DAFTAR PUSTAKA

Allison, G. T. . (1971). Essence of decision: explaining the Cuban missile crisis. Little, Brown and Company. https://archive.org/details/essenceofdecisio0000unse/page/n5/mode/2up

Arghire, I. A. (2021). More countries officially blame Russia for Solarwinds attack. SecurityWeek. https://www.securityweek.com/more-countries-officially-blame-russia-solar winds-attack/

Australian Cyber Security Centre (2020). Potential SolarWinds Orion compromise. Australian Signals Directorate. https://www.cyber.gov.au/about-us/alerts/potential-solarwinds-orion-comp romise

Australian Department of Defence & Department of Home Affairs. (2021). Attribution of cyber incident to Russia (2021). https://www.foreignminister.gov.au/minister/marise-payne/media-release/attr ibution-cyber-incident-russia

Bail, C. A., Guay, B., Maloney, E., Combs, A., Hillygus, D. S., Merhout, F., Freelon, D., & Volfovsky, A. (2019). Assessing the Russian Internet Research Agency's impact on the political attitudes and behaviors of American Twitter users in late 2017. Proceedings of the National Academy of Sciences, 117(1), 243–251. https://doi.org/10.1073/pnas.1906420116

Bala, I., Ebere Shalom, A., Egahi Junior, O., & Filibus, Y. (2024). Cyberwarfare and Arms Control: Analyzing the SolarWinds Hack of 2020. International Journal of Emerging Multidisciplinaries: Social Science, 3(1). https://doi.org/10.54938/ijemdss.2024.03.1.347

Bing, C. (2020). Suspected Russian hackers spied on U.S. Treasury emails - sources. Reuters. https://www.reuters.com/article/us-usa-cyber-treasury-exclsuive-idUSKBN2 8N0PG/

Bushwick, S. (2023). FBI takes down Hive criminal ransomware group. Scientific American. https://www.scientificamerican.com/article/fbi-takes-down-hive-criminal-ra nsomware-group1/

Buchanan, B. (2020). The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics. Harvard University Press. https://doi.org/10.2307/j.ctv3405w2m

Chandra, R. D., Azzqy, A. A. R., & Awal, S. (2023). Strategi Keamanan Siber Amerika Serikat di Masa Pemerintahan Joe Biden Terkait Isu State-Sponsored Cyber Espionage . Balcony, 7(1), 13–26. Retrieved from https://jom.fisip.budiluhur.ac.id/balcony/article/view/400

Chen, S., & Taw, J. (2023). Conventional Retaliation and Cyber Attacks. The Cyber Defense Review, 8(1), 67–86. https://www.jstor.org/stable/48730573

Chin-Rothmann, C. (2021). After the SolarWinds hack, the Biden administration must address Russian cybersecurity threats. Brookings Institution. https://www.brookings.edu/articles/after-the-solarwinds-hack-the-biden-administration-must-address-russian-cybersecurity-threats/

Corera, G. (2023). Lockbit: UK leads disruption of major cyber-criminal gang. BBC. https://www.bbc.com/news/technology-68344987

Creswell, J. W. (2009). Research design: Qualitative, quantitative, and mixed methods approaches. Sage. ISBN 978-1-4129-6557-6

CrowdStrike. (2021). SUNSPOT malware technical analysis. https://www.crowdstrike.com/en-us/blog/sunspot-malware-technical-analysis/

Cybersecurity and Infrastructure Security Agency. (2020). Emergency Directive 21-01 Older Supplemental Guidance https://www.cisa.gov/emergency-directive-21-01-older-supplemental-guidance

Cybersecurity and Infrastructure Security Agency. (2021). Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations (Alert Code AA20-352A). U.S. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a

Cybersecurity and Infrastructure Security Agency. (2023). Cyber Safety Review Board Charter. U.S. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/resources-tools/resources/cyber-safety-review-board-charter

Cybersecurity and Infrastructure Security Agency. (2025). CISA Fact Sheet. U.S. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/resources-tools/resources/cisa-fact-sheet

Cybersecurity and Infrastructure Security Agency. (2026). ED 21-01: Mitigate SolarWinds Orion code compromise (Closed). ED 21-01. https://www.cisa.gov/news-events/directives/ed-21-01-mitigate-solarwinds-orion-code-compromise-closed

