

UNISMUNC XII



Committee: The Collapse of the
Internet Order

Topic: The SolarWinds Attack of 2020

Committee Type:
Specialized

December 6, 2026



<https://www.brookings.edu/articles/the-danger-in-calling-the-solarwinds-breach-an-act-of-war/h>

Director: Aanya Sapra

Chair: Aria Yen

Table of contents:

Conference Schedule:	3
Letter From Chair/Director:	7
A Brief Overview of the Committee:	9
Written Papers:	11
Topic Background:	12
Current Situation:	14
Delegates and/or Bloc Positions:	16
Questions to Consider:	24
References:	25

Conference Schedule:

Opening Ceremonies

8:00 am - 9:00 am

Committee Session I

9:00 am - 1:00 pm

Lunch Break

1:00 pm - 2:00 pm

Committee Session II

2:00 pm - 5:30 pm

Closing Ceremonies

5:30 pm - 6:15 pm

Conference Policies:

UNISMUNC X aims to foster debate, giving students the opportunity to explore a range of topics and encouraging collaboration and teamwork among delegates. Be that as it may, UNIS stresses the importance of respectful language as UNISMUNC XII will see delegates debating topics that, at times, may be heated or passionate. MUNEX encourages you to remember to stay respectful and mindful of the other students around you. We are so excited about this conference and trust that no issues will arise. The following expectations and policies are designed so that every delegate gets the most out of UNISMUNC XII.

Attire:

The Dress Code for UNISMUNC XII is formal Western business attire, and all delegates are expected to comply with this. Exceptions may be made for character purposes in crisis committees at the chair's discretion. If you have an idea for an outfit for a crisis committee that does not fall into the parameters of traditional Western business attire, please ask your chair for permission before wearing the outfit.

Committee Assignments:

Committee assignments will be made on a first-come, first-served basis based on preference as communicated by the delegation's advisors (or individual delegates in the case of independent delegates), in order of receipt of preference. Before being assigned to a committee, payment must be received. If payment is not submitted in a timely manner, delegations face the risk of not receiving committee assignments of their choice.

Expectations in Committee:

As you engage in debates, we ask that delegates maintain politeness and respect at all times. While we recognize that you are representing your country's views, it is essential to express these perspectives without crossing the line into disrespectful or confrontational behavior.

Please respect one another when delegates are giving speeches. Only one delegate may speak at a time during moderated caucuses. To speak during a moderated caucus, you must raise your placard and wait to be recognized by the chair. During speeches, no ad hominem attacks will be

allowed, should they occur, the subject will have the right to reply. Remember to be cognizant of your words and actions, and to listen to everyone's views and positions.

The Committee Chairs and Secretariat members are responsible for determining disruptive behavior.

Examples of disrespectful behavior may include but are not limited to:

- Speaking without being recognized,
- Use of cell phones,
- Note-passing unrelated to the committee,
- Use of technology when not allowed,
- Verbal, physical, or sexual harassment of other delegates.

The pre-writing of any resolution/directive clauses, crisis notes, or speeches is strictly forbidden and will be penalized. This does not include opening remarks. This does not include any writing during the lunch break, as UNISMUNC XII committees standardly operate with 'working lunches'.

UNISMUNC has a zero-tolerance policy for any plagiarism. This includes position papers, speeches, and resolutions. Improper citation of quotes and references may result in disqualification from awards or further disciplinary action at the discretion of the chairs.

Pricing:

Please see the registration section for more information. Details on committee assignments are below.

Spectators:

Please be aware that UNISMUNC XII does not allow unregistered spectators. Student spectators are strictly prohibited. All advisors and delegates must be registered and pay the required fee(s). Non-compliance with this policy will result in exclusion from future invitations. We expect all participating delegations to respect this policy. The Secretariat reserves the right to have any

unregistered spectators removed from committee chambers and escorted off of the premises if necessary, as they see fit.

Technology:

All crisis committees are strictly no-tech. Neither laptops nor cell phones will be permitted during committee sessions in crisis committees.

General Assembly (GA) committees allow technology exclusively for the purpose of resolution writing. Delegates will be permitted to use their laptops to work on resolutions during unmoderated caucuses and outside of the committee chamber when allowed by the chair. It is, however, not permitted to use technology when a fellow delegate is speaking or during committee chambers during moderated caucuses. This includes your own speeches, so please write any notes by hand or have your opening remarks printed before the conference.

