Cyberattacks and Cyberpolitics: Subverting Systems

To what extent do cyberattacks on the US decrease American trust in government?

September 5th, 2022

Author Anna Lysenko

Supervisor Dr Joy Fitzgibbon

Laidlaw Scholars Program Report

Essay word count: 5,040

Acknowledgements:

No independent research is ever independent of the efforts and support of others. I could not have completed this project without the generous financial support of the Laidlaw Foundation. I am also grateful to the Laidlaw Foundation for the organizational support: the leadership workshops and the wide availability of resources and connections aided my research process immensely. Similarly, I am grateful to the U of T program, specifically Ms Shraddha Prasad, for always being there to help, guide, and check up on me.

I am also grateful to Dr Joy Fitzgibbon, my incredible supervisor and mentor in all ways. From my first year in her course, Dr Fitzgibbon validated my growing belief that cyberpolitics and cybersecurity are global issues that need more research and discussion. I cannot understate how much her advice has meant for me throughout researching and writing this essay.

Finally, I must thank my wonderful family for supporting me in my writing process, through words, homemade food, and hugs. I know they believe in me and my passions and that means a lot.

Trust is the foundation of all modern states. People choose to give the government legal authority over them by trusting it to protect them from harm, and act in their best humanitarian and economic interests.[1] Distrust in government leads to instability and potential state downfall. Considering how vital the trust link is for a government's existence, it is no surprise that internal and external actors seek new ways to undermine it. Historically, wars have demonstrated that a government was too weak to protect its people.[2] However, times have changed, and so have the threats to trust. Although physical wars wage, cyberspace is a new domain for weakening statehood.

From 2011 to 2021, the number of internet users has grown from 2.1 billion to 4.9 billion.[3] The growing digital landscape is creating unprecedented scales of communication and collaboration. However, as cyberspace rises to present new opportunities, cyberattacks are corresponding threats. According to SonicWall's 2022 Cyber Threat Report, there were 623.2 million global ransomware attacks in 2021, representing a 105% increase since 2020.[4] That number will rise alongside accelerating societal technological integration; cars, factories, and nuclear plants are linking into networks that are more vulnerable than technicians or consumers realize. Three recent, notable examples this essay considers are the May 2021 Colonial Pipeline (CP) attack, the May 2021 JBS meat facility attack, and the March 2020 SolarWinds data breach. Cyberattacks reveal the true vulnerability of network systems, leading to economic and reputational loss. Actors affected by cyberattacks reflect on their digital flaws and question those

[1] Uzgalis, William. 2022. "John Locke." Stanford Encyclopedia of Philosophy. Stanford University. https://plato.stanford.edu/entries/locke/.
[2] Keen, David. 2011. "The Political Economy of War', in Frances Stewart, and Valpy Fitzgerald (eds), War and Underdevelopment: Volume 1: The Economic and Social Consequences of Conflict (Oxford; online edn, Oxford Academic), https://doi.org/10.1093/acprof:oso/9780199241866.003.0003.
[3] Statista Research Department. 2022. "Number of Internet Users 2021." Statista. https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/.
[4] 2022 SonicWall Cyber Threat Report. 2022. SonicWall. https://www.sonicwall.com/medialibrary/en/white-paper/2022-sonicwall-cyber-threat-report.pdf.

entrusted to protect them from threats: the government.[5] As such, this paper considers the intersection of cyberspace, government, and trust, aiming to answer the question "To what extent do cyberattacks on the US decrease American trust in government?" An analysis of available secondary sources leads this essay to the thesis that cyberattacks on the US decrease American trust in government by making people question their belief in the state's ability to protect them from new threats to infrastructure, food security, and privacy.

The literature on cyberspace is modest in size but fierce in ideas, growing each year. This essay's primary purpose is to fill a gap in the research regarding how cyberattacks affect political society beyond their technical impacts, with a secondary purpose being to highlight potential directions for the field. This essay's methodology was case study analysis using secondary sources. The case studies and associated polls served as a vehicle to discuss the far-reaching implications of cyberattacks on power, politics, and society.

Research began with an overview of the American government's structure, and the analysis of recent polls of American public confidence in government. Next, the history of cyberspace was studied through academic articles, and author Jamie Susskind's book "Future Politics". Susskind's unique questioning of how technology alters society's notions of power provided a strong starting point for further reading.[6] News articles were used to research the three selected case studies and provide context on how the public perceives cyberattacks. Notably, news articles framed all three attacks as warnings of future dangers.[7] These worries were reflected in

[5] Shandler, Ryan, and Miguel Alberto Gomez. 2022. "The hidden threat of cyber-attacks – undermining public confidence in government." Journal of Information Technology & Politics, DOI: 10.1080/19331681.2022.2112796.
[6] Susskind, Jamie. 2020. *Future Politics: Living Together in a World Transformed by Tech*. Oxford: Oxford University Press.
[7] Bordoff, Jason. 2021. "The Colonial Pipeline Crisis Is a Taste of Things to Come." Foreign Policy. https://foreignpolicy.com/2021/05/17/colonial-pipeline-crisis-cyberattack-ransomware-cybersecurity-energy-electicity-power-grid-russia-hackers/.

John Carlin's book, *Dawn of the Code War*, and Nicole Perlroth's book, *This is How They Tell Me the World Ends*. Perlroth, a cybersecurity journalist for the New York Times, highlighted how the US government has fallen behind the underground cyberthreat landscape by failing to recognize it as a serious source of power.[8] Carlin, a former deputy attorney general in the US Department of Justice, also argues that the US government has lagged in conquering cyberspace, focusing his arguments on cybercrime, state espionage, and the "cyberwar" these activities entailed.[9] Conversely, political scientist Thomas Rid argued against the notion of "cyberwar", claiming that all cyberattacks are "sophisticated versions of three activities": sabotage, espionage, and subversion.[10]

Although the three authors held different notions of cyberwar, they agreed that cyberattacks cause immediate damage to targeted actors and cause long-term digital and sociopolitical decline.[11] Failure to address cybersecurity and prevent cyberattacks leads to governmental, organizational, and public disappointment with the state's strength, leading to demands for a stronger, more competent government.[12]

Cyberattacks are defined as attempts by state or non-state actors to damage or incapacitate a digital system or network.[13] Cybersecurity is understood as an actor's ability to prevent or deter cyberattacks, through both digital and strategic means.[14]

---

[8] Perlroth, Nicole. 2021. *This Is How They Tell Me the World Ends: the Cyberweapons Arms Race.* New York: Bloomsbury Publishing.
[9] Carlin, John P, and Garrett M Graff. 2018. *Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat*. New York: PublicAffairs.
[10] Rid, Thomas. 2017. *Cyber War Will Not Take Place.* London: Hurst & Company.
[11] Carlin and Graff, *Dawn of the Code War,* 5; Perlroth, *This Is How They Tell Me*, 11.
[12] Gordon, Susan. 2022. "How the U.S. Can Be Better Prepared against Cybersecurity Threats." NPR. NPR. https://www.npr.org/2022/01/01/1069672088/how-the-u-s-can-be-better-prepared-against-cybersecurity-threats.
[13] CSRC Content. 2022. "Cyber Attack - Glossary: CSRC." CSRC Content Editor. https://csrc.nist.gov/glossary/term/Cyber_Attack; "What Is a Cyberattack?" IBM. https://www.ibm.com/topics/cyber-attack.
[14] 2019. "Security Tip (ST04-001): Cybersecurity Definition." CISA. https://www.cisa.gov/uscert/ncas/tips/ST04-001; 2022. "What Is Cybersecurity?" IBM. https://www.ibm.com/topics/cybersecurity.

America's government form is a representational democracy: people vote for leaders to represent their governance choices.[15] Trust is critical to democracy; people trust their government to protect them from harm and promote their interests. Political scientist John Locke described this relationship as a social contract: the people consented to government authority in exchange for safety, law, and order.[16] Locke insisted the people must question their government to maintain this contract. Thus, new threats, such as cyberattacks, present a challenge to the government, since it must reaffirm its ability to uphold the contract and protect its people. This essay evaluates America's governmental failures in cybersecurity, which has led to a somewhat weakened trust bond with its people. However, cybersecurity is also acknowledged as an opportunity to strengthen American governance, a note on which this essay will touch upon in the closing section. As such, this essay takes "trust in government" to mean the extent to which Americans believe the government is effectively protecting them from harm while promoting their interests.

Here it is worth noting that the research process revealed a vast trove of resources related to the effects of misinformation and disinformation on trust in government.[17] Both topics are valuable to cyberpolitics, however, this essay overlooks them for conciseness. Furthermore, while Russia is rumored to be the aggressor in all three case studies this essay discusses, this essay frames Russia as an external malicious actor, without emphasising the specific intentions or capabilities of Russia itself.[18] This essay will also not discuss Russian cyberattacks on American elections in

[15] Bouie, Jamelle, Jon Grinspan, Jill Lepore, and Yascha Mounk. 2022. "Renewing America Series: The History of American Democracy." Council on Foreign Relations. Council on Foreign Relations. https://www.cfr.org/event/renewing-america-series-history-american-democracy.
[16] Uzgalis, "John Locke.".
[17] Ross, Robert M, David G Rand, and Gordon Pennycook. 2021. "Beyond 'Fake News': Analytic Thinking and the Detection of False and Hyperpartisan News Headlines." Judgment and Decision Making 16 (2): 484–504; Vizoso, Angel, Martin Vaz-Alvarez, and Xose Lopez-Garcia. 2021. "Fighting Deepfakes: Media and Internet Giants' Converging and Diverging Strategies Against Hi-Tech Misinformation." Media and Communication (Lisboa) 9 (1S2): 291–300. https://doi.org/10.17645/mac.v9i1.3494.
[18] Hill, Fiona, and William Brangham. 2020. "What Russia Stands to Gain from a Cyberattack against the U.S." PBS. Public Broadcasting Service. https://www.pbs.org/newshour/show/what-russia-stands-to-gain-from-a-cyberattack-against-the-u-s.

November 2020; although elections are critical to America's democratic government, this essay's has a different focus.[19] Furthermore, this essay does not claim that cyberattacks are the largest source of mistrust in government: a variety of other political factors likely have a greater effect. This essay only aims to recognize the disordering effect cyberattacks have on the government's connection with its people.

The CP attack demonstrated that cyberattacks decrease American trust in government by revealing the looming threat to critical infrastructure. The CP attack was the largest publicly disclosed cyberattack on American infrastructure, representing a critical juncture in how the public and the government understood cyberattacks as real threats to society.[20] Similar to the JBS meat attack and the SolarWinds data breach, the CP attack's menace was in its ability to make Americans doubt their government's approach to cyber and national security.