Daoud, M. (2025) Global currency, local compliance: How US dollar and allied currency regulations reshape emerging markets. International Banker. https://internationalbanker.com/banking/global-currency-local-compliance-how-us-dollar-and-allied-currency-regulations-reshape-emerging-markets/

Daniel, B. (2024). The solarwinds orion hack explained. Trusted Computing Innovator. https://www.trentonsystems.com/en-us/resource-hub/blog/solarwinds-hack-overview-prevention

Egloff, F. J. (2020). Public attribution of cyber intrusions. Journal of Cybersecurity, 6(1). https://doi.org/10.1093/cybsec/tyaa012

Erickson, J. V. (2021). Clausewitz's perspective on deterring Russian malign activities in cyberspace. Military Review. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/SO-21/Erickson-Clausewitzs-Perspective/Erickson.pdf

Fenton, N., & Kolyandr, A. (2025). Down, not out: The Russian economy under western sanctions. Center for Strategic and International Studies. https://www.csis.org/analysis/down-not-out-russian-economy-under-western-sanctions

Fiantika, F. R., Wasil, M., Jumiyati, S., Honesti, L., Wahyuni, S., Mouw, E., Mashudi, I., Hasanah, N., Maharani, A., & Ambarwati, K. (2022). Metodologi penelitian kualitatif. PT. Global Eksekutif Teknologi. https://www.researchgate.net/profile/Anita-Maharani/publication/359652702_Metodologi_Penelitian_Kualitatif/links/6246f08b21077329f2e8330b/Metodologi-Penelitian-Kualitatif.pdf

Foreign, Commonwealth & Development Office, & National Cyber Security Centre. (2021). Russia: UK and US expose global campaign of malign activity by Russian intelligence services. GOV.UK. https://www.gov.uk/government/news/russia-uk-and-us-expose-global-campaigns-of-malign-activity-by-russian-intelligence-services

F-Secure. (2015). The Dukes: 7 years of Russian cyberespionage. https://blog-assets.f-secure.com/wp-content/uploads/2020/03/18122307/F-Secure_Dukes_Whitepaper.pdf

Gia Anisa, & Fitria Widianingsih. (2024). SolarWinds Attack: Stages, Implications, and Mitigation Strategies in the Cyber Age. Electronic Integrated Computer Algorithm Journal, 2(1), 47–52. https://doi.org/10.62123/enigma.v2i1.31

Ghanbari, H., Koskinen, K., & Wei, Y. (2024). From SolarWinds to Kaseya: The rise of supply chain attacks in a digital world. Journal of Information Technology Teaching Cases. https://doi.org/10.1177/20438869241299823

Global Affairs Canada. (2021). Statement on SolarWinds cyber compromise. Government of Canada. https://www.canada.ca/en/global-affairs/news/2021/04/statement-on-solarwinds-cyber-compromise.html

Gregory, J. (2024). How has Executive Order 14028 affected federal cybersecurity so far?. IBM https://www.ibm.com/think/news/executive-order-14028-federal-cybersecurity-update

Healey, J. (2023). Twenty-five years of White House cyber policies. Lawfare. https://www.lawfaremedia.org/article/twenty-five-years-of-white-house-cyber-policies

Hunnicutt, T., Mohammed, A., & Osborn, A. (2021). U.S. imposes wide array of sanctions on Russia for 'malign' actions. Reuters. https://www.reuters.com/world/middle-east/us-imposes-wide-array-sanctions-russia-malign-actions-2021-04-15/

IISS. (2021). Cyber Capabilities and National Power: A Net Assessment. IISS https://www.iiss.org/research-paper/2021/06/cyber-capabilities-national-power/

Johnston, M. (2024.). How solarwinds makes money. Investopedia. https://www.investopedia.com/how-solarwinds-makes-money-5092559

Jones, D. (2020). Full impact of Solarwinds attack begins to emerge across tech sector, federal agencies. Cybersecurity Dive. https://www.cybersecuritydive.com/news/solarwinds-impacts-updates/592700/

Jardine, E., Porter, N., & Shandler, R. (2024). Cyberattacks and public opinion – The effect of uncertainty in guiding preferences. Journal of Peace Research, 61(1), 103–118. https://doi.org/10.1177/00223433231218178

Kimball, J., (2021). Costs of the 20-year war on terror: $8 trillion and 900,000 deaths. Brown University. https://www.brown.edu/news/2021-09-01/costsofwar

