

## REFERENCES

- Sanger, D. E. (2018). *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. New York, Crown Publisher
- CISA, (2020) "Mitigate SolarWinds Orion Code Compromise," Emergency Directive 21 -01
- United Nations, (2023) *Our Common Agenda Policy Brief 9: A New Agenda for Peace*. Press Release
- Cavelty, M. D., & Wenger, A. (2020) *Cyber security meets security politics: Complex technology, fragmented politics, and networked science*, Contemporary Security Policy
- Dan Geer, (2010) 'Cybersecurity and National Policy', Harvard National Security Journal
- Brenner, Joel. (2011) *America The Vulnerable: Inside The New Threat Matrix Of Digital Espionage, Crime, And Warfare*. New York: Penguin Press
- Clarke, Richard A., Knake, Robert K. (2010) *Cyber War: The Next Threat to National Security and What to Do about It*. Harper Collins
- Clarke, Richard A., Knake, Robert K. (2020) *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*
- Herzog, Stephen (2011). "Revisiting the Estonian Cyber Attacks: Digital threats and Multinational Responses". Journal of Strategic Security
- Cyberdefense Report (2020) *2020 Estonia's National Cybersecurity and Cyberdefense Posture* Center for Security Studies (CSS), ETH Zürich
- Camile Marie Jackson (2013) "Estonian Cyber Policy After the 2007 Attacks: Drivers of Change and Factors for Success," New Voices in Public Policy, Vol. 7

Anna-Maria Osula (2015), “*National Cyber Security Organisations: Estonia*” (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 24 March 2015).

Cavelty, M. D., & Wenger, A. (2022) *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation*. Routledge New York

Maness, R. C., & Valeriano, B. (2016). *The Impact of Cyber Conflict on International Interactions*. Armed Forces & Society

Darmono, Bambang (2010) *Konsep Dan Sistem Keamanan Nasional Indonesi*

Berkowitz, Morton and Bock, P. G., (1965). *American National Security: A Reader in Theory and Policy*. New York

Bock, P., & Berkowitz, M. (1966). *The Emerging Field of National Security*. World Politics, New York

Triwahyuni, Dewi (2016) *Strategi Keamanan Siber Amerika Serikat*

Veale, M. & Brown, I. (2020). *Cybersecurity*. Internet Policy Review

Arikunto, Suharsimi. (1998). *Prosedur Penelitian Suatu Pendekatan Praktek*. Cetakan ke-11. Jakarta: PT Rineka Cipta.

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative and Mixed Methods Approaches (4th ed.)*. Thousand Oaks, CA: Sage

Sugiyono. (2018). *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*. Bandung: Alfabeta

Merriam, Sharan B. (2009). *Qualitative Research : A Guide to Design and Implementation*. San Francisco : John Wiley & Sons, Inc.

Yin, R. (2014). *Case Study Research Design and Methods (5th ed.)*. Thousand Oaks, CA Sage Publications, Inc.

Nazir, Mohammad. (2013). *Metode Penelitian*. Bogor

Arikunto, S. (2010). *Prosedur Penelitian Suatu Pendekatan Praktik*. Jakarta: Rineka Cipta.

Moleong, Lexy J. 2013. *Metode Penelitian Kualitatif. Edisi Revisi*. Bandung : PT. Remaja Rosdakarya.

Cronin, P., Ryan, F., & Coughlan, M. (2008). *Undertaking a literature review: a step-by-step approach*. British Journal of Nursing

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook (2nd ed.)*. Sage Publications, Inc.

Cohen, Z., Marquardt, A., Fung, B. (December 16, 2020). "Massive hack of US government launches search for answers as Russia named top suspect". CNN.

Nakashima, E., Timberg, C. (2020). "DHS, State and NIH join list of federal agencies — now five — hacked in major Russian cyberespionage campaign". The Washington Post.

Bing, C., Jack S., Raphael S., J. (2021). "Exclusive: Suspected Chinese hackers used SolarWinds bug to spy on U.S. payroll agency – sources". Reuters. <https://www.reuters.com/article/us-cyber-solarwinds-china-exclusive-idUSKBN2A22K8/>. Retrieved 11 December 2023.

Sanger, D. E., Perloth, N., Schmitt, E., (2020). "Scope of Russian Hack Becomes Clear: Multiple U.S. Agencies Were Hit". The New York Times.

Stubbs, J., Satter, R., Menn, J., (2020). "U.S. Homeland Security, thousands of businesses scramble after suspected Russian hack". Reuters.

Turton, W., Riley, M., Jacobs, J. (2020). "Hackers Tied to Russia Hit Nuclear Agency; Microsoft Is Exposed". Bloomberg L.P.