The Colonial Pipeline is the largest pipeline system for refined oil products in America, running from Texas to New York.[21] The pipeline carries around 2.5 million oil barrels per day, supplying a vast portion of the population.[22] On April 29th, hackers gained access to the digital pipeline system due to a single compromised password.[23] Around 5 AM on May 7, a CP employee noticed a computer displaying a ransom note demanding cryptocurrency. Supervisors were

[19] Shackelford, Scott J.,J.D.PhD., Angie Raymond J.D., Abbey Stemler J.D.M.B.A., and Cyanne Loyle PhD. 2020. "Defending Democracy: Taking Stock of the Global Fight Against Digital Repression, Disinformation, and Election Insecurity." *Washington and Lee Law Review* 77 (4) (Fall): 1747-1809.
[20] Kerner, Sean Michael. 2022. "Colonial Pipeline Hack Explained: Everything You Need to Know." WhatIs.com. TechTarget. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know.
[21] Resnickault, Jessica, and Stephanie Kelly. 2021. "One Password Allowed Hackers to Disrupt Colonial Pipeline, CEO Tells Senators." Reuters. Thomson Reuters. https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/.
[22] Morrison, Sara. 2021. "How a Major Oil Pipeline Got Held for Ransom." Vox. Vox. https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices.
[23] Duffy, Clare. 2021. "Colonial Pipeline Attack: A 'Wake up Call' about the Threat of Ransomware." CNN. Cable News Network. https://www.cnn.com/2021/05/16/tech/colonial-ransomware-darkside-what-to-know/index.html.

notified and the entire pipeline was shut down within an hour.[24] The hackers notified Colonial that they stole nearly 100 gigabytes of employee data and threatened to leak it if the ransom was not paid. Government agencies, including the FBI, were alerted.[25] The next day, Colonial paid the hackers $4.4 million in Bitcoin for the decryption key to unlock their systems but warned the public that restoring operations would take a few days.[26] News of the attack spread online, creating a wave of public panic and national gas shortages as people queued at gas stations.[27] The sudden surge in gas prices led President Joseph Biden to declare a state of emergency on May 9, temporarily removing limits on amounts of domestic gas transported.[28] The CP restored full operation on May 12. Later investigation of the attack led to experts stating that REvil, a Russian cybercriminal organization with informal ties to the Russian government, was behind the attack.[29]

The scale and implications of the CP attack were notable, contributing to cyberattack's negative impact on public trust in government. Cyberattacks were on the rise before the CP attack; according to a report by Imperva, 58.3% of American individuals and organizations were targets of ransomware attacks in 2019, with 45% of businesses reporting that they paid the ransom to get their data back.[30] Most companies preferred to keep news of being cyberattacked away from public knowledge, fearing reputational repercussions.[31] Despite 2018 Pew polls showing that 46% of

[24] Turton, William, and Kartikay Mehrotra. 2021. "Colonial Pipeline Cyber Attack: Hackers Used Compromised Password." Bloomberg.com. Bloomberg. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password#xj4y7vzkg.
[25] Resnickault and Kelly,"One Password Allowed Hackers…".
[26] Wilkie, Christina. 2021."Colonial Pipeline Paid $5 Million Ransom One Day after Cyberattack, CEO Tells Senate." CNBC. https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html.
[27] Jones, David. 2022. "How the Colonial Pipeline Attack Instilled Urgency in Cybersecurity." Cybersecurity Dive. https://www.cybersecuritydive.com/news/post-colonial-pipeline-attack/623859/.
[28] 2021. "Remarks by President Biden on the Colonial Pipeline Incident." The White House. The United States Government. https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/05/13/remarks-by-president-biden-on-the-colonial-pipeline-incident/.
[29] Tarabay, Jamie. 2021. "Darkside, Revil Go Quiet after Colonial Pipeline, JBS Hacks." Bloomberg.com. Bloomberg. https://www.bloomberg.com/news/newsletters/2021-06-28/darkside-revil-go-quiet-after-colonial-pipeline-jbs-hacks.
[30] Imperva Editors. 2021. "2019 Cyberthreat Defense Report - Imperva." Imperva. https://www.imperva.com/resources/reports/CyberEdge-2019-CDR-Report-v1.1.pdf.
[31] Carlin and Graff, *Dawn of the Code War,* 62; Waldman, Arielle. 2022. "Enterprises Reluctant to Report Cyber Attacks to Authorities." SearchSecurity. TechTarget. https://www.techtarget.com/searchsecurity/feature/Enterprises-reluctant-to-report-cyber-attacks-to-authorities.

Americans believed that it was "very likely" that cyberattacks would damage public infrastructure in the future, the government failed to make cybersecurity a national security priority.[32] The CP attack was a monumental, symbolic case to bring the extent of the problem to public attention. The attack was a national demonstration of America's fragility in cyberspace, and a signal to all Americans affected by cyberattacks that the problem was bigger than their systems.

Many cybersecurity experts, including John Carlin and Joe R. Reeder, claimed that the CP attack was America's long-awaited digital Pearl Harbour.[33] Although previous cyberattacks on American infrastructures, such as San Francisco's MUNI light-rail system in 2016, garnered some public attention, the CP attack contextualized national cybersecurity as a real threat to the public.[34] According to polls from Politico, 46% of American voters said they saw, read or heard "a lot" about the pipeline shutdown.[35] Marty Edwards, former director of industrial control systems for the Cybersecurity and Infrastructure Security Agency (CISA) stated the attack "[showed] the impact cybersecurity has on our everyday lives".[36] State power lies in the government's ability to protect its citizens, so the ability of distant hackers to create significant disruption in American society through an invisible threat led to increased national concern.

The scale and effects of the CP attack prompted urgent questions about future cyberattacks on critical targets, such as nuclear plants, healthcare facilities, and military bases. Although some speculation may have been dramatized due to sensationalized news coverage, real

[32] Poushter, Jacob, and Janell Fetterolf. 2020. "International Publics Brace for Cyberattacks on Elections, Infrastructure, National Security." Pew Research Center's Global Attitudes Project. Pew Research Center. https://www.pewresearch.org/global/2019/01/09/international-publics-brace-for-cyberattacks-on-elections-infrastructure-national-security/.
[33] Carlin and Graff, *Dawn of the Code War,* 22; Reeder, Joe, Paul McQuade, and Scott Schipma. 2021."Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack: Insights: Greenberg Traurig LLP." Insights | Greenberg Traurig LLP. https://www.gtlaw.com/en/insights/2021/8/published-articles/cybersecuritys-pearl-harbor-moment.
[34] Weinberg, Adam. 2021. "Analysis of Top 11 Cyber Attackson Critical Infrastructure." FirstPoint. https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure/.
[35] Jenkins, Lisa Martine. 2021."Hackers, Consumers, Colonial Pipeline Deserve the Most Blame for U.S. Gas Shortages, Voters Say." Morning Consult. https://morningconsult.com/2021/05/19/gasoline-shortage-polling/.
[36] Morrison, "How a Major Oil Pipeline Got Held for Ransom.".

probes about America's state of cybersecurity became a point of national discussion. According to Rasmussen Reports, surveys found that 29% of American voters were "not very confident" the government could protect against future cyberattacks similar to the CP attack and 25% were "not at all confident".[37] The uncertain replies to the polls could serve as an indication of the general scepticism surrounding the government's effectiveness at addressing rising threats.

The CP attack demonstrated the challenge cyberattacks present to typical military notions of violence and security. In his book, Cyber War Will Not Take Place, Thomas Rid uses Carl Von Clausewitz's definition of war as "violence, fatal, instrumental, and political" to dismiss the possibility of cyberwar.[38] However, Clausewitz's definition is outdated for today's dynamic cyberconflict. Rid and political theorist David Omand pose that cyberattacks are subversive, meaning they interfere in a nation's affairs to change power systems in the aggressor's favour.[39] Cyberattacks undermine state sovereignty by demonstrating the government's incompetence at protecting its digital borders, nurturing public anxiety, and leading to societal friction and decay over time which could become violent.[40] The government's standard practice to relate violence to danger leads to a short-sighted cybersecurity response that fails to recognize the internal pressures externally-targeted cyberattacks stoke. Cybersecurity could become the new testing ground of American control over its internal stability so the American security paradigm must shift to recognize cyberattacks as critical security threats.

[37] Rasmussen Polls. 2021. "Less than Half of U.S. Voters Confident Government Can Protect Pipelines." Rasmussen Reports. https://www.rasmussenreports.com/public_content/politics/general_politics/may_2021/less_than_half_of_u_s_voters_confident_government_can_protect_pipelines.
[38] Rid, *Cyber War Will Not Take Place*, 54.
[39] Omand, David. "The Threats from Modern Digital Subversion and Sedition." Journal of Cyber Policy 3, no. 1 (2018): 5–23. https://doi.org/10.1080/23738871.2018.1448097; Rid, *Cyber War Will Not Take Place*, 247.
[40] Omand, "The Threats from Modern Digital Subversion…", 9.

Attempting to address the inadequacies which led to the CP attack and to prevent future incidents, Biden signed Executive Order 14028 on May 12.[41] The order updated software security standards for sales to the government, improved governmental information sharing and training, and refined incident response, among other actions.[42] The order was praised by cybersecurity experts and the media, as it indicated the government shifting from a case-by-case cybersecurity response to a more holistic, preventative approach.[43] Still, many experts, such as political scientist Joseph Nye and Forbes Councils member Andy Purdy, stated that this was just the beginning of what needed to be a fundamental remaking in how the government addresses cybersecurity.[44] Overall, the CP attack served as a landmark case for American cybersecurity, undermining some of the government's legitimacy by making people question the government's unpreparedness for the attack.[45]

Less than a month after the CP attack, the JBS cyberattack showed that cyberattacks weaken American trust in government by threatening food security. While the JBS attack garnered relatively less media coverage than the earlier CP attack, it led to similar questions about how the government is failing to address cybersecurity threats, as well as worries that more attacks on the

[41] Breuninger, Kevin, and Amanda Macias. 2021."Biden Signs Executive Order to Strengthen U.S. Cybersecurity Defenses after Colonial Pipeline Hack." CNBC. CNBC,. https://www.cnbc.com/2021/05/12/biden-signs-executive-order-to-strengthen-cybersecurity-after-colonial-pipeline-hack.html.
[42] Biden, Joseph, Jr. 2021."Executive Order on Improving the Nation's Cybersecurity." The White House. The United States Government. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.
[43] Morrison, "How a Major Oil Pipeline Got Held for Ransom."; Ordoñez, Franco. 2021. "In Wake of Pipeline Hack, Biden Signs Executive Order on Cybersecurity." NPR. NPR. https://www.npr.org/2021/05/12/996355601/in-wake-of-pipeline-hack-biden-signs-executive-order-on-cybersecurity.
[44] Camp, Jean. 2022. "Does Biden's Cybersecurity Order Go Far Enough?" Brookings. Brookings. https://www.brookings.edu/blog/techtank/2022/06/24/does-bidens-cybersecurity-order-go-far-enough/; Perlroth, *This Is How They Tell Me*, 56; Purdy, Andy. 2021. "Council Post: The US Needs a Stronger Commitment to Cybersecurity." Forbes. Forbes Magazine. https://www.forbes.com/sites/forbestechcouncil/2021/07/30/the-us-needs-a-stronger-commitment-to-cybersecurity/?sh=3d5f69f95daf.
[45] Breuninger and Macias, "Biden Signs Executive Order…"; Kerner, "Colonial Pipeline Hack Explained…".

agricultural industry would follow.[46] The JBS attack also exacerbated America's rivalry with Russia, since it was suspected that the same Russian cybercriminal group, REvil, was responsible for the JBS attack.[47]

JBS SA is a Brazilian-based meat company with factories around the world; it is one of the four largest global meat providers.[48] On May 30, workers at JBS realized they were targets of a sophisticated cyberattack through a ransom note on their computers.[49] Hackers infiltrated the meat supplier's network, taking control over various beef and pork slaughterhouses in America, Canada, and Australia.[50] The hackers did not tamper with the systems but threatened to damage major networks and delete important files if the ransom was not paid.[51] JBS shut down all systems, and contacted government authorities, as well as on-call cybersecurity experts in an attempt to take back system control.[52] Despite diligent efforts, on June 9, a JBS spokesperson confirmed that the company paid around $11 million in Bitcoin to get a decryption key.[53] Afterwards, JBS confirmed that it restored all operations and that it appeared that no data was stolen during the attack.[54] While all JBS meat facilities were shut down, the number of cattle slaughtered in America fell 22% in comparison to the previous week, leading to prices for choice American beef to rise more than 1%,

[46] Rosenbaum, Eric. 2021. "JBS Cyberattack: From Gas to Meat, Hackers Are Hitting the Nation, and Consumers, Where It Hurts." CNBC. CNBC. https://www.cnbc.com/2021/06/02/from-gas-to-burgers-hackers-hit-consumers-where-it-hurts.html.
[47] Tarabay, "Darkside, Revil Go Quiet...".
[48] Forbes Editors. 2011. "JBS: The Story behind the World's Biggest Meat Producer." Forbes. Forbes Magazine. https://www.forbes.com/sites/kerenblankfeld/2011/04/21/jbs-the-story-behind-the-worlds-biggest-meat-producer/?sh=449c9a297e82.
[49] Associated Press. 2021. "Largest Meat Producer Getting Back Online after Cyberattack." PBS. Public Broadcasting Service. https://www.pbs.org/newshour/world/largest-meat-producer-getting-back-online-after-cyberattack.
[50] Scheiber, Noam, Julie Creswell, and Nicole Perlroth. 2021."Ransomware Disrupts Meat Plants in Latest Attack on Critical U.S. Business." The New York Times. The New York Times. https://www.nytimes.com/2021/06/01/business/meat-plant-cyberattack-jbs.html%20%20June%201,%20updated%20June%203%202021.
[51] 2021. "Largest Meat Producer Getting Back Online after Cyberattack." PBS. Public Broadcasting Service. https://www.pbs.org/newshour/world/largest-meat-producer-getting-back-online-after-cyberattack;
[52] 2021. "Meat Company JBS Foods Confirms It Paid US$11m Ransom in Cyberattack." Global News. Global News. https://globalnews.ca/news/7936930/jbs-foods-ransomware-attack-paid/.
[53] Sganga, Nicole. 2021. "JBS Paid $11 Million Ransom after Cyberattack." CBS News. CBS Interactive. https://www.cbsnews.com/news/jbs-ransom-11-million/.
[54] 2021. "Media Statement: JBS USA Cybersecurity Attack." GlobeNewswire News Room. JBS USA, LLC. https://www.globenewswire.com/news-release/2021/05/31/2239049/17532/en/Media-Statement-JBS-USA-Cybersecurity-Attack.html.

according to the USDA.[55] While this minor price increase may not have affected average consumers, this development demonstrated the real-world effects cyberattacks have on the economy.

