CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

FEBRUARY 2024

Russia's Countervalue Cyber Approach: Utility or Futility?

Gavin Wilde

Introduction

In keeping with Moscow's extensive theorizing about information warfare, Russia's cyber aggression against Ukraine over the past decade has been overwhelmingly directed toward civilian infrastructure, aimed at demoralizing political leaders and eroding popular will. However, this countervalue approach—in contrast to a counterforce one that might have focused on Ukraine's military capability—has not only failed to achieve any discernible battlefield or political objectives, it has backfired. The net outcome of Russia's relentless cyber attacks appears to have been a digital rally-round-the-flag effect both within Ukraine and among its backers. This dynamic is not unique, however, to the cyber domain. Military scholars studying air campaigns against civilian infrastructure over previous wars might have predicted as much: bombarding adversary societies into submission has long proven a fruitless endeavor, though it nevertheless retains an allure for decisionmakers because of its relative ease.

For national security and military decisionmakers, these historical insights, Ukraine's experience since 2014, and America's gradual policy evolution all argue for increased emphasis on social adaptivity and civil resilience when considering countervalue cyber attacks. Framing such operations as normatively intolerable or somehow militarily deterrable adjuncts to conventional war—rather than as largely inevitable and recoverable outgrowths of an intelligence contest—may entail significant opportunity costs. Whether attempting or responding to countervalue cyber attacks, Russia's strategy and performance raise broader questions about the utility—or futility—of countervalue cyber operations in both war and geopolitics.

Civilian Resolve, a Familiar Target

In his 1996 book *Bombing to Win*, Robert Pape analyzed over thirty air campaigns over the previous decades' wars, concluding that coercion "hardly ever succeeds by raising costs and risks to civilians." The reason is that the bombardment of one's adversaries—be they British, German, Japanese, Vietnamese, or Iraqi—typically prompted more anger than fear, sparking a rally-round-the-flag effect for the besieged populace.[1] Jeffrey Whyte, a historian of psychological warfare, similarly recounts that so-called "morale bombing and its descendants rarely if ever produced the stated goal of weakening the resolve of enemy soldiers and civilians . . . inspir[ing] hate, not despair, in the hearts of its victims."[2]

These findings echo those of veteran U.S. air strategist Thomas Griffith, who reviewed bombing runs against electrical grids across the same wars and concluded that such attempts to erode civilian morale—and, by extension, to induce a political course-correction by the target state—were even *counterproductive* to the attacker's broader military and geopolitical objectives. In many instances, the logic of taking out civilian power supply tended to falsely mirror the ubiquity of electricity to daily life in the West.[3] Scholars have since added to the body of evidence discounting the efficacy of coercive air campaigns, particularly against civilian infrastructure.[4] These shortcomings notwithstanding, the strategy retains a persistent attractiveness for military and political leaders, which Pape attributes to "bureaucratic interests and political pressures for cheap solutions to difficult foreign policy problems."[5]

These insights seem eerily prescient in the context of a current-day campaign of coercion, albeit in an entirely different domain. Russia's long-running cyber aggression against Ukraine has been driven by the same logic: target civilian infrastructure to grind down popular and political will. Moscow has for nearly a decade pummeled its neighbor with disruptive cyber attacks and information operations, only to find Pape's truism holds firm: coercion is, indeed, hard.[6] What it could not achieve through subversion, Moscow would later attempt through brute force in February 2022. Despite some apparent attempts to coordinate cyber attacks with its kinetic military strikes during the ensuing full-scale war, Russia's cyber performance confounded prevailing Western expectations, proving both underwhelming and non-decisive.[7] The reasons for this failure likely include Moscow's choice of targets.