Stubbs, J., Satter, R., Menn, J. (2020). "U.S. Homeland Security, thousands of businesses scramble after suspected Russian hack". Reuters.

Suderman, A. (2021). "AP sources: SolarWinds hack got emails of top DHS officials". Associated Press. <https://apnews.com/article/solarwinds-hack-email-top-dhs-officials-8bcd4a4eb3be1f8f98244766bae70395>. Retrieved 11 December 2023.

Morath, E., Cambon, S. C. (2021). "SolarWinds Hack Leaves Market-Sensitive Labor Data Intact, Scalia Says". The Wall Street Journal.

Newman, L. H. (2021). *"The SolarWinds Body Count Now Includes NASA and the FAA"*. Wired

Bing, C. (2020). *"EXCLUSIVE-U.S. Treasury breached by hackers backed by foreign government – sources"*. Reuters.  
<https://www.reuters.com/world/us/suspected-russian-hackers-spied-us-treasury-emails-sources-2020-12-13/>. Retrieved 01 December 2023

Volz, Kevin Poulsen, Robert McMillan and Dustin (2020). *"WSJ News Exclusive | SolarWinds Hack Victims: From Tech Companies to a Hospital and University"*. Wall Street Journal.

Hvistendahl, M., Lee, M., Smith, J., (2020). *"Russian Hackers Have Been Inside Austin City Network for Months"*. The Intercept.

King, Ian; Mehrotra, Kartikay (2020). *"Cisco Latest Victim of Russian Cyber-Attack Using SolarWinds"*. Bloomberg.

Stubbs, Jack; McNeill, Ryan (2020). *"SolarWinds hackers broke into U.S. cable firm and Arizona county, web records show"*. Reuters.

Menn, Joseph (2020). *"Exclusive: Microsoft breached in suspected Russian hack using SolarWinds – sources"*. Reuters.

Perlroth, N. (2020). *"Microsoft Says Russian Hackers Viewed Some of Its Source Code"*. The New York Times.

Robles, C. J. (2020). *"Microsoft, SolarWinds Hacking Can Be a National Security Issue?"*. Tech Times.

Cimpanu, Catalin (2021). *"Four security vendors disclose SolarWinds-related incidents"*. ZDNet.

Miller, M. (2020). *"Schiff calls for 'urgent' work to defend nation in the wake of massive cyberattack"*. The Hill.

Miller, M. (2020). *"Senators press federal agencies for more information on Russian cyberattack"*. The Hill.

Rosenberg, Adam (December 13, 2020). *"Russian government-backed hackers breached the U.S. Treasury, Commerce departments"*. Mashable. <https://mashable.com/article/us-treasury-hacked-office-365>. Retrieved 05 December 2023

Daugherty, A. (2020). "Intel chairman Rubio says 'America must retaliate' after massive cyber hack". Miami Herald.

Shinkman, P. D. (2021). Russia Warns Against U.S. Retaliation for SolarWinds Amid Fears of Cyberwar. US News & World Report; U.S. News & World Report. - <https://www.usnews.com/news/world-report/articles/2021-03-09/russia-warns-against-us-retaliation-for-solarwinds-amid-fears-of-cyberwar>. Retrieved 31 December 2023

Barnes, E. J., & Sanger, E., D. (2021) White House Announces Senior Official Is Leading Inquiry Into SolarWinds Hacking – The New York Times. Web.archive.org. <https://web.archive.org/web/20210311170652/https://www.nytimes.com/2021/02/10/us/politics/biden-russia-solarwinds-hacking.html>. Retrieved 31 December 2023

Statement by Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger on SolarWinds and Microsoft Exchange Incidents. (2021). The White House. <https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/19/statement-by-deputy-national-security-advisor-for-cyber-and-emerging-technology-on-solarwinds-and-microsoft-exchange-incidents/>. Retrieved 27 December 2023

Reuters. (2021). Biden budget sets aside \$750 mln for SolarWinds response. Reuters. <https://www.reuters.com/technology/biden-budget-sets-aside-750-mln-solarwinds-response-2021-05-28/>. Retrieved 26 December 2023

CISA Mitigate SolarWinds Orion Code Compromise, Emergency Directive 21-01 (2020) and Supplemental Direction version 4, (2021). <https://www.cisa.gov/news-events/directives/ed-21-01-mitigate-solarwinds-orion-code-compromise>. Retrieved 01 January 2024

Starks, T. (2021). Biden budget seeks \$750 million to respond to SolarWinds compromises, plus billions more for cyber. CyberScoop. <https://cyberscoop.com/biden-budget-750-million-solarwinds-fiscal-2022/>. Retrieved 20 December 2023.