Kruti, A., Butt, U., & Bin Sulaiman, R. (2023). A review of SolarWinds attack on Orion platform using persistent threat agents and techniques for gaining unauthorized access. arXiv. https://doi.org/10.48550/arXiv.2308.10294

Lardner, T. P., Jr. (2000). Risk vulnerability assessments PDD-63 risk management overview. https://www.giac.org/paper/gsec/260/risk-vulnerability-assessments-pdd-63-risk-management-overview/100845

Laudon, K. C. ., Laudon, J. Price., & Elragal, Ahmed. (2013). *Management information systems : managing the digital firm*. Pearson. https://library.uniq.edu.iq/storage/books/file/SAMPLE-MIS,BOOK/1666784845SAMPLE-MIS,BOOK.pdf

Li, P., & Lorci, E. (2025). Navigating the Foreign Policy in Cyber Landscape: A Novel Model for State Decision-Making in Cyberspace. Uluslararası İlişkiler Dergisi, 22(87), 185–202. https://doi.org/10.33458/uidergisi.1747943

Libicki, M. C. . (2009). Cyberdeterrence and cyberwar. RAND. ISBN 978-0-8330-4734-2. https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

Libicki, M. C.. (2020). Correlations Between Cyberspace Attacks and Kinetic Attacks. paper 2020 12th International Conference on Cyber Conflict. https://ccdcoe.org/uploads/2020/05/CyCon_2020_11_Libicki.pdf

Lorci, E. (2024). Assessing power and hierarchy in cyberspace: An approach of power transition theory. Applied Cybersecurity & Internet Governance, 3(2), 7–37. https://www.acigjournal.com/pdf-190481-124460?filename=Assessing%20Power%20and.pdf

Manning, R. A. (2020). Emerging Technologies: New Challenges to Global Stability. Atlantic Council. http://www.jstor.org/stable/resrep26000

Mandiant. (2020). Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor. https://cloud.google.com/blog/topics/threat-intelligence/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor

Mandiant. (2022). Assembling the Russian Nesting Doll: UNC2452 Merged into APT29. https://cloud.google.com/blog/topics/threat-intelligence/unc2452-merged-into-apt29

Marelli, M. (2022). The SolarWinds hack: Lessons for international humanitarian organizations. https://international-review.icrc.org/sites/default/files/reviews-pdf/2022-06/the-solarwinds-hack-lessons-for-international-humanitarian-organizations-919.pdf

Matishak, M. (2023). 22 ‘hunt forward’ missions deployed overseas in 2023, Cyber Command leader says. The Record. https://therecord.media/cyber-command-hunt-forward-missions-2023-haugh-senate

Matishak, M. (2022). Cyber incident reporting bill hitches a ride on $1.5 trillion spending deal. The Record. https://therecord.media/cyber-incident-reporting-bill-hitches-a-ride-on-1-5-trillion-spending-deal

Microsoft. (2020). Microsoft internal Solorigate investigation update. Microsoft. https://www.microsoft.com/en-us/msrc/blog/2020/12/microsoft-internal-solorigate-investigation-update

Nakashima, E. (2019). U.S. Cyber Command operation disrupted internet access of Russian 'troll factory' on day of 2018 midterms. The Washington Post. https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html

Nakashima, E. (2022). Cybercom disrupted Russian and Iranian hackers throughout the midterms. The Washington Post. https://www.washingtonpost.com/national-security/2022/12/22/cybercom-russia-iran-attacks/

Nakasone, P. M.. (2019). A cyber force for persistent operations. Brown University Department of Computer Science. https://cs.brown.edu/courses/cs180/sources/2019_01_22_JFQ_CyberRoleForPersistentOperations_Nakasone.pdf

National Institute of Standards and Technology. (2021). Securing small-business and home Internet of Things (IoT) devices: Mitigating network-based attacks using Manufacturer Usage Description (MUD) (NIST Special Publication 1800-15). https://doi.org/10.6028/NIST.SP.1800-15

National Institute of Standards and Technology. (2020). Zero Trust Architecture (NIST SP 800-207). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

National Security Agency, Cybersecurity and Infrastructure Security Agency, & Federal Bureau of Investigation. (2021). Russian SVR targets U.S. and allied networks. https://media.defense.gov/2021/Apr/15/2002621240/-1/-1/0/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF

National Security Agency. (n.d.). *Mission & values*. https://www.nsa.gov/about/mission-values/

