the initial number of these groups and all non-government participants should determine the working group's maximum size. Working-group participation should be capped below the agency/vendor level to emphasize operational management and be staffed by engineering, security, and threat-intelligence job roles, not government affairs or policy/partnership/public-engagement staff. Working groups should set their own meeting frequency, but it should be no less than monthly. At least one working group should be explicitly determined as a multinational venue, with appropriate determination made by the JCPO to

ICT VENDORS

» Industry seems more comfortable with partnering with CISA than the NSA. In contrast to the NSA, CISA is more well equipped to onboard someone to be a partner and interface with the public.

» I want to be clear, CISA has 'branded' itself well … but there is lingering 'question' in some quarters. I think there are lingering questions about Government period. for starters the Cybersecurity Information Act 2015 didn't help in the way it was supposed to.

» There is friction from perceived liability in cooperation and sharing. Government needs to act like collaborative, engaged, and open partners. It must be clear that this is the channel to communicate, and that there is liability protection. There is also a lot of uncertainty about the legal risks and protections. The government would benefit from affirming protections and amplifying the correct channels to share these concerns.

» The biggest challenge for the organizing authority is the varied capabilities between organizations. If we are starting an effective sharing program we need to work on balanced capabilities, sharing tools and how to action them as well as figuring out which information to share.

» There needs to be better systems for ad hoc collaboration and communication to share to different types of organizations in a timely manner, in a way that doesn't tip off the adversary.

» When it comes to sharing, there already exists informal whisper networks. We miss things because someone who wants to share doesn't know which analyst to reach out to. How to we scale and formalize the existing informal sharing networks?

» It's difficult to attribute a cyberattack to a nation state when you're an MNC with a presence in the country at question. There is a tradeoff for the freedom customers want with the risk of abuse.

» Government shouldn't help to create an 'elite' group of big companies that get vital security information that smaller companies aren't privy to. There could be anti-trust concerns, if only some companies gain access to better information and tooling.

» Success stories that highlight government law enforcement collaboration and how it gets the private sector in a better place would be valuable to show why private companies should collaborate and partner with the US Government.

» We would love to tell more success stories, but it's difficult to do that when working with the government and needing to abide by their rules. The US Government is privacy centric and likes to control information. Information comes in, but it's hard to get it to come back out. Private sector actors are limited on sharing by these rules. We would have to change the culture of transparency in areas that are very averse to transparency. Additionally, when stories turn into prosecution, talking becomes legally prohibited.

» When building partnerships or information sharing, if it is not a two-way street then there is no incentive to share again. Feedback needs to be provided that that information was helpful, and Government needs to be as upfront as possible with what that info was used for.

SECURITY VENDORS

» There are asymmetries in all sharing communities. The focus needs to be on prioritizing what actions can make the biggest impact in the shortest period of time.

A lot of exchange currently happens in informal channels because it allows for the rules to be bent and information to be shared more freely. How do we formalize this, and encourage government entities to be comfortable with this practice?

Information needs to be packaged and shared in is a way that is actionable for the receiver.

STANDARDS/ CIVIL SOCIETY

» The Joint Cyber Planning Office (NDAA 1715 established this) that is being stood up in CISA is an ideal place to stand up this work. This new office already brings together CyberCom, NSA, and CISA all in one room.

» The decision of who should be included in these working groups should not just be made based on the size of the business but based on which companies are able to take scalable action.

ICT VENDORS

» Too much of the process is based on implicit trust. Two questions that bring that out: 1. if a tool for development is found to be vulnerable, then how can you find out what parts of the code used that tool? 2. What about your suppliers? How can you quantify how much of their code has been touched by that tool? Even further out, your supplier's supplier. Loss of visibility is the nature of the problem we are attacking right now. We don't treat our CI/CD pipeline with as much value and risk as we should. Organizations focus on scaling and so moving to automated pipelines, but haven't properly assessed their risk. If we look at common CI/CD platforms, because they are all exposed to the internet, they aren't doing proper risk management against process pipelines. We need to understand where the single points of abuse are.

» Transparency has a cost. We've started a notion of shared responsibility, not so much line, but now shared fate. We want some clarity at technical operation level, but at the end of the day, its' in our interest to improve maturity of customers. We want to build the tools and guidance how to best configure, even though it might not be our responsibilities. Providing a lot of guidance to how companies and organizations set things up. We want to continue to push to make more sophisticated buyers from government.Too much focus on where data goes and sits, not enough on how software is actually developed and resultant risk posture.

STANDARDS/ CIVIL SOCIETY

» We want to focus on the lynchpin systems, not just processes. Things like IAM, developer tools, internal data flows. We need to think about the shared responsibility between the product maker and the operator. What needs to be baked in by the product maker to help the operator defend?

» If you look at what was spent in 2019 for all localities plus the extra grants this year, there really isn't enough spending from this DHS. Words aren't matching policies with the funds. 80% of the grants go to locals, do locals know how to spend cybersecurity funds? They don't have CISOS. Becomes political decisions. If your decision is to cyber insure as the first line of defense, then that's not good. We don't even know how they're spending it. Before we increase grants, we need to identify if the program is useful in the first place for cybersecurity. Grant conversation is getting a lot of attention, but need to understand how little is spent and what it is being spent on.