The Presumption of Societal Frailty

In the 1960s, nuclear theorists in the United States debated whether to target the Soviet Union's military forces, weapons systems, and command infrastructure—so-called *counterforce* targets—or to train fire on the apparent sources of Soviet national power—so-called *countervalue* targets. These included civilian power generation and transmission, supply chains for consumer goods, financial services, and communications networks. In theory, counterforce operations diminish an adversary's military capacity to wage war, while countervalue operations erode political and popular will. Cyber scholars would later describe how states and militaries pursue such strategies in cyberspace;[8] in the case of Ukraine, Russian operators appear to have opted for a countervalue one—likely as much by design as of necessity.[9]

While Russia appears to have attempted counterforce cyber attacks in the early days of the war—disrupting the Viasat satellite communications network, likely in hopes of impeding Ukrainian military communications[10]—a recent report from Ukraine's own State Service of Special Communications and Information Protection found that as the war unfolded, Russian cyber attacks were directed less often toward military targets and instead were trained on public services and energy utilities.[11] Studies from the CyberPeace Institute, the Amsterdam Law School, and the Center for Strategic and International Studies likewise indicate that the overwhelming majority of Russian cyber attacks during the war have been directed against civilian targets and government services, with few discernible links to the Ukrainian armed forces.[12] John Hultquist, vice president of threat intelligence at cybersecurity firm Mandiant, noted that these attacks appeared designed to "strike fear into every Ukrainian and really just up the psychological toll."[13]

This strategy is consistent with Moscow's long-standing views about information's supposed coercive potential.[14] For instance, current members of the Russian General

Staff have long claimed that cyber and information warfare must be designed not only to neutralize enemy military networks, but also to degrade the adversary's morale, cultural values, and very way of life.[15] Most notably, Chief Valery Gerasimov claimed in 2014 that information and communication technologies had altered the very nature of war, prompting states to try using them to diminish each other's potential "through destruction of vitally important military *and civilian* infrastructure" (emphasis added). He went on to assert that information warfare could erode popular will, insofar as it enabled "remote, covert influence not only on critical information infrastructure, but also on the country's population, directly affecting the state's national security" by disorienting them and sparking mass panic.[16] Rattled by the prospect that social movements and popular unrest taking place elsewhere in the world might threaten regime stability in Moscow, the Kremlin thus turned "information war" into both a convenient scapegoat and a political imperative.[17]

Instead, the net effect of so much Russian aggression in the digital domain—consistent with the previous findings of air warfare theorists—was to steel Ukrainian resolve and further galvanize a historic outpouring of Western technological and cyber assistance to Kyiv.[18] Remarkably, despite the onslaught, Ukraine over the past decade has become a burgeoning tech hub and a model of digital connectivity, e-governance, and cyber resilience—successes arguably necessitated and thus accelerated by Russia's unrelenting cyber aggression.[19] In this regard, Ukraine's experience echoes that of Estonia, which, since being bombarded with cyber attacks in 2007, has become a model of digitization and a hub for international cybersecurity collaboration.[20] However costly and disruptive it has been to the victims, Moscow's countervalue cyber strategy, as part of a broader geopolitical project to re-subordinate its neighbors, has failed miserably.

Meanwhile, the operative assumption in Russia's countervalue approach—that such attacks necessarily undermine the targeted public's trust in its own government—may itself be fatally flawed. Recent surveys in the United States, the United Kingdom, and Israel found that (contrary to common punditry) countervalue cyber attacks did not undermine voters' trust in the state's ability to protect them and uniformly provoked more anger than anxiety. Moreover, such attacks may become *less* alarming as they become more frequent, reaching a "threshold of normalcy," or occur within the context of a more lethal conflict.[21] Indeed, in Ukraine's case, after tens of thousands of casualties, brutalized and displaced civilian populations, and decimated cities, it is difficult to imagine any cyber effects that would come close to rivaling such traumas.[22] Even so, such effects "potentially amount to war crimes" according to the International Criminal Court—which is now poised to review and prosecute cyber attacks that target civilians in violation of international law.[23]