The JBS case highlighted the fragility of food security in the US, prompting companies and consumers to doubt America's ability to defend supply chains from cyberattacks, especially considering exacerbated anxieties over supply chains brought on by the COVID-19 pandemic.[56] Notably, the JBS attack highlighted the cross-industry nature of cyberattacks themselves; in the CP and JBS cases, the industries affected were different yet both had similar digital vulnerabilities.[57] Cyberattacks' versatility leads to valid concerns over American food security since it is critical to a functioning state, as highlighted by American Senator John Thune's comment that "attacks like this one highlight the vulnerabilities in our nation's food supply chain security…".[58] Furthermore, the fact that JBS paid the ransom was criticized by experts such as Allie Mellen, a senior analyst at Forrester Research, as they claimed that paying cyberattacks ransoms tempts more hackers to attempt similar feats.[59] Paying the ransom also underscores the government's inability to aid companies with the necessary preparedness, speed, and efficiency to recover their systems. The American government's inability to arrest the JBS hackers prompts

[55] 2021. "U.S. Says Ransomware Attack on Meatpacker JBS Likely from Russia; Cattle Slaughter Resuming." CNBC. CNBC. https://www.cnbc.com/2021/06/01/big-north-american-meat-plants-halt-operations-after-jbs-cyberattack.html; Batista, Fabiana, Michael Hirtzer, and Mike Dorning. 2021. "JBS Cyber Hack: Meat Supplier Shuts down Some Slaughterhouses after Attack." Bloomberg.com. Bloomberg. https://www.bloomberg.com/news/articles/2021-05-31/meat-is-latest-cyber-victim-as-hackers-hit-top-supplier-jbs.
[56] Perlroth, *This Is How They Tell Me*, 154; Tsafos, Nikos, Lachlan Carey, Jane Nakano, and Sarah Ladislaw. 2021."Cyber and Other Security Risks to the U.S. Electric Power Infrastructure." Reshore, Reroute, Rebalance: A U.S. Strategy for Clean Energy Supply Chains. Center for Strategic and International Studies (CSIS). http://www.jstor.org/stable/resrep32324.6.
[57] Morrison, Sara. 2021. "Ransomware Attack Hits Another Massive, Crucial Industry: Meat." Vox. Vox. https://www.vox.com/recode/2021/6/1/22463179/jbs-foods-ransomware-attack-meat-hackers.
[58] Batista, Hirtzer, and Dorning. "JBS Cyber Hack…".
[59] Johnson, Kyle. 2021. "Should Companies Pay after Ransomware Attacks? Is It Illegal?" SearchSecurity. TechTarget. https://www.techtarget.com/searchsecurity/tip/Should-companies-pay-ransomware-and-is-it-illegal-to; Sganga, "JBS Paid $11 Million Ransom after Cyberattack.".

further questions about their ability to protect American food security in the future, thus chipping away at the trust between the government and the people.[60]

The JBS attack undermined American trust in government by highlighting America's disempowerment in cyberspace. Since the end of the Cold War, America has grown accustomed to hegemony in global military, economic, and political affairs.[61] Yet cyberspace has allowed state and non-state actors to level the playing field, as cyberattacks are cheap, deniable, and psychologically effective.[62] Cyberattack attribution ease and confidence are worth considering; a screen of ambiguity benefits attackers aiming to undermine public trust in government because anonymous attacks cast doubt over the government's ability to defend its people against an external actor, the power and intentions of which are unknown.[63] Certainty regarding an attack's origins may result in public calls for specific policy by the government, with public reactions being exacerbated by America's diplomatic relations with the suspected offender before the attack. Confident public attribution of cyberattacks redirects mistrust in government from an abstract, anxiety-inducing threat to a specific, containable one. The government's failure to address the latter could lead to its public humiliation, which could undermine its power, but the tension of an unattributed cyberattack is more potent for stirring public paranoia which could lead to state instability.

---

[60] Omand, "The Threats from Modern Digital Subversion…", 6; 2021. "Revil, a Notorious Ransomware Gang, Was behind JBS Cyberattack, the FBI Says." NPR. https://www.npr.org/2021/06/03/1002819883/revil-a-notorious-ransomware-gang-was-behind-jbs-cyberattack-the-fbi-says.

[61] Carlin and Graff, *Dawn of the Code War,* 352; Cooley, Alexander, and Daniel H. Nexon. 2022. "How Hegemony Ends." Foreign Affairs. https://www.foreignaffairs.com/articles/united-states/2020-06-09/how-hegemony-ends.

[62] Paul, Kari, and Lois Beckett. 2020. "What We Know – and Still Don't – about the Worst-Ever US Government Cyber-Attack." The Guardian. Guardian News and Media. https://www.theguardian.com/technology/2020/dec/18/orion-hack-solarwinds-explainer-us-government.

[63] Mussington, David. 2019. "Strategic Stability, Cyber Operations and International Security." Centre for International Governance Innovation. https://www.cigionline.org/articles/strategic-stability-cyber-operations-and-international-security/; Perlroth, *This Is How They Tell Me*, 238.

The JBS attack also acted as an unwelcome political continuation of America's rivalry with Russia, in part because the earlier CP attack was also likely orchestrated by the Russia-based ransomware group REvil. A study by the Pearson Institute found that 72% of Americans consider the Russian government "a big threat" to American cybersecurity, with 73% of Americans considering the Chinese government "a big threat" to the same.[64] Both governments deny all ties with cybercriminal groups but it is believed that they are complicit, choosing to ignore illegal activity and reserve the right to co-opt cyberattacks for political purposes.[65] As such, on June 1, as the JBS attack was ongoing, White House spokeswoman Karine Jean-Pierre stated "the White House is engaging directly with the Russian government on this matter and delivering the message that responsible states do not harbour ransomware criminals."[66] This statement highlighted how cyberspace could be the new domain for state conflict and prompted discussions about geopolitical actions the government could take to prosecute the responsible actors.[67]

The SolarWinds data breach demonstrated that cyberattacks decrease American trust in government by challenging governmental power over privacy. The attack is noted as one of the most significant data breaches of the 21st century, and a fascinating case into the structures and values cyberattacks target since, unlike gas and agriculture, data is incorporeal.[68] Furthermore, the SolarWinds attack directly affected the government, leaving citizens surprised to learn the

[64] Suderman, Alan. 2021. "Cyberattacks Concerning to Most in US: Pearson/AP-Norc Poll." theintelligencer.net. The Intelligencer. https://www.theintelligencer.net/news/top-headlines/2021/10/cyberattacks-concerning-to-most-in-us-pearson-ap-norc-poll/.
[65] Carlin and Graff, *Dawn of the Code War,* 121; Perlroth, *This Is How They Tell Me*, 146 .
[66] Miller, Maggie. 2021. "White House Says Cyberattack on Meat Producer JBS Likely from Russia." The Hill. The Hill. https://thehill.com/policy/cybersecurity/556329-white-house-engaging-with-russian-government-to-respond-to-jbs/.
[67] Carlin and Graff, *Dawn of the Code War,* 377; Pawlak, Patryk. 2017. "A Wild Wild Web?: Law, Norms, Crime and Politics in Cyberspace." European Union Institute for Security Studies (EUISS). http://www.jstor.org/stable/resrep17449; Perlorth, *This is How They Tell Me…*, 259.
[68] Jibilian, Isabella. 2021. "The US Is Readying Sanctions against Russia over the SolarWinds Cyber Attack. Here's a Simple Explanation of How the Massive Hack Happened and Why It's Such a Big Deal." Business Insider. Business Insider. https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12.

government's lethargic cybersecurity posture, and wondering how the government can protect its people, or be cyberspace's leader, if it cannot defend itself.[69]

On December 17, the CISA announced that they were aware of a series of compromises by an advanced persistent threat (APT) beginning as early as March 2020.[70] Malicious code was inserted into the popular network-monitoring software Orion, made by the company SolarWinds.[71] The code was distributed through a standard update package.[72] Adam Meyers, vice president for threat intelligence at the cybersecurity firm CrowdStrike which first uncovered the virus, noted that the attack began "with a tiny strip of code" which he traced back to September 2019.[73] The attack used a bait-and-switch mechanism; the attackers inserted their strip of malicious code into the finished package right after the code had undergone review, and just before it was sent away, to be interpreted by receiving devices.[74] Nearly 18,000 users installed the malicious update, including key federal agencies, from the Department of Homeland Security to the United States Department of Energy.[75] SolarWinds' malicious code had been wiped clean of all state identifiers, alluding to the vitality of cyberattack attribution, as discussed previously. [76] Still, the Russian

[69] Schwartz, Samantha. 2020. "Federal Agencies Fall Short on Cybersecurity, Undermining Standards." Cybersecurity Dive, December 17, 2020. https://www.cybersecuritydive.com/news/solarwinds-cyberattack-treasury-financial-sector-security/592301/; U.S. Government Accountability Office. 2022. "Solarwinds Cyberattack Demands Significant Federal and Private-Sector Response (Infographic)." U.S. GAO. https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic.
[70] Cybersecurity & Infrastructure Security Agency. 2020. "Alert (AA20-352A)." CISA. https://www.cisa.gov/uscert/ncas/alerts/aa20-352a.
[71] Baker, Pam. 2021. "The Solarwinds Hack Timeline: Who Knew What, and When?" CSO Online. CSO. https://www.csoonline.com/article/3613571/the-solarwinds-hack-timeline-who-knew-what-and-when.html.
[72] Macias, Amanda. 2020. "White House Acknowledges Reports of Cyberattack on U.S. Treasury by Foreign Government." CNBC. CNBC. https://www.cnbc.com/2020/12/13/cyber-hack-on-us-treasury-by-foreign-government-.html; Kari and Beckett, "What We Know – and Still Don't…";
[73] Temple-Raston, Dina. 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.
[74] Nakashima, Ellen, and Craig Timberg. 2020. "Russian Government Hackers Are behind a Broad Espionage Campaign That Has Compromised U.S. Agencies, Including Treasury and Commerce." The Washington Post. WP Company. 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.
[75] Whitaker, Bill. 2021. "Solarwinds: How Russian Spies Hacked the Justice, State, Treasury, Energy and Commerce Departments." CBS News. https://www.cbsnews.com/news/solarwinds-hack-russia-cyberattack-60-minutes-2021-07-04/.
[76] BBC Editors. 2021. "Solarwinds Hack: Russian Denial 'Unconvincing'." BBC News. BBC. https://www.bbc.com/news/technology-57156197; Temple-Raston, "A 'Worst Nightmare' Cyberattack…".

group “Cozy Bear”, a subdivision of Russia’s foreign intelligence services, is suspected to be responsible for the attack, although the Russian government has denied all claims of involvement.[77] Most believe that Russia’s intentions were cyberespionage, although the full extent of the attack remains unknown.[78]

The SolarWinds data breach eroded American trust in government by demonstrating the government’s inability to protect American privacy, both as data and as an American democratic value. According to a 2022 IPSOS poll, 84% of Americans say they are at least somewhat concerned about their privacy and that of their data online.[79] In a time where more activities are online than ever, data is a digital puzzle that may be the key to understanding citizen’s patterns; data analysis may reveal valuable insight into people’s attitudes and behaviours.[80] Malevolent actors may then use this analysis to launch calculated, targeted disinformation campaigns that influence populations over time.[81] Such actions are in opposition to the proper functioning, and spirit, of democracy. Privacy is considered a part or a prerequisite to freedom; according to Professor Benjamin J. Goold, privacy “fosters and encourages the moral autonomy of a citizen, a central requirement of a democracy”.[82] As such, data breaches such as the SolarWinds case could undermine American trust in government on a more long-term scale than other types of cyberattacks. The SolarWinds attack on privacy speaks to the threatening, subversive nature of cyberattacks, as analyzed by Thomas Rid. While data breaches are non-violent, and thus do not fit

[77] Vavra, Shannon, and Tim Starks. 2020. “How the Russian Hacking Group Cozy Bear, Suspected in the Solarwinds Breach, Plays The Long Game.” CyberScoop. https://www.cyberscoop.com/cozy-bear-apt29-solarwinds-russia-persistent/.
[78] Carlin and Graff, *Dawn of the Code War,* 273; Nakamisha and Timberg, “Russian Government Hackers Are behind a Broad Espionage Campaign…”.
[79] Newall, Mallory, and Johnny Sawyer. 2022. “A Majority of Americans Are Concerned about the Safety and... - Ipsos,”. https://www.ipsos.com/en-us/news-polls/majority-americans-are-concerned-about-safety-and-privacy-their-personal-data.
[80] Aradau, Claudia, and Tobias Blanke. 2017. “Politics of Prediction: Security and the Time/space of Governmentality in the Age of Big Data.” European Journal of Social Theory 20 (3): 373–91. https://doi.org/10.1177/1368431016667623.
[81] Ceron, Andrea, Luigi Curini, and Stefano Maria Iacus. 2017. Politics and Big Data: Nowcasting and Forecasting Elections with Social Media. Abingdon, Oxon: Routledge. https://doi.org/10.4324/9781315582733;
[82] Goold, Benjamin J. 2010. “How Much Surveillance is Too Much? Some Thoughts on Surveillance, Democracy, and the Political Value of Privacy" in DW Schartum, ed, Overvåkning i en rettsstat – Surveillance in a Constitutional Government (Fagbokforlaget: Bergen).

into Clausewitz's classical definition of warfare, they constitute a Machiavellian advantage in the age of information, which could lead to a gradual power shift.[83] As such, data breaches such as the SolarWinds case could decrease American trust in government by undercutting its democratic values.