SECURITY VENDORS

» The older the code, more likely it is to have high vulnerability density. So where's the 15 year old codebase we need to retire?

facilitate at least limited information sharing to, and within, the group.

5. Develop a Lifecycle Security Overlay: *The bulk of existing certification and standards for secure software focus on development rather than deployment; NIST should work with industry to produce consensus best practices on secure software deployment and lifecycle support, including tools to automate and implement these practices in developer workflows.*

NIST should lead a multi-stakeholder process over the next 3–6 months to work with industry in developing a software supply chain Lifecycle Security Overlay to NIST SP 800-53.[176] This effort should wrap in controls from existing families, the new supply-chain family in 800-53 rev. 5, and best practices collected in the Secure Software Development Framework (SSDF) and related industry and open-source publications like the BSA Framework for Secure Software.[177] This recommendation builds on the strong network and expertise of NIST, and follows on previous recommendations to anchor technical security obligations in standard-setting organizations.[178] Dozens of the software supply-chain attacks discovered in the last 10 years target weakly secured code signing certificates, update servers, and other tools for software deployment. The security of software is important but addressing the pace and scale of software supply chain attacks

EXECUTIVE BRANCH

If transparency is too big a step, need a radical rethink. What are the policy tools to encourage transparency? Going back to cloud data approach, they need to create tools that enable a lot more transparency. When we think about solutions that are measurable, how much do we need a modular pipeline for development? We are pretty far from being able to do this. How much can we retrofit existing tools to get this trust? Modern tools enable a lot more than just a legacy pipeline. How much do we lean there? Where's the optimal investment ratio?

176 This recommendation was originally proposed, and includes additional applications, in the predecessor to this report: Herr, et al., *Breaking Trust*.

177 Danielle Kriz, "Improving Supply-Chain Policy for U.S. Government Procurement of Technology," Council on Foreign Relations, October 28, 2015, https://www.cfr.org/report/improving-supply-chain-policy-us-government-procurement-technology. The Council on Foreign Relations has similarly highlighted the need for affected vendors to receive "specific, targeted threats and technical indicators," and for US policymakers to "facilitate more actionable cyber-threat information sharing, including informing vendors when intelligence agencies find vulnerabilities in supply chains or products," in order for vendors to appropriately defend their supply chains.

178 Ariel (Eli) Levite, "ICT Supply Chain Integrity: Principles for Governmental and Corporate Policies," Carnegie Endowment for International Peace, October 4, 2019, https://carnegieendowment.org/2019/10/04/ict-supply-chain-integrity-principles-for-governmental-and-corporate-policies-pub-79974.

demands we pay more, if not equal attention, to how that software is deployed and supported.

Sector-specific agencies implement the overlay: The NIST overlay team should support appropriate sector-specific agencies to set up implementation working groups with industry partners focused on using this overlay in their own development and contracting with third parties. NIST should feed requests for more specific controls or guidance into an eighteen-month revision cycle, producing additional guidance or changes to the overlay as needed—for example, for industrial control systems in the energy sector.[179]

Bring the overlay to the cloud: Many software developers rely, in whole or in part, on cloud vendors to host, distribute, and maintain their codebases. Industry can assert moral leadership on software supply-chain security issues, realize practical financial advantages by offering public reference implementations of the overlay in their services, and lower the complexity of secure lifecycle practices for customers. Major cloud providers should build on existing industry organizations and collaboration to lead joint development of these reference implementations and make them freely available to their current, and prospective, users.[180]

6. Give SBOM a Glide Path to Success: *Federal cyber leadership must ensure SBOM has a gradual pathway to adoption, as both a technical standard and valuable source of data on software transparency and risk, without abusing it as a silver-bullet.*

The Software Bill of Materials (SBOM) is a formal record containing the details and supply-chain relationships of the various components used in building software. This information provides software users insight into their true exposure to software supply-chain vulnerabilities and attacks. SBOM has tremendous potential value to developers and defenders alike. An SBOM allows the developer to make sure components are up to date and serves as the foundation for more advanced integrity checks and process monitoring. In the hands of customers, this kind of information creates opportunities for large enterprises and policymakers to quickly respond to new attacks, and also to hold developers accountable to policies and best practices and rigorously measure changes in vendor practices. Broad adoption of an SBOM would provide a rich source of data to better manage the risks of software from individual users to whole codebases and languages. Transparency into software supply chains is a critical first step toward organizations being able to meaningfully assess, and then manage, the risk they assume from this code. This kind of transparency would help users manage risk from several classes of observed attacks on open-source projects, including typosquatting, as well as support stronger integrity controls as might have caught the malicious DLL in SolarWind's Orion software.

However, the SBOM is not a magic wand for software security. The value of transparency lies in the effective use of that data. Users and policymakers must decide how best to take advantage of it, and the uses are myriad. Data formats and tools are available today—and are being used—but they have not yet been proven at scale. SBOM has value for those who use it now, but much of the broader value depends on widespread adoption and holding true to the interoperability assumptions asserted by its proponents.[181] SBOM

EXECUTIVE BRANCH

» My mantra has been since December, SBOM almost would not have been stopped this attack. SBOM is a necessary step for all the things we are going need moving forward. We can't do simple transparency without it.