Russian cyber operators in the military, intelligence, and security services are doubtlessly continuing to evolve and develop their arsenals—with both civilian and military targets in mind.[24] However, as scholars Erica Lonergan (née Borghard) and Shawn Lonergan have written, "once the theory of coercion meets the reality of cyber operations, many attractive targets may become too costly and out of reach . . . . Therefore, governments are more likely to pursue coercive strategies that allow for a wide variety of targets that are more easily accessible . . . inflict[ing] costs against vulnerable public and private interests."[25] As Ukraine's experience with cyber bombardment dictates—alongside the experience of the victims of air bombardments before it—such costs are often bearable to victims and fruitless to the attacker.[26] This dynamic also stems from adaptation by the targets of Russia's disruptive cyber operations themselves.[27]

From Deterrence to Resilience

Like Ukraine since 2014, the United States since 2016 has matured, in terms both of discourse and of policy on cyber issues—from hyper-focus on the threat of disruptions to acceptance of their ever-presence in an increasingly digitized world and, by extension, an emphasis on building resilience toward them. Initial strategies aimed at preventing or avoiding breaches altogether have gradually evolved to recognize that shared responsibility, a recalibrated trust relationship toward technology and networks, and security by design are more realistic aspirations.[28] With the benefit of nearly three decades of assessing and responding to the Kremlin's unique, coercive approach—including what little strategic value it appears to have yielded for Moscow—Western leaders can similarly right-size Russia's cyber threat in both their own and public perceptions.

From a military perspective, this starts by better distinguishing (and communicating) which Russian cyber activities are highly undesirable—but ultimately inevitable—and which are truly intolerable.[29] In this regard, a countervalue versus counterforce framing can set more realistic expectations about which cyber harms might reasonably be curbed or responded to by military means and which will demand more of homeland security and law enforcement agencies, private industry, civil society, and citizens themselves.[30] This also means more conscientiously categorizing observed Russian cyber behaviors, ranging from those that enable espionage to those designed for independent disruption or attack—including as part of conventional armed conflict.[31] While it is often difficult for states to distinguish among these categories, this ambiguity often leads national security leaders to adopt a starting assumption of worst-case scenarios about cyber intrusions (for instance, "cyber Pearl Harbor"), informed less by robust forensic and risk analysis than by speculative anxieties or cybersecurity industry marketing.[32] Where it so often fuels reflexive militarization, such ambiguity should instead galvanize a higher baseline of cyber-focused civil defense, diplomacy, and statecraft.[33]

This will also mean reexamining which norms do (and might) prevail in cyberspace, and prioritizing policy responses along that rubric.[34] For instance, states can, do, and will spy on each other. They will attempt to subvert each other's interests through covert means. They are unlikely to be dissuaded from doing so by the prospect of punishment. In cyberspace, this is an inevitable operational reality that has yet to be fully accepted as a political one. A range of recent scholarship therefore recommends reconceptualizing cyber operations more as part of an intelligence contest than as a means or method of war.[35] Under this framing, decisionmakers should perceive countervalue cyber operations not as a transgression of emerging norms of geopolitical conflict, but as rigid adherence to long-standing norms of interstate espionage—including informal "codes of honor among spies, and their bosses."[36] In this regard, policy responses drawn from the military tool kit—particularly concepts like deterrence—are destined to fall short.[37] Such failures might needlessly undermine public confidence and risk casting the United States as hypocritical as it pursues its own robust intelligence-gathering mission abroad.[38] As former U.S. director of national intelligence James Clapper once said, "[Like] people who live in glass houses, we should think before we throw rocks."[39]