Awards Criteria:

UNISMUNC XII Chairs, Diasas, and, in the case of crisis committees, Crisis Directors will work together to holistically evaluate delegates based on their performance throughout the entire day of debate. This includes:

- speeches given during moderated caucuses,
- performance during unmoderated caucuses (not only making one's voice heard but also including everyone in the discussion),
- writing/presenting resolutions/directions, especially those that pass,
- in crisis committees, as well as the detail and sophistication of crisis arcs.

Letter From Chair/Director:

Dear Delegates,

As the co-chair for the Collapse of the Internet Order: The SolarWinds Attack of 2020, I welcome you to UNISMUNC XII! My name is Aanya, and I have been at UNIS for four years. I am currently a sophomore, and this is my second year in MUN. Last year, in UNISMUNC XI, I participated in a crisis committee as the dias. During the year in MUN, I participated as the Assistant Secretary General of Financial Operations. Apart from UNISMUNC XI, I've been to other high school conferences, slowly gaining more experience. One thing I've learned is to come with an adequate amount of knowledge and preparation; therefore, I recommend writing a position paper and doing external research, which you can share with our other co-chair and me before the conference.

Aside from Model UN, I am from India, and I run my own club at UNIS. I enjoy topics around technology, economics, law, and finance; hence, I am excited to see which topics will follow during this committee! Furthermore, I am on UNIS' Varsity Squash team and enjoy playing squash outside of school. I've also written an article about AI and technology for the annual UNIS-UN conference, sparking my interest in dilemmas in the technological world and, ultimately, the topics of this committee. Some of my other interests include cooking, watching movies, and reading! I've lived in NYC my whole life, so I love going for walks around the city and exploring what I haven't seen before. Even outside of NYC, I've traveled and enjoy exploring many countries.

I can't wait to see your position papers, ideas, progress, and resolutions during this committee! As always, feel free to email me with any questions or concerns. I look forward to meeting you!

See you soon,

Aanya Sapra

29asapra@unis.org

Greetings Delegates,

As your co-chair, Aria Yen, I'm so glad to be a part of your UNISMUNC XII experience and see you in the Collapse of the Internet Order: The SolarWinds Attack of 2020 committee. I'm currently a sophomore in high school and have been going to UNIS since kindergarten. This is my second year in MUN at UNIS, and I've been working as the Assistant Secretary General of Public Relations. Apart from Model UN, I am on the varsity volleyball team at UNIS and have been playing volleyball for six years now. I have lived in New York City my whole life, and I couldn't imagine living anywhere else. I love the city and being able to constantly go to new places around New York.

Our co-chair and I have been working hard on this committee for a while now, and we are so excited to finally meet you guys. I strongly recommend writing a position paper, as in my experience, they have always helped me understand the committee's topic more thoroughly and prepare ideas to bring to the conference. If you decide to do so, please send the paper to me and our other co-chair before the day of the conference.

If you have any questions about the conference, please feel free to reach out to me anytime! I can't wait to meet you guys and hear some creative ideas and resolutions!

Can't wait to see you,

Aria Yen

29ayen@unis.org

A Brief Overview of the Committee:

Cyberattacks have become increasingly prominent in the 21st century. The 2019 Capital One breach. Equifax cyberattack of 2017. The SolarWinds software attack in 2020. Hackers, under the alliances of countries, or even private groups, craft meticulous code, perform a data breach, and ultimately access priceless information and resources. In the case of the SolarWinds cyberattack, the U.S. government, software companies, and high-value data were compromised from 2020 to 2021. This committee convenes in the midst of the first announcement of the SolarWinds breach. How can the U.S. government, global alliances, and growing corporations prevent further spread of calamity before it is too late?

Committee Procedure:

Moderated Caucuses are structured discussions where delegates sign themselves up to give short, regulated speeches. The speaking time and topic of discussion are set when the motion is proposed, and delegates take turns to speak.

Unmoderated Caucuses are divided between a regular unmoderated caucus and a gentleman's unmoderated caucus where everybody remains seated. A regular unmod entails a period free of structured, regulated debate, where delegates can mill about the committee and work with their blocs.

Some actions that are carried over from the usual committee procedure:

- Point of Order
- Point of Information
- Appeal to the Chair
- Suspension of Debate
- Adjournment of Debate
- Closure of Debate
- Roll Call Vote
- Set the Speaker's Time

Written Papers:

Resolutions: A piece of writing that outlines possible solutions to a problem and allows the committee to take action. Hopefully, towards the end of the committee, blocs will work together to write a resolution that can be debated and possibly passed.