ICT VENDORS

» There is effort to get cloud providers to provide these process metrics to customers in time. May be way too big for this discussion today, but this is somewhere the USG can really come in and offer assistance to define our unique social contract. +1 on the SBOM framework.

179 Michael L. Papay, et al., "Raising the Bar on Cybersecurity and Acquisition," Cybersecurity Initiative, George Washington University, 2014, http://cchs.auburn.edu/_files/raising-the-bar-on-cybersecurity-and-acquisition.pdf; "Report on Securing and Growing the Digital Economy," President's Commission on Enhancing National Cybersecurity, December 1, 2016. This report urged NIST to conduct research on supply-chain risk focused on organizational interdependencies, recommending that it "identify methods that assess the nature and extent of organizational interdependencies, quantify the risks of such interdependencies, and support private-sector measurement against standards of performance." Various organizations have highlighted the importance of ensuring that private-sector entities implement NIST standards and voluntary practices—for instance, by making them more accessible for all stakeholders.

180 A good starting point would be to involve Amazon, SAP, Microsoft, Google, Oracle, Dell, and IBM.

181 "Roles and Benefits for SBOM Across the Supply Chain," US Department of Commerce, National Telecommunications and Information Administration, September 3, 2019, https://www.ntia.doc.gov/files/ntia/publications/ntia_sbom_use_cases_2019_0904.pdf.

has been nurtured for years by a group of merry practitioners and security boffins involving some of the most sophisticated software-developing and software-consuming organizations in the United States. SBOM's adoption must be deliberate, starting with a handful of industries and clear timelines for experimentation, feedback to the broader community, and ultimate adoption. Abusing that potential to create a cure-all, one-size-fits-all solution for software security would do more harm than good, and would squander a significant opportunity.

The National Telecommunications and Information Administration (NTIA) should continue to evangelize on the role and utility of software transparency, leading a standing multi-stakeholder working group on SBOM while it pushes toward inclusion in broader international standards for specific sectors and broader technical guides. The federal CISO and GSA should work with the national cyber director (NCD) and the existing SBOM working groups to integrate SBOM requirements into selected new ICT procurement and ongoing sustainment contracts. The NCD should work with CISA, DISA, and other appropriate agencies to experiment with different uses of SBOM data to manage cyber risk and publish case studies with practical software tools for the most successful examples.

7. Apply the Overlay: *The lifecycle security overlay is a valuable tool to ensure more mature and less risky ICT vendors for the federal government; GSA and DoD should integrate the overlay into existing vendor security-maturity programs.*

Very little is to be gained from another standards document developers have to download in pdf form and make their own determination about how to implement. Part of the development of this Overlay is driving implementation through existing product and vendor risk-assessment programs, to provide incentive to make these controls practicable. The GSA should implement this overlay as criteria in its evaluation of vendor maturity through its VRAP as part of Polaris. GSA should work with 18F and other partners, as appropriate, to implement as much of the overlay into real-time metrics as possible. Evaluation against the overlay should be used as both criteria for new contracts and vendor selection, as well as a measure of vendors' ongoing security performance by agencies.

Integrate the overlay with CMMC: The DoD should integrate this supply-chain maturity model as part of its CMMC program and establish a level of performance required for prime contractors. The DoD should further implement these performance measures as new contracting requirements for information-technology procurement and the under secretary for acquisition and sustainment (USD(A&S)) should support a pilot program implementing the overlay as a real-time vendor security measure in line with GSA's program.

8. Do Not Leave Open Source Behind: *CISA should establish an open-source security team and help fund targeted grants to improve the integrity and secure management of critical open-source projects and packages.*

Open-source code was not at the heart of the Sunburst crisis, but it is a critically underdefended attack vector in the software supply chain. Software supply-chain attacks before and since Sunburst show plainly that zeroing in on proprietary code simply because it was the vector in this case could court disaster. Open-source software constitutes core infrastructure for major technology systems and critical software pipelines.[182]

DHS CISA should create a small (six- to eight-person) open-source security evangelism and support office.

ICT VENDORS

» Telling people what they need to buy, worked will for PCI/DSS, but there are limitations because its only able to manage a well scoped and well defined risk, and not risks across the board. We worked with ** institute to scope out which security practices actually had statistical outcomes? Topmost security practice is proactive tech refresh strategy. Statistically speaking, if this is true, if you get a lot of benefits from refreshing, then this may mean problems for orgs who can't afford that, and raise another argument for moving to the cloud. But thirdly, we may have to rethink how we fund cybersecurity in general. Needs to be ongoing infusion of money to continue updating infrastructure, esp in critical infrastructure. There is a framework for legacy systems. But OMB isn't given the authority, still agency by agency basis. Not all legacy is bad, but still. I think the trend for some elements of government software development, that typically uses non-traditional vendors, but also raises the spectre if some of that goes outside of the procurement context?