The SolarWinds attack eroded American trust in government by publicizing its outdated, uncoordinated cybersecurity response. In an ironic twist, the government cyberthreat detection system, named Einstein, was unable to detect SolarWinds's malicious code due to its novelty; Christopher Krebs, head of protecting government networks, noted that Einstein only caught known threats.[84] There are also concerns that the SolarWinds attack may be ongoing. John Scott-Railton, a senior researcher at Citizen Lab at the University of Toronto's Munk School of Global Affairs and Public Policy, noted that "When an aggressive group like this gets an open sesame to many desirable systems, they are going to use it widely"[85]. Kevin Mandia, the CEO of FireEye, proposed that potential targeted systems could be utilities and healthcare, which are both vital to the functions and responsibilities of a strong state.[86]

The attack exposed the government's inability to adapt to cyberspace. A state's strength lies in its ability to rise to the challenge of new threats; the government should be ahead of its people regarding cybersecurity, not use outdated systems. The invalid nature of the government's cybersecurity response was also reflected in its internal incoordination.[87] Fiona Hill, a Russia expert and former National Security Council member, commented that "What we could have done

[83] Rid, *Cyber War Will Not Take Place*, 67.
[84] Temple-Raston, "A 'Worst Nightmare' Cyberattack...".
[85] Nakashima and Timberg, "Russian Government Hackers Are behind a Broad Espionage Campaign…"; Perlroth, *This Is How They Tell Me*, 274.
[86] Temple-Raston, "A 'Worst Nightmare' Cyberattack..."; Whitaker, "Solarwinds: How Russian Spies Hacked…".
[87] Burt, Andrew, and James C. Trainor. 2020. "The U.S. Needs a Standalone Agency to Fight Cyber Attacks." Time. Time. https://time.com/5757811/cybersecurity-attacks-agency/.

is had a coherent approach and not been at odds with each other".[88] Such statements do not inspire people to trust their government to protect them from future threats and point to an overarching issue with America's cybersecurity response: it is neither dynamic nor united. In an article for Foreign Affairs, political scientists Sue Gordon and Eric Rosenbach noted that America's approach to cybersecurity remains rooted in Cold War dynamics of slow, restrained operations but cyberspace is borderless, fast-paced, and abstract.[89] While it is difficult to forge a unified front against an enigmatic enemy, internal squabbles and mismanagement cause the public to suspect their government of weakness.

Confronting the government's lacklustre approach to cybersecurity could prevent future cyberattacks, improve the weakened trust bond between Americans and their government, and reaffirm America's power in cyberspace. According to research by The Harris Poll, 33% of Americans believed defending against cyberattacks should be a top priority for the government.[90] In the three cases analysed, cyberattacks affected trust in government by making the public question their government's competence to protect them from novel threats to infrastructure, food security, and privacy. Three potential approaches to enhance American cybersecurity are increased government transparency, collaboration with the private sector, and a more formidable cyber and geopolitical approach to state and non-state attackers.[91] All three approaches would herald a

[88] Woodruff, Judy, and William Brangham. 2020. "What Russia Stands to Gain from a Cyberattack against the U.S." PBS. Public Broadcasting Service. https://www.pbs.org/newshour/show/what-russia-stands-to-gain-from-a-cyberattack-against-the-u-s.
[89] Gordon, Sue, and Eric Rosenbach. 2022. "America's Cyber-Reckoning." Foreign Affairs. https://www.foreignaffairs.com/articles/united-states/2021-12-14/americas-cyber-reckoning; Perlroth, *This Is How They Tell Me*, 355.
[90] The Harris Poll. 2022."Colonial Pipeline Cyberattack Emphasizes What Research Finds." Tanium. https://www.tanium.com/blog/colonial-pipeline-cyberattack/.
[91] Carlin and Graff, *Dawn of the Code War,* 392; Gordon and Rosenbach, "America's Cyber-Reckoning."; Perlroth, *This Is How They Tell Me*, 231; Purdy, Council Post: The US Needs a Stronger Commitment to Cybersecurity.".

paradigm shift in how the American government approaches cybersecurity: not as a distant, looming threat but as ongoing conflicts that demand immediate, credible actions.

The government must recognize cybersecurity as a dynamic, ongoing challenge to national stability, and incorporate this changing outlook into internal and external communication and beurocracy structure. As Gordon and Rosenbach discuss, the American security sector approach to cybersecurity as a centralized, gradual threat is ineffective.[92] As this essay demonstrates, cyberattacks target various critical sectors so while governmental beurocracy is necessary for order, power structures must be streamlined to improve cross-departmental communication and information sharing. CISA should assert its role as the leading American cybersecurity agency by setting a clear cybersecurity agenda and overseeing the information-sharing program. It should act as a mediator, collector, and analyser of pertinent information, piecing it together to form a holistic view of the nation's cybersecurity state in routinized reports.

The government should acknowledge past and present deficiencies, and present actionable plans for improvement, along with the new cybersecurity approach.[93] Admitting that America's previous cybersecurity posture has been lacking may inspire short-term disbelief in the government's abilities by domestic and international actors, especially ones with which America has frigid diplomatic relations. However, it could also draw long-term respect from both groups and reinspire new, global efforts to create a peaceful, prosperous cyberspace.[94] Cyberattacks undermine trust in government by exploiting the assumption that citizens will be surprised to learn about the state's unpreparedness for the attack, and the subsequent humiliation this brings; being transparent about American cybersecurity could mitigate this disconnect.[95] Locke outlined clear

[92] Gordon and Rosenbach, "America's Cyber-Reckoning.".
[93] Gordon and Rosenbach, "America's Cyber-Reckoning.".
[94] Carlin and Graff, *Dawn of the Code War,* 109.
[95] Mussington, "Strategic Stability, Cyber Operations and International Security", 8.

communication and criticism as a necessary component of a healthy democracy.[96] Sharing cyberspace shortcomings and plans with Americans would reaffirm America's commitment to this principle. Furthermore, revealing America's new, united cybersecurity approach could act as deterrence against malicious actors, as revealing their cyberspace schemes would remove the cyberattacks' covert edge, and indicate America's readiness to respond to aggression.[97] Cyberattacks present a necessary, modern challenge to America's government, and a chance to adapt and improve, with feedback from citizens and companies.

Collaboration with the private sector is another way to strengthen American cybersecurity and repair weakened trust bonds between America's government and its people. According to The Harris Poll, 84% of Americans believe government agencies, the military and private companies should partner to prevent cyberattacks.[98] The Biden administration has attempted improvements, such as implementing the Cyber Incident Reporting for Critical Infrastructure Act of 2022, but the system remains incoherent.[99] A government-private partnership would bring mutual benefits; companies are often the targets of various cyberattacks, and the government could use their information about the attacks to create a more adaptive approach to addressing the computer viruses and condemning the actors responsible for the attacks.[100] In return, the government could provide companies with more streamlined options for dealing with cyberattacks, and emphasize the importance of digital hygiene and cybersecurity awareness.[101] The US has seen recent progress

[96] Uzgalis, "John Locke.".
[97] Bordelon, Emily B. 2016. "Approaching Cyber Warfare: Geopolitics, Deterrence, and International Law."
[98] The Harris Poll, "Colonial Pipeline Cyberattack Emphasizes...".
[99] Joyce, Sean, Joseph Nocera, Matt Gorham, and Emily Stapf. 2022. "Cyber Breach Reporting to Be Required by Law for Better Cyber Defense." PwC. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/cyber-breach-reporting-legislation.html.
[100] Dobrygowski, Daniel. 2019. "Why Companies Are Forming Cybersecurity Alliances." Harvard Business Review. https://hbr.org/2019/09/why-companies-are-forming-cybersecurity-alliances.
[101] Leal, Alejandro. 2022. "Public-Private Cooperation in Cyberspace." KuppingerCole. https://www.kuppingercole.com/blog/leal/public-private-cooperation-in-cyberspace; Lostri, Euginia, James Andrew Lewis, and Georgia Wood. 2022. "A Shared Responsibility: Public-Private Cooperation for Cybersecurity." A Shared Responsibility: Public-Private Cooperation for Cybersecurity | Center for Strategic and International Studies. https://www.csis.org/analysis/shared-responsibility-public-private-cooperation-cybersecurity.

on this agenda: CISA launched the Joint Cyber Defense Collaborative initiative in August 2021, with tech giants like Amazon, Google, and Microsoft all pledging collaborative intentions.[102]

A more long-term approach to cybersecurity could be setting clear domestic and international cyberspace norms, and researching how countries can capitalize on cyberspace's opportunities in peaceful ways. Research and norms could both be supported by international organizations such as the United Nations, simultaneously encouraging state responsibility and future collaboration.[103] Particular emphasis could be placed on public cyberattack attribution, prosecution, and extradition of the hackers responsible for attacks.[104] However, it has been noted that for collaboration to be productive, there must be actionable steps from both parties.[105] After the CP attack, Colonial Chief Executive Officer Joseph Blount stated, "the government needs to focus on the actors themselves…we don't have a political capability of shutting down the host countries that have these bad actors in them.".[106]

Legislation and foreign policy are both critical to improving cybersecurity and underpinning American trust in government. Cybersecurity experts, including Joseph Nye and Adam Segal, argue that although cyberspace is somewhat separated from traditional geopolitical actions, it is an extension of real-world politics and should therefore be treated as such.[107] Nye

---

[102] Koziol, Jack. 2022. "Cybersecurity Awareness: What It Is and How to Start." Forbes. Forbes Magazine. https://www.forbes.com/advisor/business/what-is-cybersecurity-awareness/; Reilly, Dan. 2021. "Cybersecurity Experts Say Public-Private Partnership Is the Key to Preventing Future Attacks." Fortune. Fortune. https://fortune.com/2021/11/16/cybersecurity-future-government-corporation-partnership-data-breach/.

[103] Kiyan, Olga. 2021."Establishing Cybersecurity Norms in the United Nations: The Role of U.S.-Russia Divergence." Harvard International Review. Harvard International Review, https://hir.harvard.edu/establishing-cybersecurity-norms-in-the-united-nations-the-role-of-u-s-russia-divergence/.

[104] Goel, Sanjay. 2020. "How Improved Attribution in Cyber Warfare Can Help De-Escalate Cyber Arms Race." Connections 19, no. 1: 87–95. https://www.jstor.org/stable/26934538; Nye, "The End of Cyber-Anarchy?"; Riordan, "The Geopolitics of Cyberspace:…"; Harkins, Ryan, and Erin English. 2022."Guarding the Public Sector: Seven Ways State Governments Can Boost Their Cybersecurity." Marsh McLennan. https://www.marshmclennan.com/insights/publications/2018/oct/guarding-the-public-sector--seven-ways-state-governments-can-boo.html; Nye, "The End of Cyber-Anarchy?"; Marciano, Miri, Walter Bohmayr, and Or Klier. 2022. "A Geopolitical Lens for Cyber Resilience." Boston Consulting Group. https://www.bcg.com/en-ca/publications/2022/geopolitical-lens-for-cyber-resilience.