<https://www.cisa.gov/news/2021/08/05/cisa-launches-new-joint-cyber-defense-collaborative>. Retrieved 26 December 2023.

Gunderman, D., (2022). US Congress Passes Cyber Incident Reporting Mandate. [https://www.databreachtoday.com/us-congress-passes-cyber-incident-reporting-mandate-a-18704?rf=2022-03-14-ENEWS-ACQ-DBT-Slot1-ART18704&mkt\\_tok=MDUxLVpYSS0yMzcAAAGDKBaxjiiLV\\_vg84lgpjicEk3U8DdBNsTz4mp](https://www.databreachtoday.com/us-congress-passes-cyber-incident-reporting-mandate-a-18704?rf=2022-03-14-ENEWS-ACQ-DBT-Slot1-ART18704&mkt_tok=MDUxLVpYSS0yMzcAAAGDKBaxjiiLV_vg84lgpjicEk3U8DdBNsTz4mp). Retrieved 02 January 2024.

LI, S. (2021). 17TH CONGRESS 1ST SESSION. [https://www.warner.senate.gov/public/\\_cache/files/4/2/422a0de2-3c56-4e56-a4be-0e83af5b0065/F90B3C493BA4FAB09E546FAF40E4B116.alb21b95.pdf](https://www.warner.senate.gov/public/_cache/files/4/2/422a0de2-3c56-4e56-a4be-0e83af5b0065/F90B3C493BA4FAB09E546FAF40E4B116.alb21b95.pdf). Retrieved 02 January 2024.

The White House. (2021). Executive order on improving the nation's cybersecurity. The White House. <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>. Retrieved 01 January 2024.

CISA (2023). [https://www.cisa.gov/sites/default/files/2023-04/CISA\\_Zero\\_Trust\\_Maturity\\_Model\\_Version\\_2\\_508c.pdf](https://www.cisa.gov/sites/default/files/2023-04/CISA_Zero_Trust_Maturity_Model_Version_2_508c.pdf). Retrieved 04 January 2024.

Strengthening American Cybersecurity Act of 2022 - <https://www.congress.gov/bill/117th-congress/senate-bill/3600#:~:text=The%20bill%20requires%20reporting%20and,and%20disclosure%20of%20reported%20information>. Retrieved 02 January 2024

White House, Office of the Press Secretary, Presidential Policy Directive — Critical Infrastructure Security and Resilience. (2023) <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

Lahut, S. S., Jake. (2020). Biden says he will “not stand idly by” on the massive US cyberattack that Trump hasn't bothered to address yet. Business Insider. Retrieved January 12, 2024, from

<https://www.businessinsider.com/biden-statement-solarwinds-cyberattack-trump-russia-2020-12>. Retrieved 02 January 2024

Baker, P. (2021). The SolarWinds hack timeline: Who knew what, and when? CSO Online. <https://www.csoonline.com/article/570537/the-solarwinds-hack-timeline-who-knew-what-and-when.html>. Retrieved 02 January 2024

The White House (2021). Memorandum on Revitalizing America's Foreign Policy and National Security Workforce, Institutions, and Partnerships. <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/04/memorandum-revitalizing-americas-foreign-policy-and-national-security-workforce-institutions-and-partnerships/>. Retrieved 02 January 2024

U.S. Department of the Treasury. (2023). NSM-3 Finance and Economic Interagency Policy Committee (IPC). <https://home.treasury.gov/about/careers-at-treasury/nsm-3-finance-and-economic-interagency-policy-committee-ipc>. Retrieved 02 January 2024

Matishak, M. (2022) Biden signs cyber incident reporting bill into law. (n.d.). Therecord.media. <https://therecord.media/biden-signs-cyber-incident-reporting-bill-into-law>. Retrieved 02 January 2024

Baksh, M. (2022) Cyber-Incident Reporting Legislation Clears House in Bipartisan Spending Bill. <https://www.nextgov.com/cybersecurity/2022/03/cyber-incident-reporting-legislation-clears-house-bipartisan-spending-bill/363022/>. Retrieved 02 January 2024

Following SolarWinds & Colonial Hacks, Senators Collins, Warner, Rubio Introduce Bipartisan Cyber Reporting Legislation (2022). <https://www.king.senate.gov/newsroom/press-releases/following-solarwinds-and-colonial-hacks-senators-collins-warner-rubio-introduce-bipartisan-cyber-reporting-legislation>. Retrieved 02 January 2024

Peters, Portman, Warner & Collins Introduce Amendment to Annual Defense Bill to Strengthen Public and Private Sector Cybersecurity. (2022). Committee on Homeland Security & Governmental Affairs.