Moreover, in an era where "persistent engagement"—a theory of constant, proactive contact with adversaries in cyberspace[40]—is to be a centerpiece of the Pentagon's own cyber strategy, it can also help decisionmakers more critically grapple with the question of efficacy.[41] Foremost: Do countervalue cyber operations—those aimed at eroding adversary morale, resolve, or societal cohesion—stem from any reasonable expectation of impact? Or, as in air bombardments from previous conflicts, are countervalue targets simply more abundant and accessible relative to counterforce ones? Would an offensive cyber operation be, as Griffith described, "undertaken more out of knowledge about the supply of power" than because of any insight about the effects of knocking it out?[42] In this same vein, Russian military intelligence (the GRU) apparently jeopardized its own long-running digital penetration into the networks of Ukraine's largest mobile service provider, Kyivstar, in favor of a cyber attack that knocked service offline in late 2023. The impact appears to have been largely symbolic, however—the company restored service within a matter of days.[43] Whether the attack contributed anything concrete to the Kremlin's war effort—beyond addressing the GRU's need to be seen "doing something" in support of it—is unclear.[44]

Cause for Introspection

This in no way minimizes the risk of Russian cyber espionage and subversion, nor discounts the prospect that it may pivot toward counterforce operations on the battlefield or improve upon countervalue ones against publics. However, Russia's performance in Ukraine does raise broader questions for military and cyber strategists: Is there any degree of success in countervalue cyber operations sufficient to compensate for counterforce failures? Were Russia's operational shortcomings in Ukraine situationally unique or more broadly indicative of an upper limit of utility for countervalue cyber operations in war and geopolitics?[45] Like all cyber-related questions, a host of unknown variables demands humility in answering them. The true extent of cyber operations in this war is likely known only to Ukrainian and Russian commanders. Even so, for militaries, there is at least a plausible case to be made that countervalue cyber operations—whether conducting or responding to them—entail significant opportunity costs that might drain resources and focus better concentrated elsewhere.

Cyber scholar Martin C. Libicki notes that the efficacy of cyberattacks is "strongly, perhaps overwhelmingly, determined by features of those systems [they] are targeted against."[46] For hardened battlefield systems, this logic is readily apparent. It is what makes a successful counterforce cyber operation—like electronically disabling an air defense system to enable a successful bombing run against a military target—such a daunting challenge.[47] Insofar as sociopolitical cohesion can also be considered such a system, civil adaptability and resilience are more likely to be decisive in blunting countervalue operations than is commonly appreciated. Rather than posing what Erica Lonergan calls "unpalatable choices between capitulation and escalation" in response to any Russian cyber operations whatsoever, a resilience-based approach "obviates that need by anticipating that setbacks will be part of the strategic environment and, therefore, preparing in advance to address them."[48]

Russia's countervalue cyber operations—however disruptive and costly—can reasonably be seen as Moscow's cheap solution to its mounting foreign policy problems, a sign of highly sophisticated intelligence tradecraft being squandered in service of a deeply flawed military strategy. Meanwhile, the historical rubble from air bombardments, the rugged determination of Ukrainian society today, and the gradual evolution of American thinking about cybersecurity all seem to call for more faith and focus in domestic and civil resilience and less fear and fixation on Russia's putative cyber prowess.

About the Author

Gavin Wilde is a senior fellow in the Technology and International Affairs Program at the Carnegie Endowment for International Peace, where he applies his expertise on Russia and information warfare to examine the strategic challenges posed by cyber and influence operations, propaganda, and emerging technologies.

Notes

[1] Robert A. Pape, “Beyond Strategic Bombing,” in *Bombing to Win*, 1st ed., Air Power and Coercion in War (Cornell University Press, 1996), 314–331.

[2] Jeffrey Whyte, *The Birth of Psychological War: Propaganda, Espionage, and Military Violence from WWII to the Vietnam War*, British Academy Monographs (Oxford, UK: Oxford University Press, 2023), 7.

[3] Thomas E. Griffith, “Strategic Attack of National Electrical System” (thesis, School of Advanced Airpower Studies, Maxwell Air Force Base, October 1994), v, 46, 50, https://media.defense.gov/2017/Dec/29/2001861964/-1/-1/0/T_GRIFFITH_STRATEGIC_ATTACK.PDF.