[105] Lostri, Lewis, and Wood, "A Shared Responsibility: Public-Private Cooperation....".

[106] Turton, and Mehrotra. "Colonial Pipeline Cyber Attack….".

[107] Andres, Richard B. 2019. "Cyber Conflict and Geopolitics." Great Decisions, 69–78. https://www.jstor.org/stable/26739054; Riordan, Shaun. 2018. "The Geopolitics of Cyberspace: a Diplomatic Perspective." Brill. Brill Research Perspectives in

argues that ensuring national cybersecurity means reacting to cyberattacks through both digital and geopolitical tools, such as threats and sanctions.[108] Cyberattacks present tempting opportunities for states to anonymously undermine America, and addressing the root causes of such motivations could lead to fewer cyberattacks.[109] Evidence of this was former President Barack Obama's meeting with Chinese President Xi Jinping in 2015, after which cyberattacks on American businesses decreased.[110] Demonstrations of concrete policy actions by the government could be an effective way to earn citizens' trust, as they would see that cyberspace is being managed as an important issue, equal to that of other national concerns.

In 2021, President Biden moved the government in the right direction by outlining a three-pronged cyberspace agenda by modernizing cyber defences, increasing international activity, and ensuring America establish a competitive cyberspace edge.[111] These actions could indicate that America is on its way to regaining the trust of its people and growing as a cyberspace power, but further policy is necessary.

Cyberattacks on the US decrease American trust in government by making citizens question the government's capability to protect them from threats to infrastructure, food, and privacy.[112] The nature of cyberattacks themselves is threatening since they have versatile targets

---

Diplomacy and Foreign Policy.
https://www.researchgate.net/publication/334228866_The_Geopolitics_of_Cyberspace_a_Diplomatic_Perspective.
[108] Nye, Joseph Jr. 2022. "The End of Cyber-Anarchy?" Foreign Affairs, February 15, 2022.
https://www.foreignaffairs.com/articles/russian-federation/2021-12-14/end-cyber-anarchy.
[109] Bordelon, Emily B. 2016. "Approaching Cyber Warfare: Geopolitics, Deterrence, and International Law."; Nye, "The End of Cyber-Anarchy?".
[110] Carlin and Graff, *Dawn of the Code War,* 304; Spetalnick, Matt, and Michael Martina. 2015. "Obama Announces 'Understanding' with XI on Cyber Theft but Remains Wary." Reuters. Thomson Reuters. https://www.reuters.com/article/uk-usa-china-idAFKCN0RO2HZ20150926; Welsh, Teresa. 2015. "President Obama, Chinese President Xi Jingping Announce Agreement to ..." U.S. News. https://www.usnews.com/news/articles/2015/09/25/president-obama-chinese-president-xi-jingping-announce-agreement-to-stop-hacking.
[111] 2021. "Background Press Call on Improving Cybersecurity of U.S. Critical Infrastructure." The White House. The United States Government. https://www.whitehouse.gov/briefing-room/press-briefings/2021/07/28/background-press-call-on-improving-cybersecurity-of-u-s-critical-infrastructure/.
[112] Mussington, "Strategic Stability, Cyber Operations and International Security."; Perlroth, *This Is How They Tell Me*, 287.

across critical sectors. Unlike other threats to national security, cyberattacks can be launched by mysterious malicious state and non-state actors from within and beyond borders, who exploit cyberspace's anonymity.[113] The direct damage cyberattacks present serve as a catalyst for undermining public trust in government by introducing uncertainty into national cybersecurity. By increasing insecurity about their safety, cyberattacks make citizens question their government's approach to cyber and national security, and its general capabilities as a state. While this effect may be subtle, this doubt exacerbates an already tense political climate and a precarious point for American democracy.[114] Disregarding the importance of cybersecurity in cultivating American power is unwise; with increasing innovation in the technology sector, including the development of quantum computers and novel viruses, cyberspace will continue to rise as a field of economic, social, and political vitality.[115] Addressing the current challenges cyberattacks present to cybersecurity, trust, and democracy is necessary to reaping long-term state rewards in the form of robust American cyberspace stature, and a stronger, more developed, democracy.

Uncertainty is resolved with clarity. Cyberattacks may decrease trust in government by planting doubt about the government's ability to protect its people but open information sharing, collaboration with the private sector, legal reinforcement, and geopolitical actions against perpetrators could instead incite America's growth as a democratic, progressive nation. More challenges are sure to challenge the American government's strength and bond with its people in the future: today, the question is whether the government will be strong enough to rethink cyberspace's challenges, and rise to its opportunities or risk failure on all fronts.

[113] Mussington, "Strategic Stability, Cyber Operations and International Security."; Woodruff, and Brangham,"What Russia Stands…".
[114] The Harris Poll, "Colonial Pipeline Cyberattack Emphasizes What Research Finds."; Shandler, and Gomez, "The hidden threat of cyber-attacks...".
[115] Gordon and Rosenbach, "America's Cyber-Reckoning.".

Appendix One:

Gallup Analytics "Confidence in Institutions" Polls:

Gallup. "Confidence in Institutions." Gallup.com. Gallup, August 4, 2022. https://news.gallup.com/poll/1597/confidence-institutions.aspx.

Congress

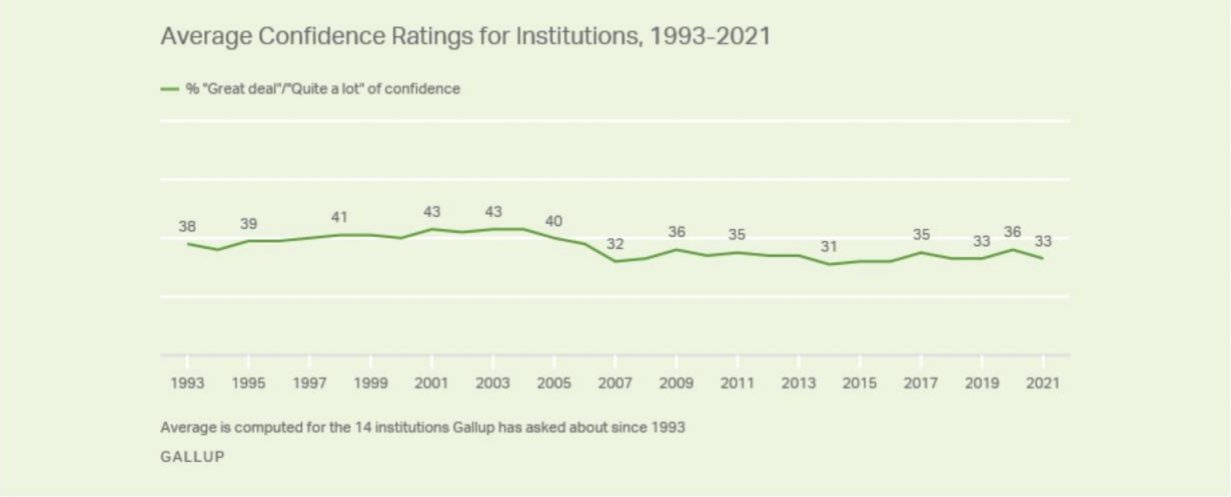
	Great deal	Quite a lot	Some	Very little	None (vol.)	No opinion	Great deal/Quite a lot
	%	%	%	%	%	%	%
2022	2	5	36	54	3	*	7
2021	5	7	37	47	4	*	12
2020	6	7	42	41	4	*	13
2019	4	7	36	48	4	1	11
2018	5	6	39	46	2	1	11
2017	6	6	39	44	3	1	12
2016	3	6	35	52	3	*	9
2015	4	4	37	48	5	1	8
2014	4	3	36	50	7	1	7
2013	5	5	37	47	5	1	10
2012	6	7	34	47	5	1	13
2011	6	6	40	44	4	1	12
2010	4	7	37	45	5	2	11
2009	6	11	45	34	4	1	17
2008	6	6	45	38	3	2	12
2007	4	10	46	36	3	1	14
2006	5	14	44	32	3	2	19
2005	8	14	51	25	1	1	22

The presidency

	Great deal	Quite a lot	Some	Very little	None (vol.)	No opinion	Great deal/Quite a lot
	%	%	%	%	%	%	%
2022	10	13	28	45	4	*	23
2021	16	22	29	29	4	1	38
2020	22	17	23	32	5	1	39
2019	24	14	17	38	6	1	38
2018	22	15	18	40	4	1	37
2017	19	13	20	42	5	1	32
2016	16	20	27	33	3	1	36
2015	16	17	27	35	5	1	33
2014	14	15	27	36	8	1	29
2013	19	17	27	30	5	1	36
2012	17	20	27	32	4	1	37
2011	15	20	28	32	4	1	35
2010	16	20	26	31	6	1	36
2009	26	25	24	19	4	1	51
2008	13	13	25	41	7	2	26
2007	12	13	28	39	7	1	25
2006	15	18	25	36	4	1	33
2005	21	23	27	25	3	1	44

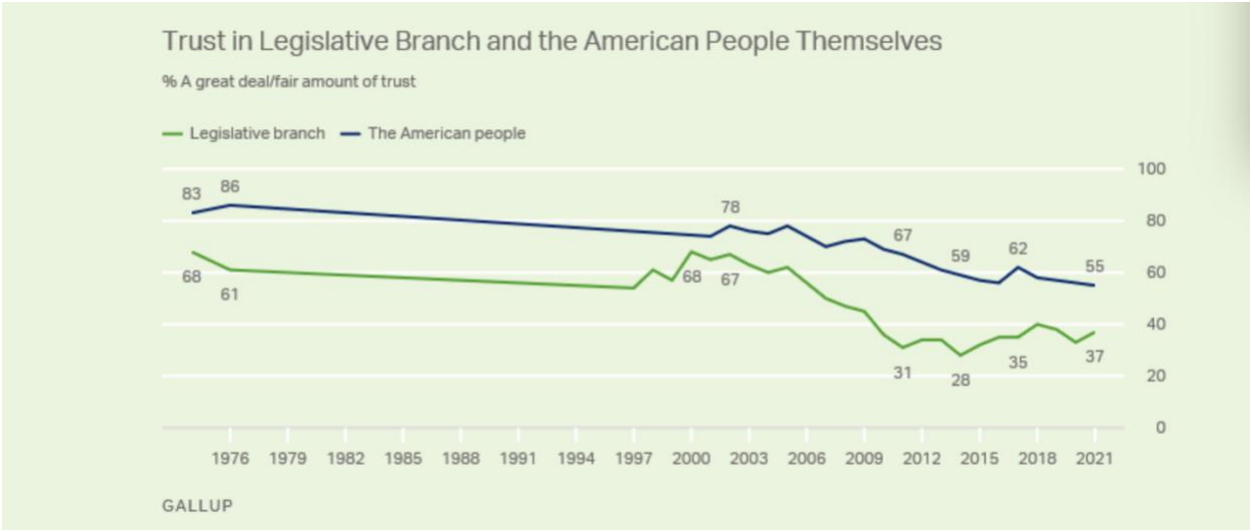
Gallup Analytics “Americans’ Confidence in Major US Institutions Dips” Polls:

Brenan, Megan. “Americans' Confidence in Major U.S. Institutions Dips.” Gallup.com. Gallup, November 20, 2021. https://news.gallup.com/poll/352316/americans-confidence-major-institutions-dips.aspx.



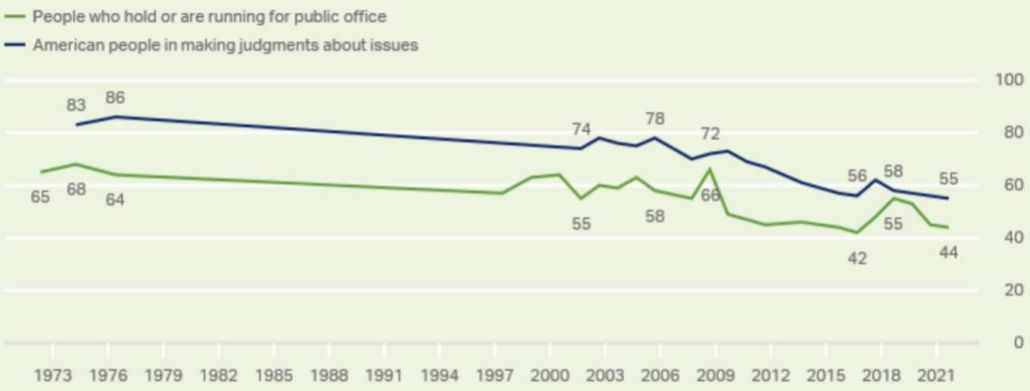
Gallup Analytics “Americans’ Trust Themselves” Polls:

Newport, Frank. “Americans' Trust in Themselves.” Gallup.com. Gallup, November 20, 2021. https://news.gallup.com/opinion/polling-matters/355553/americans-trust-themselves.aspx.