<https://www.hsgac.senate.gov/media/dems/peters-portman-warner-and-collins-introduce-amendment-to-annual-defense-bill-to-strengthen-public-and-private-sector-cybersecurity/>. Retrieved 02 January 202

Starks, T. (2021). Incident reporting, ransomware payment legislation faces trouble in Senate. CyberScoop. <https://cyberscoop.com/incident-reporting-ransomware-payment-legislation-senate-scott-amendment/>. Retrieved 02 January 2024

Stubbs, J., McNeill, R. (2020). SolarWinds hackers broke into U.S. cable firm and Arizona county, web records show. <https://web.archive.org/web/20201222111858/https://uk.reuters.com/article/us-usa-cyber-idUKKBN28S2B9>. Retrieved 01 January 2024

Senate RPC. (2021). The SolarWinds Cyberattack. <https://www.rpc.senate.gov/policy-papers/the-solarwinds-cyberattack>. Retrieved 02 January 2024

Scroxtton, A. (2021). Biden picks cyber veteran to reinvigorate security response. Computer Weekly. [https://www.computerweekly.com/news/252494470/Biden-picks-cyber-veteran-to-reinvigorate-security-response?\\_ga=2.222700318.468031876.1702366418-1706617175.1702366418&\\_gl=1\\*1m5v3bx\\*\\_ga\\*MTcwNjYxNzE3NS4xNzAyMzY2NDE4\\*\\_ga\\_TQKE4GS5P9\\*MTcwMjM3NjE3OS4yLjEuMTcwMjM3NjIxMS4wLjAuMA](https://www.computerweekly.com/news/252494470/Biden-picks-cyber-veteran-to-reinvigorate-security-response?_ga=2.222700318.468031876.1702366418-1706617175.1702366418&_gl=1*1m5v3bx*_ga*MTcwNjYxNzE3NS4xNzAyMzY2NDE4*_ga_TQKE4GS5P9*MTcwMjM3NjE3OS4yLjEuMTcwMjM3NjIxMS4wLjAuMA). Retrieved 02 January 2024

Lin, H. (2020). Reflections on the SolarWinds Breach. Lawfare . <https://www.lawfaremedia.org/article/reflections-solarwinds-breach>. Retrieved 02 January 2024

Jensen, B., Valeriano, B., & Montgomery, M. (2020). The Strategic Implications of SolarWinds. Lawfare. <https://www.lawfaremedia.org/article/strategic-implications-solarwinds>. Retrieved 02 January 2024

The White House. (2023). NATIONAL CYBERSECURITY STRATEGY.



<https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>. Retrieved 01 December 2023.

Vasquez, C. (2023). White House releases National Cybersecurity Strategy implementation plan. CyberScoop. <https://cyberscoop.com/national-cybersecurity-strategy-implementation-plan-2/>. Retrieved 14 January 2024

Jindal, D., Soliman, M. (2023). The 2023 National Cybersecurity Strategy: How Does America Think About Cyberspace? [Review of The 2023 National Cybersecurity Strategy: How Does America Think About Cyberspace?]. Middle East Institute. <https://www.mei.edu/publications/2023-national-cybersecurity-strategy-how-does-america-think-about-cyberspace>. Retrieved 14 January 2024

Joshi, A., & Dobrykowski, D. (2023, March 9). The US has announced its National Cybersecurity Strategy: Here's what you need to know. World Economic Forum. <https://www.weforum.org/agenda/2023/03/us-national-cybersecurity-strategy/>. Retrieved 14 January 2024

Lostri, E., & Pell, S. (2023). The Biden Administration's Implementation Plan for the National Cybersecurity Strategy. Lawfare. <https://www.lawfaremedia.org/article/the-biden-administration-s-implementation-plan-for-the-national-cybersecurity-strategy>. Retrieved 14 January 2024

Sara, W, (2020) *"SolarWinds Recap: All of the Federal Agencies Caught Up in the Orion Breach,"* FedScoop.

Kovacs, E. (2020). "FBI, CISA, ODNI Describe Response to SolarWinds Attack". Security Week. <https://www.securityweek.com/fbi-cisa-odni-describe-response-solarwinds-attack/>. Retrieved 10 December 2023.

Sanders, C. (2021). "Biden budget sets aside \$750 mln for SolarWinds response". Reuters. <https://www.reuters.com/technology/biden-budget-sets-aside-750-mln-solarwinds-response-2021-05-28/>. Retrieved 01 January 2024.