National Security Agency. (2021). CSA SVR targets US allies. Russian SVR Targets U.S. and Allied Networks https://media.defense.gov/2021/Apr/15/2002621240/-1/-1/0/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF

Naurah, N. (2023). Deretan Negara Dengan Kasus Serangan Siber terbanyak di Dunia, Ada Indonesia?. GoodStats. https://goodstats.id/article/deretan-negara-dengan-kasus-serangan-siber-terbanyak-di-dunia-ada-indonesia-PdwM0

Newmeyer, K. P. (2012). Who Should Lead U.S. Cybersecurity Efforts? PRISM, 3(2), 115–126. http://www.jstor.org/stable/26469733

National Institute of Standards and Technology (NIST). (2020). Zero trust architecture (NIST Special Publication 800-207). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

North Atlantic Council (NATO). (2021). North Atlantic Council statement following the announcement by the United States of actions with regard to Russia. North Atlantic Treaty Organization. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2021/04/15/north-atlantic-council-statement-following-the-announcement-by-the-united-states-of-actions-with-regard-to-russia

Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. International Security, 41(3), 44–71. https://doi.org/10.1162/ISEC_a_00266

Osinga, F., & Sweijs, T. (2021). NL ARMS Netherlands annual review of military studies 2020: Deterrence in the 21st century—insights from theory and practice. ISBN 978-94-6265-418-1

Peisert, S., Schneier, B., Okhravi, H., Massacci, F., Benzel, T., Landwehr, C., Mannan, M., Mirkovic, J., Prakash, A., & Michael, J. B. (2021). Perspectives on the Solarwinds incident. IEEE Security & Privacy, 19(2), 7–13. https://doi.org/10.1109/msec.2021.3051235

Polyakova, A., & Boulègue, M. (2021). The evolution of Russian hybrid warfare. Center for European Policy Analysis. https://cepa.org/wp-content/uploads/2021/01/CEPA-Hybrid-Warfare-1.28.21.pdf

Pomerleau, M. (2023). US Cyber Command conducts 'hunt forward' mission in Latin America for first time, official says. DefenseScoop. https://defensescoop.com/2023/06/08/us-cyber-command-conducts-hunt-forward-mission-in-latin-america-for-first-time-official-says/

Pope, S. (2020). Microsoft internal Solorigate investigation update. Microsoft Security Response Center. https://www.microsoft.com/en-us/msrc/blog/2020/12/microsoft-internal-solorigate-investigation-update

Ramakrishna, S. (2021). New findings from our investigation of SUNBURST. https://www.solarwinds.com/blog/new-findings-from-our-investigation-of-sunburst

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/

Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. Journal of Strategic Studies, 38(1–2), 4–37. https://doi.org/10.1080/01402390.2014.977382

Rollins, J., & Henning, A. C. (2009). Comprehensive national cybersecurity initiative: Legal authorities and policy considerations (Report No. R40427). Congressional Research Service. https://www.everycrsreport.com/files/20090310_R40427_bc2bdcec7c5e009207f51bd775ed6757b61de42f.pdf

Roth, A. (2021). Russia expels 10 US diplomats as part of retaliation for sanctions. The Guardian. https://www.theguardian.com/world/2021/apr/16/russia-expels-10-us-diplomats-etaliation-sanctions

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/

Sanger, D. E. (2018). The perfect weapon: War, sabotage, and fear in the cyber age. Crown. ISBN 10: 0451497902

Sanger, D. E., & Perlroth, N. (2021). FireEye, a top cybersecurity firm, says it was hacked by a nation-state. The New York Times. https://www.nytimes.com/2020/12/08/technology/fireeye-hacked-russians.html

Sanger, D. E., Perlroth, N., & Barnes, J. E. (2021). As understanding of Russian hacking grows, so does alarm. The New York Times. https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html

Satter, R., & Menn, J. (2020). SolarWinds hackers accessed Microsoft source code, the company says. Reuters. https://www.reuters.com/article/world/solarwinds-hackers-accessed-microsoft-source-code-the-company-says-idUSKBN29620B/

Shahryarifar, S. (2016). Rational Actor Model in foreign policy analysis. International Journal of Law and Political Science, 5(1), 22–27. https://jhss-khazar.org/wp-content/uploads/2016/02/YEN-_2_Volume19number1.7.IR-pub-1-1.pdf