U.S. Adults' Trust in Politicians and the American People, 1972-2021

% A great deal/fair amount of trust



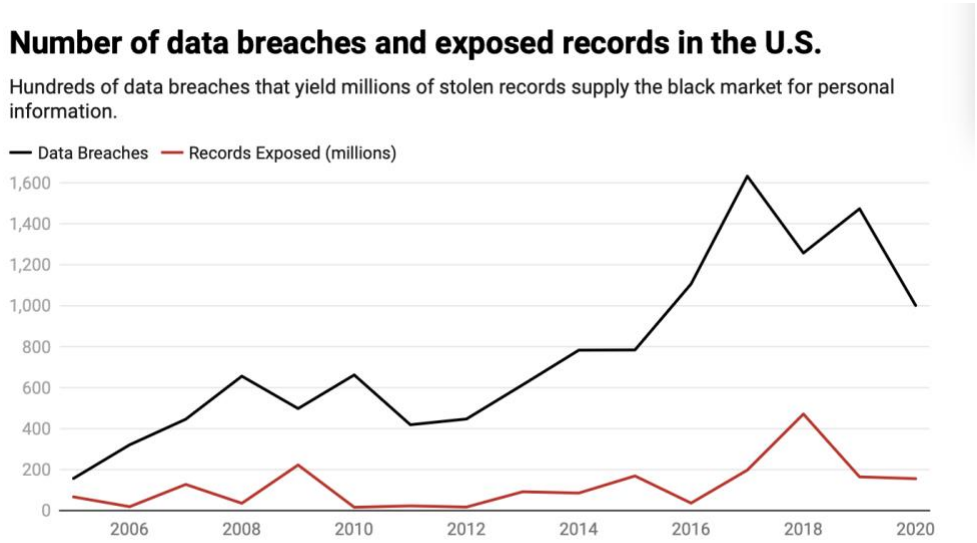
How much trust and confidence do you have in general in men and women in political life in this country who either hold or are running for public office -- a great deal, a fair amount, not very much or none at all?

More generally, how much trust and confidence do you have in the American people as a whole when it comes to making judgments under our democratic system about the issues facing our country -- a great deal, a fair amount, not very much or none at all?

GALLUP

Appendix Two:

Sen, Ravi. “Here's How Much Your Personal Information Is Worth to Cybercriminals – and What They Do with It.” PBS. Public Broadcasting Service, May 14, 2021. https://www.pbs.org/newshour/science/heres-how-much-your-personal-information-is-worth-to-cybercriminals-and-what-they-do-with-it.



	Walmart account with credit card attached	$10	$14
Payment Processing Services	Stolen PayPal account details, minimum $100	$199	$30
	PayPal transfer from stolen account, $1000 – $3000	$320	$340
	PayPal transfers from stolen account, $3000+	$156	$180
	Western Union transfer from stolen account, above $1000	$98	$45
Social Media	Hacked Facebook account	$75	$65
	Hacked Instagram account	$55	$45
	Hacked Twitter account	$49	$35
	Hacked Gmail account	$156	$80

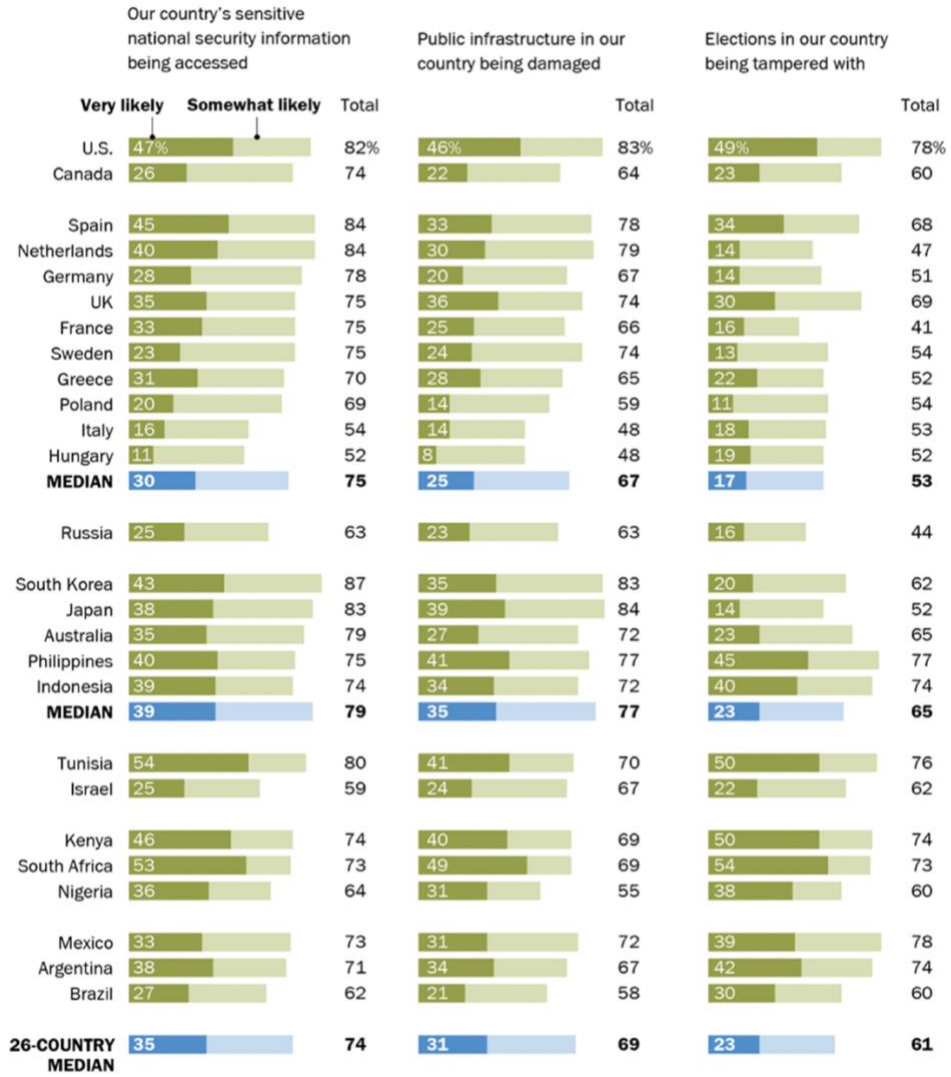
Table: The Conversation, CC-BY-ND • Source: PrivacyAffairs.com • Get the data

Appendix Three:

Poushter, Jacob, and Janell Fetterolf. 2020. "International Publics Brace for Cyberattacks on Elections, Infrastructure, National Security." Pew Research Center's Global Attitudes Project. Pew Research Center. https://www.pewresearch.org/global/2019/01/09/international-publics-brace-for-cyberattacks-on-elections-infrastructure-national-security/.

People around the world think cyberattacks on sensitive government data, public infrastructure and elections are likely in the future

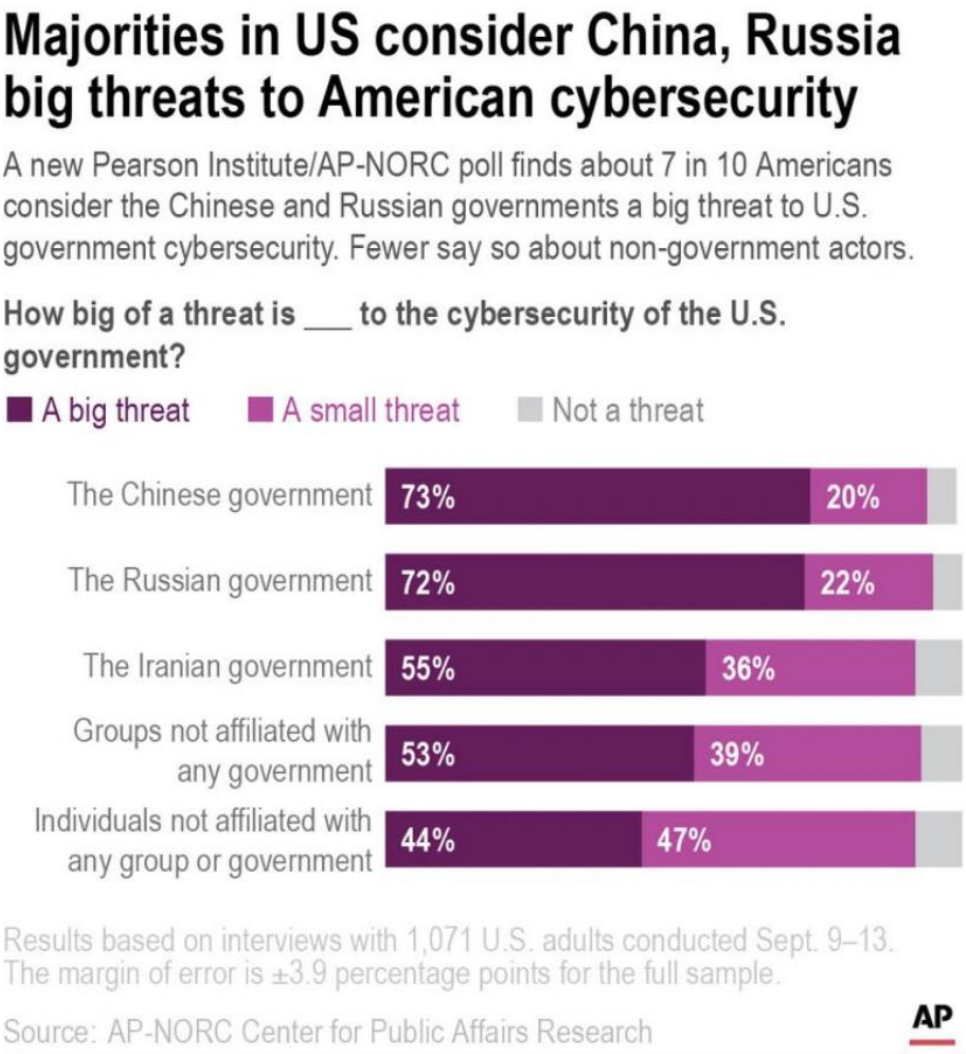
It is ___ that, in the future, a cyberattack will result in ...



Note: Total includes those who say a cyberattack is "very" or "somewhat" likely and those who volunteer such attacks have already happened.
Source: Spring 2018 Global Attitudes Survey. Q48a-c.

Appendix Four:

Suderman, Alan. 2021. "Cyberattacks Concerning to Most in US: Pearson/AP-Norc Poll." theintelligencer.net. The Intelligencer. https://www.theintelligencer.net/news/top-headlines/2021/10/cyberattacks-concerning-to-most-in-us-pearson-ap-norc-poll/.



Works Cited:

"2019 Cyberthreat Defense Report - Imperva." 2021. Imperva. https://www.imperva.com/resources/reports/CyberEdge-2019-CDR-Report-v1.1.pdf.

"Alert (AA20-352A): Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations." 2020. CISA. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/uscert/ncas/alerts/aa20-352a.

"Background Press Call on Improving Cybersecurity of U.S. Critical Infrastructure." 2021. The White House. The United States Government. https://www.whitehouse.gov/briefing-room/press-briefings/2021/07/28/background-press-call-on-improving-cybersecurity-of-u-s-critical-infrastructure/.

"Critical Infrastructure Partnerships and Information Sharing." 2022. Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/critical-infrastructure-partnerships-and-information-sharing.

"Executive Order on Improving the Nation's Cybersecurity." 2021. The White House. The United States Government. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

"JBS USA Cyberattack Media Statement." 2021. JBS Foods. https://jbsfoodsgroup.com/articles/jbs-usa-cyberattack-media-statement-june-9.

"Largest Meat Producer Getting Back Online after Cyberattack." 2021. PBS. Public Broadcasting Service. https://www.pbs.org/newshour/world/largest-meat-producer-getting-back-online-after-cyberattack.

"Meat Buyers Scramble after Cyberattack Hobbles JBS." 2021. The Wall Street Journal. Dow Jones & Company. https://www.wsj.com/articles/meatpacker-jbs-hit-by-cyberattack-affecting-north-american-australian-operations-11622548864.