[4] Abigail Post, “Flying to Fail: Costly Signals and Air Power in Crisis Bargaining,” *Journal of Conflict Resolution* 63, no. 4 (April 1, 2019): 869–895, https://doi.org/10.1177/0022002718777043; and Susan Hannah Allen and Carla Martinez Machain, “Understanding the Impact of Air Power,” *Conflict Management and Peace Science* 36, no. 5 (September 1, 2019): 545–558, https://doi.org/10.1177/0738894216682485.

[5] Pape, *Bombing to Win*, 314, 326–327. Also see Stephanie Carvin, “How Not to War,” *International Affairs* 98, no. 5 (September 6, 2022): 1695–1716, https://doi.org/10.1093/ia/iiac189.

[6] The term “cyber attack” herein refers to offensive cyber operations specifically intended to disrupt, destroy, or manipulate data or communications channels. These are often designed by militaries to have their own distinct effects—independent from, in support of, or in lieu of kinetic (or physical) ones. They are not to be conflated with cyber-enabled espionage or intelligence-gathering, surveillance, and reconnaissance.

[7] Jon Bateman, “Russia’s Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications,” Carnegie Endowment for International Peace, December 16, 2022, https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657.

[8] Max Smeets, “The Strategic Promise of Offensive Cyber Operations,” *Strategic Studies Quarterly* 12, no. 3 (2018): 90–113; Erica D. Borghard and Shawn W. Lonergan, “The Logic of Coercion in Cyberspace,” *Security Studies* 26, no. 3 (July 3, 2017): 452–481, https://doi.org/10.1080/09636412.2017.1306396; Austin Long, “A Cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning,” *Journal of Cybersecurity* 3, no. 1 (March 1, 2017): 19–28, https://doi.org/10.1093/cybsec/tyw016; and Henry Farrell and Charles L. Glaser, “The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine,” *Journal of Cybersecurity* 3, no. 1 (March 1, 2017): 7–17, https://doi.org/10.1093/cybsec/tyw015.

[9] Gavin Wilde, “Cyber Operations in Ukraine: Russia’s Unmet Expectations,” Carnegie Endowment for International Peace, December 12, 2022, https://carnegieendowment.org/2022/12/12/cyber-operations-in-ukraine-russia-s-unmet-expectations-pub-88607.

[10] Kim Zetter, “Viasat Hack ‘Did Not’ Have Huge Impact on Ukrainian Military Communications, Official Says,” Zero Day, September 26, 2022, https://www.zetter-zeroday.com/p/viasat-hack-did-not-have-huge-impact.

[11] “Russia’s Cyber Tactics: Lessons Learned in 2022,” State Service of Special Communications and Information Protection of Ukraine, March 8, 2023, https://cip.gov.ua/en/news/russia-s-cyber-tactics-lessons-learned-in-2022-ssscip-analytical-report-on-the-year-of-russia-s-full-scale-cyberwar-against-ukraine.

[12] “Cyber Attacks in Times of Conflict,” CyberPeace Institute, October 30, 2023, https://cyberconflicts.cyberpeaceinstitute.org; Grace B. Mueller et al., “Cyber Operations During the Russo-Ukrainian War,” Center for Strategic and International Studies, July 13, 2023, https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war; and Peter B. M. J. Pijpers, “Revisiting the Stability/Instability Paradox in Cyberspace: Lessons From the Russo-Ukraine War,” Amsterdam Law School Research Paper no. 2023-28, July 19, 2023, https://doi.org/10.2139/ssrn.4514908.

[13] Maggie Miller, “Russia’s Cyberattacks Aim to ‘Terrorize’ Ukrainians,” Politico, January 11, 2023, https://www.politico.com/news/2023/01/11/russias-cyberattacks-aim-to-terrorize-ukrainians-00077561.

[14] Tim Stevens, “Information Matters: Informational Conflict and the New Materialism,” *SSRN Electronic Journal*, 2012, https://doi.org/10.2139/ssrn.2146565; and Keir Giles and Anthony Seaboyer, “The Russian Information Warfare Construct,” Defense Research and Development Canada, March 2019, https://cradpdf.drdc-rddc.gc.ca/PDFS/unc341/p811007_A1b.pdf.