LEGISLATIVE BRANCH

» Are there ways to make Federal guidance more navigable? CISA proposed making available basic configuration to prioritize some protections.

182 Herr, et al., *Breaking Trust*; Goodin, "New Type of Supply-chain Attack Hit Apple, Microsoft and 33 Other Companies", Ars Technica, February 16, 2021, https://arstechnica.com/information-technology/2021/02/supply-chain-attack-that-fooled-apple-and-microsoft-is-attracting-copycats/.

This group should help high-value asset programs identify common open-source dependencies, encourage collaboration between the United States and allies in supporting the security of open-source projects identified as critical by the office, and act as a community liaison/security evangelist for the open-source community across the federal government. This Open-Source Security office inside of CISA should participate in the JCPO working-group meetings to help integrate important open-source project owners, where appropriate, and funnel guidance back to open-source community partners. This office would require new funding in the long term but could be spun up out of an existing program and initially staffed using similar authorities as those used to bring outside cybersecurity experts in to support Operation Warp Speed and CISA's work with the health sector.[183]

The US Congress should appropriate suitable funds, no less than $35 million annually, along with unambiguous grant-making authority to CISA to support baseline security improvements in critical open-source security packages. These funds should be administered through both an open, rolling grant-application process and spot grants of up to $500,000 to the highest-risk open-source codebases, as determined by CISA and approved or modified by the NCD. Grant implementation and evaluation should be overseen by CISA in conjunction with the US Computer Emergency Response Team (US-CERT). A portion of these funds should also be used to support the purchase of project management, ticketing, and coordination tools by these open-source projects, so that they can better utilize volunteer technical labor contributed by others.

9. Change an Architecture, Change the World: *Sunburst exposed how important major cloud service providers' threat models are to the security of their customers; the NCD should drive a regular convening and review of these models to help surface and advocate for appropriate technical reforms and identify supportive policies.*

The Sunburst adversary was remarkably successful moving through victim networks after initial compromise, in large part because of its successful abuse of IAM systems. As cloud computing becomes more common and its deployment into mixed on-premises/cloud environments more significant, the likelihood that a low-probability, high-consequence failure might affect sensitive users and data rises. The largest cloud vendors must ensure their threat models for these systems, and corresponding engineering and security investments, keep up with an evolving threat landscape.[184]

The office of the NCD, supported by NSA-CD, should host a quarterly convening of suitable industry CISOs and product security design leadership. These sessions are intended to drive valuable shifts to the core

STANDARDS/ CIVIL SOCIETY

» No machine is going to have 100% detection. Cloud has a lot of promise, but with industry and government, the real effect of cloud is shifting responsibility from detection and response to owner to the vendor. Response in the cloud by YOURSELF is basically absent. Along with that goes the monitoring of it. Larger M&M security model. If it gets breached, and SSO breached, then nobody is minding the store at that point.

No good feel for what security I am actually buying and what the minimum benchmarks are. I want to do my job well but just don't know enough or have enough clear guidance. Abandon hope, no matter what I do, that I may not have the type of capabilities that I should have?

ICT VENDORS

» Who is best positioned to actually drive change? CSPs and large providers—tremendous immaturity on buyer side. Not so much shared responsibility with clean line between vendor and customer. More shared fate. If a customer has a problem, regardless of whether we've done everything right, it's in our interest to mature their security. Either giving insight or building safer, foolproof tools with good config guidance. In an ideal world, IT admins don't have to worry At what point do vendors have to take on this responsibility now? SolarWinds shouldn't have to think about the build process is safe, because they should just be able to assume the build process is just secure.It is crazy that point in time assessments are still the standard. Need to look at the process that was used to make the software. … do they do architectural analysis, spot check artifacts, where is the threat model for this piece of the software … Need to hold them to process.

183 "CISA Adds Top Cybersecurity Experts to Join COVID-19 Response Efforts," Cybersecurity and Infrastructure Security Agency, July 22, 2020, https://www.cisa.gov/news/2020/07/22/cisa-adds-top-cybersecurity-experts-join-covid-19-response-efforts.

184 Charles Clancy, et al., "Deliver Uncompromised: Securing Critical Software Supply Chains," MITRE, January 2021. This recent MITRE report includes discussion of this sort of protection of linchpin technologies in a section discussing Crown Jewels defense, alongside other useful technical protections for software integrity.

architecture of the largest commercial cloud providers and, thus, impact the widest set of users.[185] At these sessions, participants should submit documentation detailing their threat model for systems designated as "linchpins" by the NCD supported by OSTP, CISA, the federal CISO, and other entities as appropriate. Subsequent submissions include concise description of engineering investments and security design changes made in response to feedback to the submitted threat models.

These quarterly meetings should be used to review contentious changes proposed by the JCPO working groups or elsewhere. CISA's JCPO should brief findings and trends from these working groups to the office of the NCD on a regular basis. Where proposed changes to technology design or configuration have not been adopted or remain in question, NCD should leverage any of its policy tools or ongoing strategy processes, including this quarterly convening, to advocate for the changes with industry and further coordinate them with other ecosystem security initiatives the office has in place.