"Meat Company JBS Foods Confirms It Paid US$11m Ransom in Cyberattack." 2021. Global News. Global News. https://globalnews.ca/news/7936930/jbs-foods-ransomware-attack-paid/.

"Media Statement: JBS USA Cybersecurity Attack." 2021. GlobeNewswire News Room. JBS USA, LLC. https://www.globenewswire.com/news-release/2021/05/31/2239049/17532/en/Media-Statement-JBS-USA-Cybersecurity-Attack.html.

"Remarks by President Biden on the Colonial Pipeline Incident." 2021. The White House. The United States Government. https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/05/13/remarks-by-president-biden-on-the-colonial-pipeline-incident/.

"Revil, a Notorious Ransomware Gang, Was behind JBS Cyberattack, the FBI Says." 2021. NPR. NPR. https://www.npr.org/2021/06/03/1002819883/revil-a-notorious-ransomware-gang-was-behind-jbs-cyberattack-the-fbi-says.

"Solarwinds Hack Was 'Largest and Most Sophisticated Attack' Ever: Microsoft President." 2021. Reuters. Thomson Reuters. https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AF03R.

"Solarwinds Hack: Russian Denial 'Unconvincing'." 2021. BBC News. BBC. https://www.bbc.com/news/technology-57156197.

"U.S. Says Ransomware Attack on Meatpacker JBS Likely from Russia; Cattle Slaughter Resuming." 2021. CNBC. CNBC. https://www.cnbc.com/2021/06/01/big-north-american-meat-plants-halt-operations-after-jbs-cyberattack.html.

"What Russia Stands to Gain from a Cyberattack against the U.S." 2020. PBS. Public Broadcasting Service. https://www.pbs.org/newshour/show/what-russia-stands-to-gain-from-a-cyberattack-against-the-u-s.

Alspach, Kyle. 2022."SEC Cyber Reporting Regs May Be Stuck. CISA Is Poised to Do Better." Protocol. Protocol. https://www.protocol.com/enterprise/sec-cisa-cyberattack-incident-reporting.

Andres, Richard B. 2019. "Cyber Conflict and Geopolitics." Great Decisions, 69–78. https://www.jstor.org/stable/26739054.

Aradau, Claudia, and Tobias Blanke. 2017. "Politics of Prediction: Security and the Time/space of Governmentality in the Age of Big Data." European Journal of Social Theory 20 (3): 373–91. https://doi.org/10.1177/1368431016667623.

Associated Press. 2021. "Largest Meat Producer Getting Back Online after Cyberattack." PBS. Public Broadcasting Service. https://www.pbs.org/newshour/world/largest-meat-producer-getting-back-online-after-cyberattack.

Baker, Pam. 2021. "The Solarwinds Hack Timeline: Who Knew What, and When?" CSO Online. CSO. https://www.csoonline.com/article/3613571/the-solarwinds-hack-timeline-who-knew-what-and-when.html.

Batista, Fabiana, Michael Hirtzer, and Mike Dorning. 2021. "JBS Cyber Hack: Meat Supplier Shuts down Some Slaughterhouses after Attack." Bloomberg.com. Bloomberg. https://www.bloomberg.com/news/articles/2021-05-31/meat-is-latest-cyber-victim-as-hackers-hit-top-supplier-jbs#xj4y7vzkg.

Biden, Joseph. 2021. "Executive Order on Improving the Nation's Cybersecurity." The White House. The United States Government, May 12, 2021.

https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

Bordelon, Emily B. 2016. “Approaching Cyber Warfare: Geopolitics, Deterrence, and International Law.”.

Bordoff, Jason. 2021. “The Colonial Pipeline Crisis Is a Taste of Things to Come.” Foreign Policy. https://foreignpolicy.com/2021/05/17/colonial-pipeline-crisis-cyberattack-ransomware-cybersecurity-energy-electicity-power-grid-russia-hackers/.

Bossetta, Michael. 2018. “THE WEAPONIZATION OF SOCIAL MEDIA: SPEAR PHISHING AND CYBERATTACKS ON DEMOCRACY.” *Journal of International Affairs* 71, no. 1.5: 97–106. https://www.jstor.org/stable/26508123.

Bouie, Jamelle, Jon Grinspan, Jill Lepore, and Yascha Mounk. 2022. “Renewing America Series: The History of American Democracy.” Council on Foreign Relations. Council on Foreign Relations. https://www.cfr.org/event/renewing-america-series-history-american-democracy.

Brenan, Megan. 2021. “Americans' Confidence in Major U.S. Institutions Dips.” Gallup.com. Gallup. https://news.gallup.com/poll/352316/americans-confidence-major-institutions-dips.aspx.

Breuninger, Kevin, and Amanda Macias. 2021. “Biden Signs Executive Order to Strengthen U.S. Cybersecurity Defenses after Colonial Pipeline Hack.” CNBC. CNBC. https://www.cnbc.com/2021/05/12/biden-signs-executive-order-to-strengthen-cybersecurity-after-colonial-pipeline-hack.html.

Burt, Andrew, and James C. Trainor. 2020. “The U.S. Needs a Standalone Agency to Fight Cyber Attacks.” Time. Time. https://time.com/5757811/cybersecurity-attacks-agency/.

Camp, Jean. 2022. “Does Biden's Cybersecurity Order Go Far Enough?” Brookings. Brookings. https://www.brookings.edu/blog/techtank/2022/06/24/does-bidens-cybersecurity-order-go-far-enough/.

Carley, Kathleen M. 2020. "Social Cybersecurity: An Emerging Science." *Computational and Mathematical Organization Theory* 26 (4) (12): 365-381. doi:https://doi.org/10.1007/s10588-020-09322-9. http://myaccess.library.utoronto.ca/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fscholarly-journals%2Fsocial-cybersecurity-emerging-science%2Fdocview%2F2473306603%2Fse-2.

Ceron, Andrea, Luigi Curini, and Stefano Maria Iacus. 2017. Politics and Big Data: Nowcasting and Forecasting Elections with Social Media. Abingdon, Oxon: Routledge. https://doi.org/10.4324/9781315582733.

Chappell, Bill, Greg Myre, and Laurel Wamsley. 2020. “What We Know about Russia's Alleged Hack of the U.S. Government and Tech Companies.” NPR. NPR. https://www.npr.org/2020/12/15/946776718/u-s-scrambles-to-understand-major-computer-hack-but-says-little.

Chaudhary, Tarun, Jenna Jordan, Michael Salomone, and Phil Baxter. 2018. “Patchwork of Confusion: The Cybersecurity Coordination Problem.” OUP Academic. Oxford University Press. https://academic.oup.com/cybersecurity/article/4/1/tyy005/5199384.

Cooley, Alexander, and Daniel H. Nexon. 2022. “How Hegemony Ends.” Foreign Affairs. https://www.foreignaffairs.com/articles/united-states/2020-06-09/how-hegemony-ends.

Cybersecurity & Infrastructure Security Agency. 2020. “Alert (AA20-352A).” CISA. https://www.cisa.gov/uscert/ncas/alerts/aa20-352a.

Dobrygowski, Daniel. 2019. “Why Companies Are Forming Cybersecurity Alliances.” Harvard Business Review. https://hbr.org/2019/09/why-companies-are-forming-cybersecurity-alliances.

Duffy, Clare. 2021. “Colonial Pipeline Attack: A 'Wake up Call' about the Threat of Ransomware.” CNN. Cable News Network. https://www.cnn.com/2021/05/16/tech/colonial-ransomware-darkside-what-to-know/index.html.

Forbes Editors. 2011. “JBS: The Story behind the World's Biggest Meat Producer.” Forbes. Forbes Magazine. https://www.forbes.com/sites/kerenblankfeld/2011/04/21/jbs-the-story-behind-the-worlds-biggest-meat-producer/?sh=449c9a297e82.

Fowler, Bree. 2022. “SolarWinds Hack Shows Government, Private Sector Need to Collaborate on Security, Cisa Head Says.” CNET. CNET. https://www.cnet.com/tech/services-and-software/solarwinds-hack-shows-government-private-sector-need-to-collaborate-on-security-cisa-head-says/.

Gallup. 2022. “Confidence in Institutions.” Gallup.com. Gallup. https://news.gallup.com/poll/1597/confidence-institutions.aspx.

Gordon, Sue, and Eric Rosenbach. 2022. “America's Cyber-Reckoning.” Foreign Affairs. https://www.foreignaffairs.com/articles/united-states/2021-12-14/americas-cyber-reckoning.

Gordon, Susan. 2022.“How the U.S. Can Be Better Prepared against Cybersecurity Threats.” NPR. NPR. https://www.npr.org/2022/01/01/1069672088/how-the-u-s-can-be-better-prepared-against-cybersecurity-threats.

Harkins, Ryan, and Erin English. 2022. “Guarding the Public Sector: Seven Ways State Governments Can Boost Their Cybersecurity.” Marsh McLennan.

https://www.marshmclennan.com/insights/publications/2018/oct/guarding-the-public-sector--seven-ways-state-governments-can-boo.html.

Jenkins, Lisa Martine. 2021. “Hackers, Consumers, Colonial Pipeline Deserve the Most Blame for U.S. Gas Shortages, Voters Say.” Morning Consult. https://morningconsult.com/2021/05/19/gasoline-shortage-polling/.

Jibilian, Isabella. 2021. “The US Is Readying Sanctions against Russia over the SolarWinds Cyber Attack. Here's a Simple Explanation of How the Massive Hack Happened and Why It's Such a Big Deal.” Business Insider. Business Insider. https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12.

Johnson, Kyle. 2021. “Should Companies Pay after Ransomware Attacks? Is It Illegal?” SearchSecurity. TechTarget. https://www.techtarget.com/searchsecurity/tip/Should-companies-pay-ransomware-and-is-it-illegal-to.

Jones, David. 2022. “How the Colonial Pipeline Attack Instilled Urgency in Cybersecurity.” Cybersecurity Dive. https://www.cybersecuritydive.com/news/post-colonial-pipeline-attack/623859/.

Joyce, Sean, Joseph Nocera, Matt Gorham, and Emily Stapf. 2022. “Cyber Breach Reporting to Be Required by Law for Better Cyber Defense.” PwC. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/cyber-breach-reporting-legislation.html.

Keen, David. 2011 'The Political Economy of War', in Frances Stewart, and Valpy Fitzgerald (eds), War and Underdevelopment: Volume 1: The Economic and Social Consequences of Conflict (Oxford, 2000; online edn, Oxford Academic), https://doi.org/10.1093/acprof:oso/9780199241866.003.0003, accessed 31 Aug. 2022.

Kerner, Sean Michael. 2022. “Colonial Pipeline Hack Explained: Everything You Need to Know.” WhatIs.com. TechTarget. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know.

Kiyan, Olga. 2021. “Establishing Cybersecurity Norms in the United Nations: The Role of U.s.-Russia Divergence.” Harvard International Review. Harvard International Review. https://hir.harvard.edu/establishing-cybersecurity-norms-in-the-united-nations-the-role-of-u-s-russia-divergence/.

Klimburg, Alexander. 2011. “Mobilising Cyber Power.” *Survival* 53, no. 1: 41–60. doi:10.1080/00396338.2011.555595.

Koziol, Jack. 2022. “Cybersecurity Awareness: What It Is and How to Start.” Forbes. Forbes Magazine. https://www.forbes.com/advisor/business/what-is-cybersecurity-awareness/.

Leal, Alejandro. 2022. “Public-Private Cooperation in Cyberspace.” KuppingerCole. https://www.kuppingercole.com/blog/leal/public-private-cooperation-in-cyberspace.

Leithauser, Tom. 2018. "Microsoft: Political Cyber Attacks Disrupted." *Cybersecurity Policy Report* (Aug 27): 1. http://myaccess.library.utoronto.ca/login?qurl=https%3A%2F%2Fwww.proquest.com%2Ftrade-journals%2Fmicrosoft-political-cyber-attacks-disrupted%2Fdocview%2F2108801781%2Fse-2%3Faccountid%3D14771.

Lostri, Euginia, James Andrew Lewis, and Georgia Wood. 2022. “A Shared Responsibility: Public-Private Cooperation for Cybersecurity.” A Shared Responsibility: Public-Private Cooperation for Cybersecurity | Center for Strategic and International Studies. https://www.csis.org/analysis/shared-responsibility-public-private-cooperation-cybersecurity.