[15] Antti Vasara, “Theory of Reflexive Control: Origins, Evolution, and Application in the Framework of Contemporary Russian Military Strategy,” Finnish National Defence University, 2020, 68–70.

[16] Timothy Thomas, “Russian Military Thought: Concepts and Elements,” MITRE Corporation, August 2019, 188.

[17] Justin Sherman and Gavin Wilde, “No Water’s Edge: Russia’s Information War and Regime Security,” Carnegie Endowment for International Peace, January 4, 2023, https://carnegieendowment.org/2023/01/04/no-water-s-edge-russia-s-information-war-and-regime-security-pub-88644.

[18] Nick Beecroft, “Evaluating the International Support to Ukrainian Cyber Defense,” Carnegie Endowment for International Peace, November 3, 2022, https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322; and Dan Black, “Russia’s War in Ukraine: Examining the Success of Ukrainian Cyber Defences,” International Institute for Strategic Studies, March 2023, https://www.iiss.org/en/research-paper/2023/03/russias-war-in-ukraine-examining-the-success-of-ukrainian-cyber-defences/.

[19] Eric Rosenbaum, “Eastern Europe Created Its Own Silicon Valley. Russia’s Invasion of Ukraine Risks It All,” CNBC, March 5, 2022, https://www.cnbc.com/2022/03/05/the-eastern-european-silicon-valley-boom-in-the-middle-of-russias-war.html; Gavin Wilde and Arthur Nelson, “How Cyber Support

to Ukraine Can Build Its Democratic Future,” CyberScoop, April 18, 2023, https://cyberscoop.com/ukraine-cyber-aid-russia-war; and “International Security and Estonia 2023,” Estonian Foreign Intelligence Service, January 31, 2023, https://raport.valisluureamet.ee/2023/en/.

[20] Esther Naylor, “Estonia’s Crucial Role in Tackling Growing Cyber Threats,” Chatham House, June 22, 2020, https://www.chathamhouse.org/2020/06/estonias-crucial-role-tackling-growing-cyber-threats.

[21] Sharon Matzkin, Ryan Shandler, and Daphna Canetti, “The Limits of Cyberattacks in Eroding Political Trust: A Tripartite Survey Experiment,” *British Journal of Politics and International Relations*, November 16, 2023, https://doi.org/10.1177/13691481231210383.

[22] Bateman, ““Russia’s Wartime Cyber Operations in Ukraine.”

[23] Andy Greenberg, “The International Criminal Court Will Now Prosecute Cyberwar Crimes,” *Wired*, September 7, 2023, https://www.wired.com/story/icc-cyberwar-crimes; and Lindsay Freeman, “Ukraine Symposium – Accountability for Cyber War Crimes,” Lieber Institute, April 14, 2023, https://lieber.westpoint.edu/accountability-cyber-war-crimes.

[24] Margarita Konaev and Owen J. Daniels, “The Russians Are Getting Better,” *Foreign Affairs*, September 6, 2023, https://www.foreignaffairs.com/ukraine/russians-are-getting-better-learning.

[25] Borghard and Lonergan, “The Logic of Coercion in Cyberspace,” 480.

[26] This does not discount cyber coercion as a tool of statecraft in peacetime contexts, nor in service of more circumscribed political goals. For instance, as part of a broader political pressure campaign, recent Iranian cyber attacks—against primarily governmental targets in Albania—appear to have played at least some role in softening Tirana’s support for an exiled Iranian opposition group operating from Albanian territory. See “Will Iran Succeed in Dismantling Its Most Organized Exiled Opposition?” Amwaj Media, December 13, 2023, https://amwaj.media/media-monitor/will-iran-succeed-in-dismantling-most-organized-exiled-opposition.