Enhance the Adaptability of Federal Cyber Risk Management

Brittleness is the enemy of an effective and adaptable response, yet much of the current risk-management landscape is premised on slow and circuitous processes. The result is an authorization pipeline significantly better at keeping technologies out of users' hands than at flowing good information and defensive updates rapidly to the organizations in need of them. The most common source of failure to comply with the OMB Circular A-130 was cited as lack of sufficient guidance and excessive complexity.[186]

Rather than solving the problem with a new program, these recommendations suggest the federal government can get faster and leaner, providing a rapid onboarding pathway for mature cloud providers' services subject to more effective security and design reviews, enhancing executive-branch capacity to eliminate or consolidate policies, and to better leverage capabilities to monitor and enforce baked into cloud deployments.

10. Create a Trusted Traveler Program for FedRAMP: *Use an express lane through FedRAMP to rapidly onboard new cloud services reliant on carefully reviewed and better secured linchpin systems per Recommendation 9.*

The US Congress should direct GSA's FedRAMP to create a program for rapid onboarding of new cloud services reliant on systems assessed and blessed through the NCD's linchpin review process (Recommendation 9) as determined by a list issued by the office of the NCD. It is in the federal government's interest to push broader adoption of more secure systems as fast and as far as possible. With industry, a robust mechanism to speed the authorization of new services through FedRAMP is one of cloud service providers' loudest and most consistent demands.

Any company participating in the NCD Linchpin Review process and the JCPO working groups should receive automatic and continual access to this rapid-onboarding program through FedRAMP. The onboarding should institute a rapid security review, ensuring services go from submission to authorization in less than thirty days, with the goal of shortening this timeline to one working week within two years. Any change in FedRAMP authorities to accomplish this program must be matched by sufficient increases in funding to accommodate this significant shift toward more timely authorization.

"SUNBURST IS NOT A ONE-OFF SUCCESS BY THE ADVERSARY, BUT RATHER THE PRODUCT OF SYSTEMIC INADEQUACIES THAT COULD QUICKLY REVEAL THEMSELVES AGAIN IN THE FUTURE IF NOT ADDRESSED."

185 This discussion of operational collaboration, and its impact on critical industries beyond core technology vendors, is a central theme of the recently released 2021 New York Cyber Task Force Report. "Enhancing Readiness for National Cyber Defense through Operational Collaboration," Columbia University School of International and Public Affairs, 2021, https://www.sipa.columbia.edu/sites/default/files/embedded-media/NYCTF – Enhancing Readiness for National Cyber Defense through Operational Collaboration.pdf.

186 "Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks."

11. Evolve and Default to Secure: *The federal CISO should lead a rolling review of federal cyber risk-management policies, together with the NCD leveraging CISA and OMB's BoD authority to make any recommendations permanent absent default-to-deny appeal to the NCD.*

Empower the federal CISO in conjunction with the NCD, supported by CISA, NSA-CD, and the FASC to conduct a rolling strategic review/architectural audit of federal enterprise cyber risk management. Recommendations made by the review become provisional policy within thirty days through Binding Operational Directive (BoD) from CISA and approval by the office of the federal CISO on behalf of OMB. Agencies may review and appeal for changes, modifications, or budgetary modification to support the new policies to the office of the NCD. NCD can rule on these appeals and recommend budgetary adjustments to OMB through the office of the federal CISO. Any request not reviewed or granted within thirty days becomes standing policy. The NCD should also use its budgetary review authority to address non-compliance with these policies.

12. Govern Through the Cloud: *As cloud adoption widens, the federal CISO and CISA should apply federal cyber risk governance directly through those cloud services' built-in telemetry and policy enforcement tools.*

One of the structural advantages of cloud computing is that it is not a single product but, rather, a stack of technologies enabling providers to readily track behaviors within their cloud environment and provide this data to users. The federal government must define its own governance strategy for cybersecurity, but has an opportunity to enforce cybersecurity policies on agencies and departments and collect data-tracking implementation and performance of these policies directly through cloud services. Many of these policy-enforcement mechanisms and data-collection tools are already "baked in" to cloud services; the challenge is mostly in determining how to take advantage of them.

The federal CISO and CISA should immediately allow agencies and departments to satisfy any guidance or directive regarding the security and integrity of their IT systems with a feature or data stream directly from any of their authorized cloud services. CISA should immediately permit satisfaction of a BoD or related guidance be demonstrated by an agency or department switching on an appropriate data stream from their cloud services and pointing it to CISA for real-time monitoring. The federal CISO should seek to develop new guidance and cybersecurity governance documentation that maps to widely used cloud service products, features, and tools to prevent the need for agencies or departments to determine their own manner of implementation.

STANDARDS/ CIVIL SOCIETY

» Anything you can do to leverage bureaucratic inertia is the way to go. What does default to secure look like?What are the organizational imperatives driving rigidity. Centralize the bottom of the stack, diversify and specialize up top. Manageable number of service providers (5-10) who can better coordinate and share info, acting closer to a single unit.To me the real key is looking at the blockers for implementing 25 years of legislation. There are underlying motivations, agency interests, resources, etc. What reasons have held up implementation, not just bureaucracy, that drive the conflict?The .gov community is getting used to these things from CISA, and having an opt out mechanism until CISA goes back and checks in. Now the CISOs and CIOs have a tangible document to bring to leadership and force action.