Macias, Amanda. 2020. “White House Acknowledges Reports of Cyberattack on U.S. Treasury by Foreign Government.” CNBC. CNBC. https://www.cnbc.com/2020/12/13/cyber-hack-on-us-treasury-by-foreign-government-.html.

McLean, Rob, Alexis Benveniste, and Allie Malloy. 2021. “Major Meat Producer JBS USA Hit by Cyberattack, Likely from Russia.” CNN. Cable News Network. https://www.cnn.com/2021/06/01/tech/jbs-usa-cyberattack-meat-producer/index.html.

Miller, Maggie. 2021. “White House Says Cyberattack on Meat Producer JBS Likely from Russia.” The Hill. The Hill. https://thehill.com/policy/cybersecurity/556329-white-house-engaging-with-russian-government-to-respond-to-jbs/.

Morrison, Sara. 2021. “How a Major Oil Pipeline Got Held for Ransom.” Vox. Vox. https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices.

Morrison, Sara. 2021. “Ransomware Attack Hits Another Massive, Crucial Industry: Meat.” Vox. Vox. https://www.vox.com/recode/2021/6/1/22463179/jbs-foods-ransomware-attack-meat-hackers.

Musil, Steven. 2021.“Biden Signs Executive Order Aimed at Shoring up US Cybersecurity.” CNET. CNET. https://www.cnet.com/news/privacy/biden-signs-executive-order-aimed-at-shoring-up-us-cybersecurity/.

Mussington, David. 2019. “Strategic Stability, Cyber Operations and International Security.” Centre for International Governance Innovation. https://www.cigionline.org/articles/strategic-stability-cyber-operations-and-international-security/.

Naím, Moisés. 2017.“How Democracies Lose in Cyberwar.” The Atlantic. Atlantic Media Company, March 6, 2017.

https://www.theatlantic.com/international/archive/2017/02/democracy-cyber-war/516351/.

Nakashima, Ellen, and Craig Timberg. 2020. “Russian Government Hackers Are behind a Broad Espionage Campaign That Has Compromised U.S. Agencies, Including Treasury and Commerce.” The Washington Post. WP Company. 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.

Neuman, Scott, and Dustin Jones. 2021. “U.S. Slaps New Sanctions on Russia over Cyberattack, Election Meddling.” NPR. NPR. https://www.npr.org/2021/04/15/987585796/u-s-slaps-new-sanctions-on-russia-over-cyber-attack-election-meddling.

Newall, Mallory, and Johnny Sawyer. 2022. “A Majority of Americans Are Concerned about the Safety and ... - Ipsos,”. https://www.ipsos.com/en-us/news-polls/majority-americans-are-concerned-about-safety-and-privacy-their-personal-data.

Newport, Frank. 2021.“Americans' Trust in Themselves.” Gallup.com. Gallup. https://news.gallup.com/opinion/polling-matters/355553/americans-trust-themselves.aspx.

Nicholas, Paul. 2022. “Working to Preserve the Stability of Cyberspace.” The Diplomat, September 21, 2017. https://thediplomat.com/2017/09/working-to-preserve-the-stability-of-cyberspace/.

Nye, Joseph Jr. 2022. “The End of Cyber-Anarchy?” Foreign Affairs. https://www.foreignaffairs.com/articles/russian-federation/2021-12-14/end-cyber-anarchy.

Ordoñez, Franco. 2021. “In Wake of Pipeline Hack, Biden Signs Executive Order on Cybersecurity.” NPR. NPR. https://www.npr.org/2021/05/12/996355601/in-wake-of-pipeline-hack-biden-signs-executive-order-on-cybersecurity.

Paul, Kari, and Lois Beckett. 2020. “What We Know – and Still Don't – about the Worst-Ever US Government Cyber-Attack.” The Guardian. Guardian News and Media. https://www.theguardian.com/technology/2020/dec/18/orion-hack-solarwinds-explainer-us-government.

Perlroth, Nicole. 2021. This Is How They Tell Me the World Ends : the Cyberweapons Arms Race. New York: Bloomsbury Publishing.

Poushter, Jacob, and Janell Fetterolf. 2020.“International Publics Brace for Cyberattacks on Elections, Infrastructure, National Security.” Pew Research Center's Global Attitudes Project. Pew Research Center.

https://www.pewresearch.org/global/2019/01/09/international-publics-brace-for-cyberattacks-on-elections-infrastructure-national-security/.

Purdy, Andy. 2021. “Council Post: The US Needs a Stronger Commitment to Cybersecurity.” Forbes. Forbes Magazine. https://www.forbes.com/sites/forbestechcouncil/2021/07/30/the-us-needs-a-stronger-commitment-to-cybersecurity/?sh=3d5f69f95daf.

Rasmussen Polls. 2021. “Less than Half of U.S. Voters Confident Government Can Protect Pipelines.” Rasmussen Reports. https://www.rasmussenreports.com/public_content/politics/general_politics/may_2021/less_than_half_of_u_s_voters_confident_government_can_protect_pipelines.

Reeder, Joe, Paul McQuade, and Scott Schipma. 2021. “Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack: Insights: Greenberg Traurig LLP.” Insights | Greenberg Traurig LLP. https://www.gtlaw.com/en/insights/2021/8/published-articles/cybersecuritys-pearl-harbor-moment.

Reilly, Dan. 2021.“Cybersecurity Experts Say Public-Private Partnership Is the Key to Preventing Future Attacks.” Fortune. Fortune. https://fortune.com/2021/11/16/cybersecurity-future-government-corporation-partnership-data-breach/.

Rep. 2022 SonicWall Cyber Threat Report. SonicWall. https://www.sonicwall.com/medialibrary/en/white-paper/2022-sonicwall-cyber-threat-report.pdf.

Resnickault, Jessica, and Stephanie Kelly. 2021. “One Password Allowed Hackers to Disrupt Colonial Pipeline, CEO Tells Senators.” Reuters. Thomson Reuters. https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/.

Rid, Thomas. 2013. Cyber War Will Not Take Place. London: Hurst.

Riordan, Shaun. 2018. “The Geopolitics of Cyberspace: a Diplomatic Perspective.” Brill. Brill Research Perspectives in Diplomacy and Foreign Policy. https://www.researchgate.net/publication/334228866_The_Geopolitics_of_Cyberspace_a_Diplomatic_Perspective.

Rosenbaum, Eric. 2021. “JBS Cyberattack: From Gas to Meat, Hackers Are Hitting the Nation, and Consumers, Where It Hurts.” CNBC. CNBC. https://www.cnbc.com/2021/06/02/from-gas-to-burgers-hackers-hit-consumers-where-it-hurts.html.

Scheiber, Noam, Julie Creswell, and Nicole Perlroth. 2021. “Ransomware Disrupts Meat Plants in Latest Attack on Critical U.S. Business.” The New York Times. The New York Times. https://www.nytimes.com/2021/06/01/business/meat-plant-cyberattack-jbs.html%20%20June%201,%20updated%20June%203%202021.

Schwartz, Samantha. 2020. “Federal Agencies Fall Short on Cybersecurity, Undermining Standards.” Cybersecurity Dive. https://www.cybersecuritydive.com/news/solarwinds-cyberattack-treasury-financial-sector-security/592301/.

Sen, Ravi. 2021. “Here's How Much Your Personal Information Is Worth to Cybercriminals – and What They Do with It.” PBS. Public Broadcasting Service. https://www.pbs.org/newshour/science/heres-how-much-your-personal-information-is-worth-to-cybercriminals-and-what-they-do-with-it.

Sganga, Nicole. 2021. “JBS Paid $11 Million Ransom after Cyberattack.” CBS News. CBS Interactive, June 10, 2021. https://www.cbsnews.com/news/jbs-ransom-11-million/.

Shackelford, Scott J.,J.D.PhD., Angie Raymond J.D., Abbey Stemler J.D.M.B.A., and Cyanne Loyle PhD. 2020. "Defending Democracy: Taking Stock of the Global Fight Against Digital Repression, Disinformation, and Election Insecurity." *Washington and Lee Law Review* 77 (4) (Fall): 1747-1809. http://myaccess.library.utoronto.ca/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fscholarly-journals%2Fdefending-democracy-taking-stock-global-fight%2Fdocview%2F2501927603%2Fse-2%3Faccountid%3D14771.

Shandler, Ryan, and Miguel Alberto Gomez. 2022. The hidden threat of cyber-attacks – undermining public confidence in government, Journal of Information Technology & Politics, DOI: 10.1080/19331681.2022.2112796.

Sorvino, Chloe. 2022. “JBS Cyberattack Shines A Spotlight on the Biggest Risk to Big Meat: Consolidation.” Forbes. Forbes Magazine. https://www.forbes.com/sites/chloesorvino/2021/06/02/jbs-cyberattack-shines-a-spotlight-on-the-biggest-risk-to-big-meat-consolidation/?sh=27fca2661dbb.

Statista Research Department. 2022. “Number of Internet Users 2021.” Statista. https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/.

Suderman, Alan. 2021. “Cyberattacks Concerning to Most in US: Pearson/AP-Norc Poll.” theintelligencer.net. The Intelligencer. https://www.theintelligencer.net/news/top-headlines/2021/10/cyberattacks-concerning-to-most-in-us-pearson-ap-norc-poll/.

Susskind, Jamie. 2018. Future Politics : Living Together in a World Transformed by Tech. First edition. Oxford, United Kingdom: Oxford University Press.

Tarabay, Jamie. 2021. “Darkside, Revil Go Quiet after Colonial Pipeline, JBS Hacks.” Bloomberg.com. Bloomberg. https://www.bloomberg.com/news/newsletters/2021-06-28/darkside-revil-go-quiet-after-colonial-pipeline-jbs-hacks.

Temple-Raston, Dina. 2021. “A 'Worst Nightmare' Cyberattack: The Untold Story of the Solarwinds Hack.” NPR. NPR. https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

The Harris Poll. 2022. “Colonial Pipeline Cyberattack Emphasizes What Research Finds.” Tanium. https://www.tanium.com/blog/colonial-pipeline-cyberattack/.

Tsafos, Nikos, Lachlan Carey, Jane Nakano, and Sarah Ladislaw. 2021.“Cyber and Other Security Risks to the U.S. Electric Power Infrastructure.” Reshore, Reroute, Rebalance: A U.S. Strategy for Clean Energy Supply Chains. Center for Strategic and International Studies (CSIS). http://www.jstor.org/stable/resrep32324.6.

Turton, William, and Kartikay Mehrotra. 2021. “Colonial Pipeline Cyber Attack: Hackers Used Compromised Password.” Bloomberg.com. Bloomberg. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password#xj4y7vzkg.

U.S. Government Accountability Office. 2022. “Solarwinds Cyberattack Demands Significant Federal and Private-Sector Response (Infographic).” U.S. GAO. https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic.

Uzgalis, William. 2022. “John Locke.” Stanford Encyclopedia of Philosophy. Stanford University. https://plato.stanford.edu/entries/locke/.

Vavra, Shannon, and Tim Starks. 2020. “How the Russian Hacking Group Cozy Bear, Suspected in the Solarwinds Breach, Plays The Long Game.” CyberScoop. https://www.cyberscoop.com/cozy-bear-apt29-solarwinds-russia-persistent/.

Waldman, Arielle. 2022.“Enterprises Reluctant to Report Cyber Attacks to Authorities.” SearchSecurity. TechTarget. https://www.techtarget.com/searchsecurity/feature/Enterprises-reluctant-to-report-cyber-attacks-to-authorities.

Weinberg, Adam. 2021. “Analysis of Top 11 Cyber Attackson Critical Infrastructure.” FirstPoint. https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure/.

Whitaker, Bill. 2021. “Solarwinds: How Russian Spies Hacked the Justice, State, Treasury, Energy and Commerce Departments.” CBS News. CBS Interactive. https://www.cbsnews.com/news/solarwinds-hack-russia-cyberattack-60-minutes-2021-07-04/.

Whyte, Christopher. 2020. “Cyber conflict or democracy “hacked”? How cyber operations enhance information warfare.” *Journal of Cybersecurity*, Volume 6, Issue 1, tyaa013, https://doi.org/10.1093/cybsec/tyaa013.

Wilkie, Christina. 2021. “Colonial Pipeline Paid $5 Million Ransom One Day after Cyberattack, CEO Tells Senate.” CNBC. CNBC. https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html.

Woodruff, Judy, and William Brangham. 2020. “What Russia Stands to Gain from a Cyberattack against the U.S.” PBS. Public Broadcasting Service. https://www.pbs.org/newshour/show/what-russia-stands-to-gain-from-a-cyberattack-against-the-u-s.