SolarWinds. (2024). SolarWinds becomes first software provider to align with new CISA secure software development guidance. https://www.solarwinds.com/company/newsroom/press-releases/solarwinds-becomes-first-software-provider-to-align-with-new-cisa-secure-software-development-guidance

Suderman, A. (2021). AP sources: SolarWinds hack got emails of top DHS officials. AP News. https://apnews.com/article/solarwinds-hack-email-top-dhs-officials-8bcd4a4eb3be1f8f98244766bae70395

Sun, M. (2014). Balance of power theory in today's international system. E-International Relations. https://www.e-ir.info/2014/02/12/balance-of-power-theory-in-todays-international-system/

Sybikowska, B. (2022). The New Cold War: Cyber Frontline. Polish Political Science Review, Sciendo, vol. 10 no. 2, pp. 14-31. https://doi.org/10.2478/ppsr-2022-0010

Temple-Raston, D. (2021). A 'worst nightmare' cyberattack: The untold story of the SolarWinds hack. NPR. https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack

The White House. (1998). The Clinton Administration's policy on critical infrastructure protection: Presidential decision directive 63 [White paper]. Center for Space Policy and Strategy. https://csps.aerospace.org/sites/default/files/2021-08/Critical%20Infrastructure%20Protection%20white%20paper%20May98.pdf

The White House. (2003). National strategy to secure cyberspace 2003. https://energy.gov/sites/prod/files/National%20Strategy%20to%20Secure%20Cyberspace.pdf

The White House. (2009). Cyberspace policy review - Assuring a Trusted and Resilient Information and Communications Infrastructure. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/UnitedStates_2009_Cyberspace_Policy_Review_final_0.pdf

The White House. (2011). International strategy for cyberspace: Prosperity, security, and openness in a networked world. https://nsarchive.gwu.edu/sites/default/files/documents/20685798/04.pdf

The White House. (2016). Presidential policy directive: United States cyber incident coordination. https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

The White House. (2018). National Cyber Strategy 2018. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

The White House. (2021). Fact sheet: Imposing costs for harmful foreign activities by the Russian government. https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/

The White House. (2021). INTERNATIONAL STRATEGY FOR CYBERSPACE https://nsarchive.gwu.edu/sites/default/files/documents/20685798/04.pdf

The White House. (2023). National cybersecurity strategy 2023. https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Tidy, J. (2021). REvil: Day of reckoning for notorious cyber gang. BBC News. https://www.bbc.com/news/technology-59215167

Trautman, L. J. (2015). Cybersecurity: What About U.S. Policy? http://dx.doi.org/10.2139/ssrn.2548561

Tucker, E., & Madhani, A. (2021). US expels Russian diplomats, imposes sanctions for hacking. AP News. https://apnews.com/article/us-expel-russia-diplomats-sanctions-6a8a54c7932ee8cbe51b0ce505121995

United Nations General Assembly (UN-GGE). (2021). Report of the Group of Governmental Experts on advancing responsible State behaviour in cyberspace in the context of international security (Document A/76/135). United Nations. https://dig.watch/wp-content/uploads/2022/08/UN-GGE-Report-2021.pdf

U.S. Congress. (2015). S.754 - 114th Congress: Cybersecurity Information Sharing Act of 2015. https://www.congress.gov/bill/114th-congress/senate-bill/754

U.S. Congress. (2020). CRS product R44926. https://www.congress.gov/crs-product/R44926

U.S. Congress. (2021). CRS product R46926. https://www.congress.gov/crs-product/R46926

U.S. Congress, Select Committee on Intelligence. (2021). Open hearing: Hack of U.S. networks by a foreign adversary (S. Hrg. 117-79). Congress.gov. https://www.congress.gov/event/117th-congress/senate-event/328260/text

U.S. Congress. (2025). CRS product IF10470. https://www.congress.gov/crs-product/IF10470

U.S. Department of Justice. (2023). Justice Department disrupts prolific ALPHV/BlackCat ransomware variant. U.S. DoJ. https://www.justice.gov/archives/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant

U.S. Department of State. (2021). Holding Russia to account (Press statement). https://2021-2025.state.gov/holding-russia-to-account

U.S. Department of State. (2024). United States International Cyberspace and Digital Strategy (FINAL 2024-05-15). https://2021-2025.state.gov/wp-content/uploads/2024/07/United-States-International-Cyberspace-and-Digital-Strategy-FINAL-2024-05-15_508v03-Section-508-Accessible-7.18.2024.pdf