» Part of BODs was the ability to drive resources, an emergency directive normally costs time. Emergency directives are patching, and people doing work not contracts, or finances. BODs have a more financial impact, ...It's hard to direct people to make those big changes, it takes more capital and time and isn't necessarily how organizations want to spend their resources.

LEGISLATIVE BRANCH

» A lot of what we're talking about is [CISA's] legal authority. I've been impressed with their ability to execute emergency measures, but their BODs have been more of a mixed bag. National Cyber Director's office, for exactly this reason, has language to [drive budgetary resources].

STANDARDS/ CIVIL SOCIETY

» Some agencies can get out of the cybersec business entirely, lean on the service provider. Focus on building enduring, overarching frameworks that allow plug in of the mutable below.The lower you are in the stack, toward the transport layer and such you want more centralization. The more you get to agency operations, the more you want specialization. You will never fully centralize this in the federal government. You need a few key centers of excellence... how much infosec governance can you bake into a cloud platform (vice USG) — how could you structure USG to "catch" that?

ICT VENDORS

» We need to get on a good glide path to solve some of these fundamental problems right now. I think the solutions there are automation, automated measurement, systems monitoring their own health, security coprocessors, keeping an eye on the environment and adjusting in real time, ... All 3 hyperscalers are doing automated cloud instrumentation key for fundamentals.Thinking about this amongst the big customers of the cloud. Ideally in a few years, it'll be the whole compliance requirement, all measured in real-time

» There is effort to get cloud providers to provide these process metrics to customers in time. People should be able to see this [metrics] information from the vendor.We have had the most success by going through people's suppliers/ IT to offer support. Now we need to just offer it instead of having it be offered as a security package to buy.

CONCLUSION

The problem is not that "software is eating the world." Rather, it is our failure to confront the world that software has wrought. Efforts to improve the baseline defensibility of the technology ecosystem and reform federal cybersecurity policies must be informed by the strategic logic of the intelligence contest in which the United States and its allies are engaged. The enormous volume and rapid pace of activity in cyberspace are, in part, due to the large and increasing number of actors armed with malicious cyber capability. The tools necessary for cyber operations, from the basic to the complex, provide malicious capabilities and are also force multipliers, enabling comparatively weak actors to have outsized impacts. Actors like the United States are still the big fish, but even small fish have teeth with the potential to weaken larger adversaries, and the waters provide no safety.

There is a well-recognized spectrum of state support and coordination with non-state groups.[187] Actors with less sophistication are still able to utilize the weaknesses of the software supply chain to hit a disproportionate number of targets—and from there can choose to exploit only those that are valuable and manageable. The 2017 Kingslayer case has been attributed to a Chinese group responsible for previous intrusions against services and manufacturing firms, targets that included sensitive intellectual property aligned with past Chinese-state espionage targets, but the group has not been positively linked to government agencies. Tortoiseshell, a non-state hacking group with no known state affiliation, was linked to an exploitation of eleven Saudi IT companies as a part of a larger software supply-chain intrusion in 2019.[188] This group's ability to leverage both custom and off-the-shelf malware to successfully execute a software supply-chain incursion against eleven companies without access to the resources of a state actor illustrates the lowering threshold of action for these types of incidents, providing prospective financial benefits and access for future operations. While seventeen of the intrusions against software updates profiled in the Breaking Trust dataset are attributed to states, the other nineteen remain unknown or positively linked to criminal groups.

There is a bias in this reporting toward the English-speaking world, and the United States and Western Europe in particular, further obscuring the development of this intelligence contest in the global South, as well as West and Central Asia. Offensive cyber capabilities are available to states like the United Arab Emirates and Egypt, both in the semi- and self-regulated markets.[189] Even training and technical support are offered as part of these packages to supplement tools and techniques freely available on the Internet. These tools, from the basic to the complex, not only provide malicious capabilities but are force multipliers, enabling comparatively weak actors to have outsized impacts. Sunburst and most of the case studies above may have been attributed to state actors, but this kind of access is by no means solely accessible to them. Non-state actors will only continue to increase in skill and abundance.

The cyber domain is a realm of intense interconnectivity that underpins much of daily life and national security. The discovery late in 2020 that Sunburst malware had infected not only thousands of private networks, but also US government agencies, led some spectators to embrace alarmist views of this event as the first step in full-fledged cyber war.[190] Sunburst was a masterclass in intelligence operations, the effects of which are likely to continue rippling out over the coming years, but it was not an act of war. The compromise of so many federal and high-value private-sector networks likely yielded valuable information, and it provided access sufficient for more disruptive assaults like introducing disinformation, deletion, or subtle alteration of data, though there is not yet any public evidence of this on target networks, and all indications released publicly suggest this was indeed a successful act of espionage.