Working Papers: The drafts of resolutions, i.e., resolutions before they are voted on by the committee – committee blocs work together to write these, brainstorming and fully outlining detailed solutions to the issues at hand. Then, they are voted on and formally become resolutions.

Topic Background:

SolarWinds, a software company based in America, was founded in 1999 by brothers Donald and David Yonce. SolarWinds provides essential IT management and numerous observability software products for large tech companies and government agencies. One of SolarWinds' most infamous software products is the Orion IT-monitoring software, which was distributed to nearly 18,000 customers, accentuating the gravity of the supply-chain attack. FireEye was the first to publicly disclose the attack in December 2020, and companies like Microsoft and the U.S. government were able to attribute the attack to the Russian Foreign Intelligence Service's orchestration of the attack, which was associated with the hacker group with the name of APT29/Cozy Bear/NOBELIUM. The attackers first made an entrance into SolarWind's environment in 2019 to conduct initial tests. The malicious code was first exposed to the update in February 2020. The Orion update was a legitimate SolarWinds update. However, due to the previous breach in 2019, the hackers were able to input the malicious code, dubbed "SUNBURST", so that the update remained verified and passed through the SolarWinds system. This update, later downloaded by U.S. government sectors and high-profile tech companies, allowed hackers to enter select victims' networks. This enabled access to administrative credentials, high-value targets, and the opportunity to impersonate high-profile individuals for enhanced resource access. Since the attack, strengthening cybersecurity, especially in supply chain security, has been strongly emphasized by governments. The incident shows how small weaknesses in cybersecurity can affect thousands of organizations globally; however, if the events of precaution didn't take place as soon as they did during the first breach, the outcome of the hack could have been radically different. Because of this recognition, organizations are increasingly using stricter

cybersecurity standards. For example, in response to cyberattacks in general, many organizations have implemented Zero Trust architecture (where every user is verified before gaining access to the desired resources) and monitor third-party software providers. How can the same companies, reconstructed in the replica first breach, use new technology, software, and advanced protection tactics to protect the government faster than they did in 2019/2020? Or does enhanced knowledge also mean more astute hackers?

Current Situation:

In September, 2019, the attackers gained unauthorized access to the SolarWinds software and building environment. These anonymous nation-state actors ran a customized benign piece of code as a test-run injection through SolarWinds' Orion software. During this dry-run period, the hackers omitted the malicious payloads while attentively monitoring the compilation processes to ensure the code didn't trigger errors or alerts. This test run period ran until November 2019. From November 2019 to December, the hackers compromised SolarWinds'

Microsoft Office 365 spaces. This unlocked great access to administrative communications and further details into SolarWinds' structure.

In early 2020, the hackers deployed "SUNSPOT." This was malware designed to run undetected through SolarWinds' servers in hopes of investigating the commands that ran SolarWinds' Orion. The most profound breach, in February 2020, allowed the "SUNSPOT" malware to latch onto and compile a new Orion update, instantaneously swapping the code with a trojanized version. This stronger version with a backdoor was named "SUNBURST". The "SUNBURST" update was unknowingly spread to customer portals in late March 2020, allowing the SUNBURST code to slip into the software of many SolarWinds users. A few months later, the attackers' active exploitation occurred. The hackers selectively analyzed 18,000 customers with the compromised malware and selected around 100 valuable high-profile targets, including significant U.S. government sectors, to infiltrate and perform espionage.

The first definitive action was initiated in late November 2020, when FireEye identified an anomaly regarding its previously installed 2FA. This led to the investigation of unrecognized requests and ultimately uncovered the attack on their software. This prompted a rigorous forensic investigation throughout FireEye's Operations Center, which exposed the hacker's infiltration of their corporate system and their "Red Team" testing tools. This broke the silence of the hacker's incursion, spreading the first wave of awareness and exposing the anonymous hackers' breach.

By December 2020, the route the hackers took, how widespread it is, and the other firms, companies, and governments impacted remain unknown. And most importantly, the road to solving the hackers' breach is yet to be uncovered. This hack has the potential to grow larger than some of the biggest cyberattacks. So how can companies work together to prevent future supply chain attacks? This situation requires collaboration, or even the separation of bonds

between companies and cybersecurity services, to minimize the effects of the attack and ultimately provide new measures that will prevent any similar breaches in the future. Will international leaders successfully be able to strengthen cybersecurity? Or will the internet never fully regain consumers' trust again?