[27] Miguel Alberto Gomez and Christopher Whyte, “Breaking the Myth of Cyber Doom: Securitization and Normalization of Novel Threats,” *International Studies Quarterly* 65, no. 4 (December 17, 2021): 1137–1150, https://doi.org/10.1093/isq/sqab034; and Lars Gjesvik and Kacper Szulecki, “Interpreting Cyber-Energy-Security Events: Experts, Social Imaginaries, and Policy Discourses Around the 2016 Ukraine Blackout,” *European Security* 32, no. 1 (January 2, 2023): 104–124, https://doi.org/10.1080/09662839.2022.2082838.

[28] “National Cybersecurity Strategy,” White House, March 1, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf; “Zero Trust Maturity Model,” Cybersecurity and Infrastructure Security Agency, April 2023, https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf; “Secure By Design: Shifting the Balance of Cybersecurity Risk,” Cybersecurity and Infrastructure Security Agency, October 2023, https://www.cisa.gov/sites/default/files/2023-10/SecureByDesign_1025_508c.pdf; and “US Cyberspace Solarium Report 2.0,” U.S. Cyberspace Solarium Commission, March 11, 2020, 31–110, https://cybersolarium.org/march-2020-csc-report/march-2020-csc-report.

[29] Lester Godefrey, “Shape or Deter? Managing Cyber-Espionage Threats to National Security Interests,” *Studies in Intelligence* 66, no. 1 (March 2022): 1–10.

[30] Jason Healey, “The Cyber Budget Shows What the U.S. Values—and It Isn’t Defense,” Lawfare, June 1, 2020, https://www.lawfaremedia.org/article/cyber-budget-shows-what-us-values—and-it-isnt-defense.

[31] Martin C. Libicki, “Drawing Inferences from Cyber Espionage,” in *2018 10th International Conference on Cyber Conflict (CyCon)*, IEEE, 2018, 109–122, https://doi.org/10.23919/CYCON.2018.8405013; Thomas Rid and Peter McBurney, “Cyber-Weapons,” *RUSI Journal* 157, no. 1 (February 1, 2012): 6–13, https://doi.org/10.1080/03071847.2012.664354; Gary Brown, “Spying and Fighting in Cyberspace: What Is Which?,” *Journal of National Security Law & Policy* 8, no. 621 (October 2017): 626–627; and Andru E. Wall, “Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action, ” *Harvard National Security Journal* 3, no. 1 (December 2, 2011): https://harvardnsj.org/wp-content/uploads/2012/01/Vol-3-Wall.pdf.

[32] Myriam Dunn Cavelty, “The Militarisation of Cyberspace: Why Less May Be Better,” in *2018 10th International Conference on Cyber Conflict (CyCon)*, IEEE, 2012, 141–153, https://ccdcoe.org/uploads/2012/01/2_6_Dunn-Cavelty_TheMilitarisationOfCyberspace.pdf.

[33] Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (Oxford University Press, 2017), 185; and Michael Garcia, “The Militarization of Cyberspace? Cyber-Related Provisions in the National Defense Authorization Act, ” Third Way, April 5, 2021, https://www.thirdway.org/memo/the-militarization-of-cyberspace-cyber-related-provisions-in-the-national-defense-authorization-act.

[34] Erica D. Lonergan and Jacquelyn Schneider, “The Power of Beliefs in US Cyber Strategy: The Evolving Role of Deterrence, Norms, and Escalation,” *Journal of Cybersecurity* 9, no. 1 (January 1, 2023): https://doi.org/10.1093/cybsec/tyad006.

[35] Godefrey, “Shape or Deter?”; Robert Chesney and Max Smeets, *Deter, Disrupt, or Deceive: Assessing Cyber Conflict as an Intelligence Contest* (Georgetown University Press, 2023).