Sunburst was not an isolated or unprecedented incident. The presence of similar intrusions from major US

187 Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge: Cambridge University Press, 2018).

188 Herr, et al., *Breaking Trust*; "Tortoiseshell Group Targets IT Providers in Saudi Arabia in Probable Supply Chain Attacks," Symantec, September 18, 2019, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/tortoiseshell-apt-supply-chain.

189 Winnona DeSombre, et al., *Countering Cyber Proliferation: Zeroing in on Access-as-a-Service*, *Atlantic Council*, March 2, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/countering-cyber-proliferation-zeroing-in-on-access-as-a-service.

190 Herb Scribner, "An Act of War? U.S. Government, Businesses Hit by Cyberattack," MSN December 18, 2020, https://www.msn.com/en-us/news/politics/an-act-of-war-us-government-businesses-hit-by-cyberattack/ar-BB1c37rF

adversaries against comparable types of software and targets over the past decade, including those profiled here and more in the Breaking Trust dataset and elsewhere, underline that fact.[191] Sunburst and the other seven cases of software supply-chain incursion discussed in this report are a small sample illustrating the impressive capability of these types of incidents in the global intelligence contest. In this contest, state and non-state actors aim to gather greater relevant information on real and perceived adversaries, while denying reciprocal benefits to the same.

In the aftermath of Sunburst, defenders must find leverage of their own and enhance the speed of response as they play out engagements on their home territory. This should take place in parallel with improving real-time information sharing with offense, persistently engaged with adversaries on intermediary and hostile networks. Policy responses from the United States and allies must become sharper and better coordinated—acknowledging a degree of intelligence failure alongside impactful industry lapses. Neither governments nor their citizens can afford the plodding pace of many existing policy-coordination mechanisms, nor underinvestment in nascent but promising reforms. Industry must also recognize its own role in precipitating this crisis, owing to shortfalls by some to adhere to reasonable or adequate security practices and continuing failure by others to address security concerns in major products, even where those do not fall neatly into the category of a recorded vulnerability.

Breaking trust is non-trivial and restoring it will require that much more concentrated purpose and clarity of outcome at a time when both are in short supply. For the technology industry, the insecurity of software supply chains is a crisis in waiting. For the national security establishment, it is a crisis realized. But, the short-term response to Sunburst has demonstrated the extraordinary technical and collaborative capability of the security community. Capability to drive new investments to secure the load-bearing bugs, implement revised policies and straightforward tools to make code deployment easier, and expand on community-led efforts to bring supply-chain security further out of the darkness of the byzantine and proprietary, and into the harsh light of day.

Trust in software is not created in a vacuum, rarely by any single vendor, and never in isolation from the user—government or otherwise. Indeed, trust in software one did not build may be practically impossible, leaving the task one of establishing and rigorously enforcing tolerable levels of distrust in others' code.[192] Getting the long game right is essential to maintaining the strength and security of the United States in this evolving contest for information, and with it the chance for leverage in the cyber domain. Improvements will benefit from leadership, some measure of new talent, and resources. But, they will also demand persistence, at least as much as that of the adversary, if not a measure more.

"BREAKING TRUST IS NON-TRIVIAL AND RESTORING IT WILL REQUIRE THAT MUCH MORE CONCENTRATED PURPOSE AND CLARITY OF OUTCOME AT A TIME WHEN BOTH ARE IN SHORT SUPPLY."

191 Herr, et al., *Breaking Trust*.

192 Ken Thompson, "Reflections on Trusting Trust," *Communications of the AMC,* August 1984, https://users.ece.cmu.edu/~ganger/712.fall02/papers/p761-thompson.pdf.

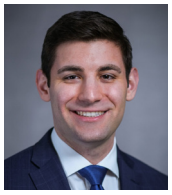
ABOUT THE AUTHORS

Dr. Trey Herr is the director of the Cyber Statecraft Initiative under the Scowcroft Center for Strategy and Security at the Atlantic Council. His team works on cybersecurity and geopolitics including cloud computing, the security of the internet, supply chain policy, cyber effects on the battlefield, and growing a more capable cybersecurity policy workforce. Previously, he was a senior security strategist with Microsoft handling cloud computing and supply chain security policy as well as a fellow with the Belfer Cybersecurity Project at Harvard Kennedy School and a non-resident fellow with the Hoover Institution at Stanford University. He holds a PhD in Political Science and BS in Musical Theatre and Political Science.

William Loomis is an assistant director with the Atlantic Council's Cyber Statecraft Initiative, within the Scowcroft Center for Strategy and Security. In this role, he manages a wide range of projects at the nexus of geopolitics and national security with cyberspace. Prior to joining the Atlantic Council, he worked on market research and strategy at an emerging technology start-up in Madrid, Spain. Originally from New York, he holds a BA in Political Science, with a focus on International Relations and Securities Studies from Colgate University.

Emma Schroeder is an assistant director with the Atlantic Council's Cyber Statecraft Initiative, within the Scowcroft Center for Strategy and Security. Her focus in this role is on developing statecraft and strategy for cyberspace that is useful for both policymakers and practitioners. Originally from Duxbury, Massachusetts, she holds an MA in History of War from King's College London's War Studies Department. She also attained her BA in International Relations & History, with a concentration in Security Studies, from the George Washington University's Elliott School of International Affairs.