Characters:

*These characters' roles correspond to their role in 2020. *These roles may have changed in present-day**

PHOTO	PERSON / POSITION	BACKGROUND
	President & CEO of ICANN (Göran Marby)	Göran Marby is the former CEO and President of the Internet Corporation for Assigned Names and Numbers (ICANN), a non-profit corporation based in California. He held this position for 6 years, from May 2016 to December 2022.
	CEO of FireEye/Mandiant (Kevin Mandia)	Kevin Mandia is a cybersecurity expert who was the CEO of FireEye/Mandiant. His company first discovered the SolarWinds breach after noticing suspicious activity within the company's systems. Later during the hack, Mandia spoke about how FireEye is almost always a prominent target for large cyberattacks like the SolarWinds attack, but he also emphasized that smaller firms should also be protected.
	CEO of Intel (Bob Swan)	Bob Swan is the CEO of Intel, one of the largest semiconductor and technology companies in the world. He managed the cybersecurity efforts at Intel. Intel is one of the corporations that were heavily involved in the SolarWinds attack (due to their involvement with SolarWinds-adjacent networks).



**U.S. Secretary of
the Treasury
(Steven Mnuchin)**

Mnuchin was the U.S. Treasury Secretary and managed U.S. government finances and economic policy. The Treasury Department was one of the agencies affected by the SolarWinds attack, and Mnuchin was one of the first to declare and identify that the hackers were able to penetrate that sector.



**U.S. Attorney
General /
Department of
Justice (William
Barr)**

Barr is a former U.S. Attorney General, managing federal law enforcement and legal action for large cybercrimes. This was necessary during the SolarWinds cyberattack as some sectors of the U.S. government were greatly compromised by the SolarWinds attack. Barr greatly underlined the Russian involvement with the cyberattack, and took it upon himself to refer the president to bring higher awareness to the U.S.'s cybersecurity.



**Head of the
Australian Cyber
Security Centre
(ACSC) (Abigail
Bradshaw)**

Bradshaw is the former Head of the Australian Cyber Security Centre, which is Australia's national cybersecurity agency. She was responsible for maintaining Australian government networks during the time of the SolarWinds attacks. Also, for any potential future attacks, Bradshaw ensured that the Australian IT system was further enhanced, strengthened, and kept in better cyber hygiene.



CEO of the UK's National Cyber Security Centre (NCSC) (Lindy Cameron)

Lindy Cameron was the UK's National Cyber Security Centre, working in that sector for 3 years and 4 months, and in the British Government for 28 years. As an expert in cybersecurity, she gave guidance on cybersecurity and the UK's response to the SolarWinds attack during the span of the attack. Ms. Cameron also helped contribute to the U.K.'s management enhancements to prevent and strengthen their technology for any potential similar situations.



The European Commissioner for Budget and Administration (Johannes Hahn)

Johannes Hahn, the European Commissioner, managed the European Union's budget and administration. He managed security matters affecting the European Union's institutions and evaluated risks from SolarWinds' attack. Hahn revealed that the EU's IT networks were compromised during the attack, and later helped the EU join the U.K., U.S., Canada, and NATO's attribution of the attack to Russia's espionage campaign.



The Director and chief of the Computer Emergency Response Team for all EU institutions, bodies, and agencies (Saâd Kadhi)

Kadhi led the Computer Emergency Response Team for EU institutions. He managed cybersecurity monitoring and incident response across the EU. During the SolarWinds attack, he led investigations to recognize threats as well as improving defenses against the SolarWinds breach.



**CEO of Amazon
Web Services
(Andy Jassy)**

Andy Jassy was one of the former CEOs of Amazon Web Services, the world's largest cloud computing provider. Later, in July 2021, he officially became the CEO of Amazon. Jassy was involved, using his connections and team to investigate its own private servers, confirming that the SolarWinds Orion software wasn't at large by the cyberattack, leading to a decline in the request to testify in the case. This led to criticism from the Senate Intelligence Committee. AWS was also involved in previous cyberattacks such as the Capital One cyberattacks of 2019.



**President of
Microsoft (Brad
Smith)**

Brad Smith became Microsoft's president and vice chairman in 2021. He is known to represent Microsoft's cybersecurity, privacy, and technology policy issues. He played a major role in the investigation of the attack and voiced his knowledge surrounding the threat by being one of the first to testify and explain the background, code, and external involvement of the attack. He then advocated for stronger cybersecurity cooperation around the world.



**U.S. Secretary of
Energy (Dan
Brouillette)**

During the SolarWinds attack, Dan Brouillette led the Department of Energy. He oversaw the energy infrastructure and nuclear security programs in the United States. Simultaneously, officials assessed whether the SolarWinds breach affected U.S. energy infrastructure systems.