U.S. Department of the Treasury. (2021). Treasury sanctions Russia with sweeping new sanctions authority (press release). https://home.treasury.gov/news/press-releases/jy0127

U.S. Department of Defence. (2015). The DOD Cyber Strategy 2015. https://nsarchive.gwu.edu/document/21384-document-25

U.S. Department of Defense. (2018). Cyber strategy 2018. https://dodcio.defense.gov/Portals/0/Documents/Library/CyberStrategy2018.pdf

U.S. Department of Defense. (2020). FY2020 Budget Request — Overview Book. https://comptroller.war.gov/Portals/45/Documents/defbudget/fy2020/fy2020_Budget_Request_Overview_Book.pdf

U.S. Department of Defense. (2021). FY2021 Budget Request — Overview Book. https://comptroller.war.gov/Portals/45/Documents/defbudget/fy2021/fy2021_Budget_Request_Overview_Book.pdf

U.S. Department of Defense. (2022). FY2022 Budget Request — Overview Book. https://comptroller.war.gov/Portals/45/Documents/defbudget/FY2022/FY2022_Budget_Request_Overview_Book.pdf

U.S. Department of Defense. (2023). FY2023 Budget Request — Overview Book. https://comptroller.war.gov/Portals/45/Documents/defbudget/FY2023/FY2023_Budget_Request_Overview_Book.pdf

U.S. Government Accountability Office. (2022). GAO-22-105117: Technology Modernization Fund: Implementation of recommendations can improve fee collection and proposal cost estimates. https://www.gao.gov/assets/gao-22-105117.pdf

U.S. Government Accountability Office. (2021). SolarWinds cyberattack demands significant federal and private sector response. https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic

U.S. Senate Republican Policy Committee. (2021). The SolarWinds cyberattack. https://www.rpc.senate.gov/policy-papers/the-solarwinds-cyberattack

U.S. Senate Select Committee on Intelligence. (2024). Hearing on the SolarWinds hack. https://www.congress.gov/event/117th-congress/senate-event/328260/text

Valeriano, B., & Jensen, B. (2021). Building a national cyber strategy: The process and implications of the Cyberspace Solarium Commission report. In 2021 13th International Conference on Cyber Conflict (CyCon) (pp. 189-214). https://doi.org/10.23919/CyCon51939.2021.9467806

Vienna Convention on Diplomatic Relations, April 18, 1961, 500 U.N.T.S. 95. https://legal.un.org/ilc/texts/instruments/english/conventions/9_1_1961.pdf

Waldman, A. (2020). CISA: Solarwinds backdoor attacks are “ongoing”: TechTarget. Search Security. https://www.techtarget.com/searchsecurity/news/252493842/CISA-SolarWinds-backdoor-attacks-are-ongoing?utm

Walton, R. (2020). DOE confirms its systems were compromised by SolarWinds hack. Utility Dive. https://www.utilitydive.com/news/doe-confirms-its-systems-were-compromised-by-solarwinds-hack/592441/

Weiss, D. C. (2021). Hackers accessed at least 80% of email accounts in New York federal prosecutors' offices, DOJ says. ABA Journal. https://www.abajournal.com/news/article/hackers-accessed-at-least-80-of-emails-in-new-york-federal-prosecutors-offices-justice-department-says

Whitney, L. (2021). How the SolarWinds attack may affect your organization's cybersecurity. TechRepublic. https://www.techrepublic.com/article/how-the-solarwinds-attack-may-affect-your-organizations-cybersecurity/

Willett, M. (2021). Lessons of the SolarWinds Hack. Survival, 63(2), 7–26. https://doi.org/10.1080/00396338.2021.1906001

Wilson, S. (2021). SolarWinds recap: The federal agencies caught in the Orion breach. FedScoop. https://fedscoop.com/solarwinds-recap-federal-agencies-caught-orion-breach/

Yin, R. K. (2018). Case Study Research and Applications: Design and Methods (6th ed.). Thousand Oaks, CA: SAGE Publications. ISBN: 9781506336169

Zacks. (2020). SolarWinds (SWI) depreciates 17% on cyberattack revelation. Nasdaq. https://www.nasdaq.com/articles/solarwinds-swi-depreciates-17-on-cyberattack-revelation-2020-