Stewart Scott is an assistant director with the Atlantic Council's GeoTech Center. In this role, he manages a wide range of projects at the intersection of emerging technologies and dynamic geopolitical landscapes. He also conducts research and provides written analysis for publication on Atlantic Council platforms and works on joint projects with other centers in the Atlantic Council. Stewart earned his BA from Princeton University at the School of Public and International Affairs along with a minor in Computer Science. His course of study centered on misinformation, social media policy, online extremism, journalism, and American political and economic history. He joined the Atlantic Council after interning with its Cyber Statecraft Initiative in the Scowcroft Center for Strategy and Security.



Simon P. Handler is the assistant director of the Atlantic Council's Cyber Statecraft Initiative, within the Scowcroft Center for Strategy and Security. In this role, he manages a wide range of projects at the nexus of geopolitics and international security with cyberspace. Prior to joining the Atlantic Council, he served as a special assistant in the United States Senate, where he worked on foreign policy issues. During his time on the Hill, he was a congressional fellow with the Wilson Center's Congressional Cybersecurity Lab and Congressional Artificial Intelligence Lab, and completed the East-West Center's Congressional Staff Program on Asia. He holds a BA in International Relations & Global Studies, with a concentration in International Security, and Middle Eastern Languages & Cultures from the University of Texas at Austin.

Tianjiu Zuo is a research associate at the Atlantic Council's Cyber Statecraft Initiative, within the Scowcroft Center for Strategy and Security. He primarily focuses on the risks and implications of cloud computing and examines cyber-related national security issues. He is currently a sophomore at Duke University, pursuing a BS in economics and a BA in public policy.

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*Richard W. Edelman
*C. Boyden Gray
*Alexander V. Mirtchev
*John J. Studzinski

TREASURER
*George Lund

DIRECTORS
Stéphane Abrial
Todd Achilles
*Peter Ackerman
Timothy D. Adams
*Michael Andersson
David D. Aufhauser
Colleen Bell
*Rafic A. Bizri
*Linden P. Blue
Philip M. Breedlove
Myron Brilliant
*Esther Brimmer
R. Nicholas Burns
*Richard R. Burt
Michael Calvey
Teresa Carlson
James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
*Helima Croft
Ralph D. Crosby, Jr.
*Ankit N. Desai
Dario Deste
*Paula J. Dobriansky
Joseph F. Dunford, Jr.
Thomas J. Egan, Jr.
Stuart E. Eizenstat
Thomas R. Eldridge
*Alan H. Fleischmann
Jendayi E. Frazer
Courtney Geduldig
Thomas H. Glocer
John B. Goodman
*Sherri W. Goodman
Murathan Günal
Amir A. Handjani
Katie Harbath
Frank Haun
Michael V. Hayden
Amos Hochstein
*Karl V. Hopkins
Andrew Hove
Mary L. Howell
Ian Ihnatowycz
Wolfgang F. Ischinger
Deborah Lee James
Joia M. Johnson
*Maria Pica Karp
Andre Kelleners
Astri Kimball Van Dyke
Henry A. Kissinger
*C. Jeffrey Knittel
Franklin D. Kramer
Laura Lane
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mark Machin
Mian M. Mansha
Marco Margheri
Chris Marlin
William Marron
Neil Masterson
Gerardo Mato
Timothy McBride
Erin McGrain
John M. McHugh
H.R. McMaster
Eric D.K. Melby
*Judith A. Miller
Dariusz Mioduski
*Michael J. Morell
*Richard Morningstar
Dambisa F. Moyo
Virginia A. Mulberger
Mary Claire Murphy
Edward J. Newberry
Thomas R. Nides
Franco Nuschese
Joseph S. Nye
Ahmet M. Ören
Sally A. Painter
Ana I. Palacio
*Kostas Pantazopoulos
Alan Pellegrini
David H. Petraeus
W. DeVier Pierson
Lisa Pollina
Daniel B. Poneman
*Dina H. Powell McCormick
Robert Rangel
Thomas J. Ridge
Lawrence Di Rita
Michael J. Rogers
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Rajiv Shah
Wendy Sherman
Kris Singh
Walter Slocombe
Christopher Smith
James G. Stavridis
Michael S. Steele
Richard J.A. Steele
Mary Streett
*Frances M. Townsend
Clyde C. Tuggle
Melanne Verveer
Charles F. Wald
Michael F. Walsh
Gine Wang-Reese
Ronald Weiser
Olin Wethington
Maciej Witucki
Neal S. Wolin
*Jenny Wood
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Ashton B. Carter
Robert M. Gates
James N. Mattis
Michael G. Mullen
Leon E. Panetta
William J. Perry
Colin L. Powell
Condoleezza Rice
Horst Teltschik
John W. Warner
William H. Webster

**Executive Committee Members*

List as of February 8, 2021

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council
1030 15th Street, NW, 12th Floor,
Washington, DC 20005
(202) 463-7226, www.AtlanticCouncil.org