**CEO of Cloudflare
(Matthew Prince)**

Matthew Prince is the co-founder and CEO of Cloudflare, a tech company that provides internet security, networking, and DDoS protection services. Prince is a billionaire and is the wealthiest person in Utah. Prince often speaks publicly about protective cybersecurity practices, especially after the SolarWinds breach, acting in a key leadership role to educate and inform others about the importance of cybersecurity.



**CEO of
CrowdStrike
(George Kurtz)**

George Kurtz is the co-founder and CEO of CrowdStrike, a major cybersecurity firm specializing in threat intelligence and endpoint protection. During and after the SolarWinds attack in 2021, CrowdStrike helped study the attackers' strategies and shared their findings with the public, specifically the "SUNSPOT" malware the hackers utilized. Kurtz spoke about the attack and provided solutions to cyber protection alongside other major companies, explaining the key details and steps behind the attack.



**Commander of U.S.
Cyber Command
(General Paul M.
Nakasone)**

General Paul M. Nakasone was the Commander of U.S. Cyber Command and director of the NSA, meaning he was a key leader of the U.S. military cyber operations and defended national security networks during the cyberattacks. During the SolarWinds attack, he coordinated work to investigate the breach, strengthen cybersecurity, and prevent nation-state cyber threats in the future. Nakasone identified major blind spots in U.S. intelligence and pushed for greater collaboration to prevent the effects of the attack in the future.



The Director of the Russian SVR (Foreign Intelligence Service) (Sergey Naryshkin)

Naryshkin was Head of Russia's Foreign Intelligence Service (SVR). This agency is widely linked to the SolarWinds cyberattack. Both the US and UK have blamed him for the cyberattack in 2020, although Naryshkin has denied the allegations by saying that the creative achievements of the attack were unattainable by the SVR; therefore, they couldn't take the credit.



CEO of SolarWinds (Sudhakar Ramakrishna)

Ramakrishna became the CEO of SolarWinds in January 2021, shortly after the SolarWinds attack was revealed. He strongly influenced the company's recovery by implementing security reforms in order to rebuild trust with customers. Ramakrishna had previous plans when he joined SolarWinds in the midst of the attack, playing a key role by handling the situation with pragmatic and mindful approaches.



Secretary-General of the International Telecommunication Union (Houlin Zhao)

Houlin Zhao was the Head of the International Telecommunication Union, which is the United Nations agency responsible for information and communication technologies. Zhao advocated for different countries to work together to prevent cyber threats. He contributed to international efforts to improve cybersecurity and spread awareness of cyber threats around the world.



**The Director of
CISA (U.S.
Cybersecurity and
Infrastructure
Security
Agency)(Brandon
Wales)**

Brandon Wales was the Acting Director of CISA and led the agency's response to the SolarWinds attack. He also improved federal cybersecurity efforts by managing investigations and strengthening U.S. cybersecurity defenses against future threats. Wales was one of th



**Department of
Homeland Security
(Chad Wolf)**

Chad Wolf is an American former government official who became the acting United States Secretary of Homeland Security in November 2019. The Department of Homeland Security was involved during the 2020 attacks due to the SolarWinds software update, compromising federal information, data, and privacy.



**CEO of Cisco
(Chuck Robbins)**

Chuck. Robbins is the CEO and chairman of Cisco, an information technology company. He joined Cisco in 1997 and has worked his way up to the CEO by working in various positions for the company. He became CEO in 2015 after being personally selected by John Chambers, the former CEO. Cisco was one of the many companies that had reliance on SolarWinds. Though its own properties remained unharmed due to the attack, the CEO and the company of Cisco itself had to make sure the attack didn't spread despite their best efforts.



**President of
Ukraine
(Volodymyr
Zelenskyy)**

Volodymyr Zelenskyy is the President of Ukraine and offered a crucial perspective on the Russian Foreign Intelligence Service, the perpetrators who were allegedly behind the attack. Ukraine's administration had faced digital warfare from the alleged Russian hackers, CozyBear, who have continuously targeted government infrastructure and military systems during vulnerable periods. Zelenskyy's prior relations with the attackers can provide critical insight to the SolarWinds attacks.