[36] Robert Chesney, “Sanctioning Russia for SolarWinds: What Normative Line Did Russia Cross?,” Lawfare, April 15, 2021, https://www.lawfaremedia.org/article/sanctioning-russia-solarwinds-what-normative-line-did-russia-cross; and Perri Adams et al., “Responsible Cyber Offense,” Lawfare, August 2, 2021, https://www.lawfaremedia.org/article/responsible-cyber-offense.

[37] Brad D. Williams, “Nakasone: Cold War-Style Deterrence ‘Does Not Comport to Cyberspace,’” Breaking Defense , November 4, 2021, https://breakingdefense.com/2021/11/nakasone-cold-war-style-deterrence-does-not-comport-to-cyberspace.

[38] Julian E. Barnes and Edward Wong, "In Risky Hunt for Secrets, U.S. and China Expand Global Spy Operations," *New York Times*, September 17, 2023, https://www.nytimes.com/2023/09/17/us/politics/us-china-global-spy-operations.html.

[39] Sydney J. Freedberg Jr., "DNI, NSA Seek Offensive Cyber Clarity; OPM Not An 'Attack,'" Breaking Defense, September 10, 2015, https://breakingdefense.sites.breakingmedia.com/2015/09/clapper-rogers-seek-cyber-clarity-opm-not-an-attack.

[40] Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, "Persistent Engagement in Cyberspace Is a Strategic Imperative," *National Interest*, July 6, 2022, https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/persistent-engagement-cyberspace.

[41] "DOD Releases 2023 Cyber Strategy Summary," U.S. Department of Defense, September 12, 2023, https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF.

[42] Griffith, "Strategic Attack of National Electrical System," 46. Also see James R. Cody, "AWPD-42 to Instant Thunder: Consistent Evolutionary Thought, or Revolutionary Change?" (thesis, School of Advanced Airpower Studies, Maxwell Air Force Base, June 1996), 7–8, https://apps.dtic.mil/sti/tr/pdf/ADA424862.pdf.

[43] Martin Fornusek, "Kyivstar Restores Mobile Internet Following Cyberattack," *Kyiv Independent*, December 15, 2023, https://kyivindependent.com/kyivstar-restores-mobile-internet-following-hack.

[44] Mike Martin, "Fear Russian Nukes, Not Cyberwarriors," UnHerd, October 27, 2020, https://unherd.com/2020/10/russias-cyberwar-is-the-least-of-our-worries.

[45] Lennart Maschmeyer, "A New and Better Quiet Option? Strategies of Subversion and Cyber Conflict," *Journal of Strategic Studies* (July 27, 2022): 1–25, https://doi.org/10.1080/01402390.2022.2104253.

[46] Martin C. Libicki, "Cyberwar as a Confidence Game," *Strategic Studies Quarterly* 5, no. 1 (Spring 2011): 132–147.

[47] "Operation Orchard/Outside the Box (2007)," International Cyber Law: Interactive Toolkit, September 17, 2021, https://cyberlaw.ccdcoe.org/wiki/Operation_Orchard/Outside_the_Box_(2007); Daniel Moore, *Offensive Cyber Operations: Understanding Intangible Warfare* (Oxford, New York: Oxford University Press, 2022); and Nadiya Kostyuk and Yuri M. Zhukov, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?," *Journal of Conflict Resolution* 63, no. 2 (February 1, 2019): 317–347, https://doi.org/10.1177/0022002717737138.

[48] Erica Lonergan, "A Grand Strategy Based on Resilience," War on the Rocks, January 4, 2021, https://warontherocks.com/2021/01/a-grand-strategy-based-on-resilience. See also Keir Giles, "Russian Cyber and Information Warfare in Practice: Lessons Observed From the War on Ukraine," Chatham House, December 14, 2023, 49–50, https://www.chathamhouse.org/sites/default/files/2023-12/2023-12-14-russian-cyber-info-warfare-giles.pdf.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

Carnegie does not take institutional positions on public policy issues; the views represented herein are those of the author(s) and do not necessarily reflect the views of Carnegie, its staff, or its trustees.