**Deputy National
Security Advisor of
the United States
(Anne Neuberger)**

Anne Neuberger served as the Deputy National Security Advisor of the U.S. for the Biden Administration. During the time this committee is set in, Neuberger was appointed to take the lead in the government response to the SolarWinds attack. Neuberger worked to centralize the response, outline expectations, and identify additional vulnerabilities related to the cyberattacks. Her presence was crucial in coordinating the U.S. government response to the attacks.



**Director of the
Federal Bureau of
Investigation of the
United States
(Christopher
Wray)**

Christopher Wray was the former Director of the Federal Bureau of Investigation who led the FBI's national response to the SolarWinds attack. The FBI worked to identify who conducted the breach and contacted likely targeted organizations and government agencies to prevent further damage. Additionally, the FBI worked with federal agencies including the CISA (Cybersecurity and Infrastructure Security Agency) and the NSA (National Security Agency) in order to triage data.



**Ambassador of the
Russian Federation
to the United States
of America
(Anatoly Antonov)**

Anatoly Antonov was the Russian Ambassador. Hired by the Russian government, he denied U.S. allegations of Russian involvement in the SolarWinds attack. He and was temporarily sent to Moscow (the capital of Russia).

Questions to Consider:

- What actions are necessary to resolve the havoc imposed by SolarWinds?
- What programs, platforms, or organizations could emerge from the journey to solve the SolarWinds attack?
- How can the method to resolve the SolarWinds breach be improved compared to the actions already taken in the past?
- Which companies are going to be the most affected by the hack, and what can other companies do to maintain the structure of the internet and software systems?
- Which corporation/country has the potential to collect strategic advantages from the SolarWinds hack, and how can international communities respond to the misuse of those advantages?
- What roles can companies, firms, and individuals take to minimize the effects of the cyberattack and prevent it from building?
- How can organizations strengthen cybersecurity without limiting technological innovation?

References:

Cassidy, Francesca. "Insights from the CEO Who Walked in on a Cyber Calamity." *Raconteur*, 4 Nov. 2022, www.raconteur.net/leadership/ceo-solarwinds-cyber-calamity. Accessed 27 July 2026.

UK and US call out Russia for SolarWinds compromise. 15 Apr. 2021. *National Cyber Security Centre*, www.ncsc.gov.uk/news/uk-and-us-call-out-russia-for-solarwinds-compromise. Accessed 27 July 2026.

"SolarWinds hack: Russian denial 'unconvincing.'" *BBC*, 18 May 2021, www.bbc.com/news/technology-57156197?scrlybrkr=4d82be7b. Accessed 28 July 2026.

NSA-CISA-FBI Joint Advisory on Russian SVR Targeting U.S. and Allied Networks. 28 Sept. 2021. *Cybersecurity and Infrastructure Security Agency*, www.cisa.gov/news-events/alerts/2021/04/15/nsa-cisa-fbi-joint-advisory-russian-svr-targeting-us-and-allied-networks. Accessed 22 July 2026.

"Lindy Cameron at Cyber 2021, Chatham House." *National Cyber Security Centre*, 11 Oct. 2021, www.ncsc.gov.uk/speech/lindy-cameron-first-year. Accessed 26 July 2026.

Mason, Max. "Aussie cyber chief warns business to improve its hygiene." *The Australian Financial Review*, 16 Mar. 2021, www.afr.com/technology/aussie-cyber-chief-warns-business-to-improve-its-hygiene-20210314-p57amr. Accessed 27 July 2026.

Wilkie, Christina. "Politics Attorney General Barr breaks with Trump, says SolarWinds hack 'certainly appears to be the Russians.'" *CNBC*, 21 Dec.

2020, www.cnn.com/2020/12/21/

[barr-says-solarwinds-hack-certainly-appears-to-be-the-russians-.html](#).

Accessed 28 July 2026.

Collier, Kevin. "Treasury also hacked in suspected Russian campaign, Mnuchin says." *NBC News*, 21 Dec. 2020. *NBC News*, www.nbcnews.com/tech/security/treasury-also-hacked-suspected-russian-campaign-mnuchin-says-n1251938.

Accessed 28 July 2026.

Temple-Raston, Dina. "A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack." *NPR*, New York Public Radio, 16 Apr. 2021, www.npr.org/2021/04/16/985439655/

[a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack](#).

Accessed 28 July 2026.

Oladimeji, Saheed, and Sean Michael Kerner. "SolarWinds hack explained: Everything you need to know." *TechTarget*, 3 Nov. 2023, www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know?sa=D.

Accessed 28 July 2026.

SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic). 22 Apr. 2021. U.S. Government Accountability Office, www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-in-fographic. Accessed 28 July 2026.