The Subversive Trilemma

Why Cyber Operations Fall Short of Expectations

Lennart Maschmeyer

For three decades, states have engaged in cyber conflict, yet the strategic utility of cyber operations remains unclear. Strategic utility refers to measurable contributions toward a state's political goals or shifts in the balance of power.[1] Similar to the 1920s–1940s air power debates, scholars have expected new technology to revolutionize conflict and provide independent utility.[2] When warplanes first emerged, some experts predicted the end of conventional warfare because airplanes were able "to strike mortal blows to the heart of the enemy at lightning speed."[3] Similarly, when the World Wide Web gained popularity in the 1990s, some analysts predicted a future of cyberwar in which "neither mass nor mobility but information" would become decisive.[4] Subsequent theorizing envisioned strategic cyber strikes similar to strategic aerial attacks, shaping fears of a "cyber Pearl Harbor."[5] There is, however, a key difference between the two.

Lennart Maschmeyer is a senior researcher at the Center for Security Studies at ETH Zürich.

The author thanks Ronald Deibert, Jesse Driscoll, Nadiya Kostyuk, Gabrielle Lim, Jon Lindsay, Louis Pauly, Irene Poetranto, Max Smeets, Lucan Way, the team at the Citizen Lab at the University of Toronto, the team at the Center for Security Studies at ETH Zürich (especially Alexander Bollfrass, Myriam Dunn Cavelty, Mauro Gilli, Enzo Nussio, and Andreas Wenger), as well as the anonymous reviewers for their helpful comments on earlier drafts of this article. He is also grateful to Lesia Bidochko, Daria Goriacheva, Oksana Grechko, and Mariya Green for research assistance. The author is also indebted to Olga Paschuk for her interpretation services in Ukraine. Finally, the author thanks Lisa Maschmeyer for designing figure 1. The online appendix for this article is available at doi.org/10.7910/DVN/IZ65MC.

1. Robert A. Pape, *Bombing to Win: Air Power and Coercion in War* (New York: Cornell University Press, 1996), p. 57.
2. See, for example, Winn Schwartau, *Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age*, 2nd ed. (New York: Thunder's Mouth, 1996); Dima Adamsky and Kjell Inge Bjerga, "Introduction to the Information-Technology Revolution in Military Affairs," *Journal of Strategic Studies*, Vol. 33, No. 4 (2010), pp. 463–468, doi.org/10.1080/01402390.2010.489700; Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security*, Vol. 38, No. 2 (Fall 2013), pp. 7–40, doi.org/10.1162/ISEC_a_00138; and Jacquelyn Schneider, "The Capability/Vulnerability Paradox and Military Revolutions: Implications for Computing, Cyber, and the Onset of War," *Journal of Strategic Studies*, Vol. 42, No. 6 (2019), pp. 841–863, doi.org/10.1080/01402390.2019.1627209.
3. Giulio Douhet, *The Command of the Air*, trans. Dino Ferrari (Washington, D.C.: Office of Air Force History, 1983), p. 15.
4. John Arquilla and David Ronfeldt, "Cyberwar Is Coming!" *Comparative Strategy*, Vol. 12, No. 2 (1993), pp. 141–165, doi.org/10.1080/01495939308402915.
5. James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival*, Vol. 53, No. 1 (2011), pp. 23–40, doi.org/10.1080/00396338.2011.555586; Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: HarperCollins, 2010); and James J. Wirtz, "The Cyber Pearl Harbor," in Emily O. Goldman and John Arquilla, eds., *Cyber Analogies* (Monterey, Calif.: Naval Postgraduate School, 2014).

International Security, Vol. 46, No. 2 (Fall 2021), pp. 51–90, https://doi.org/10.1162/isec_a_00418

World War II demonstrated the terribly destructive capacity of aerial bombing, confirming its combat effectiveness (or the capacity to destroy target sets).[6] Consequently, scholarly debate has primarily examined "whether the destruction of target sets attains political goals."[7] In contrast, "cyber wars" remain hypothetical, the combat effectiveness of cyber operations remains unproven, and scholars increasingly question their utility in warfare.[8]

Instead, a new "cyber revolutionary" school of thought asserts that information technology revolutionizes conflict short of war by increasing the effectiveness of nonmilitary instruments. Lucas Kello argues that "the virtual weapon is expanding the range of possible harm and outcomes between the concepts of war and peace," creating a novel strategic state of "unpeace."[9] Despite its different focus, this new revolutionary thesis rests on remarkably similar assumptions about the operational effectiveness of cyber operations as the cyberwar theories that preceded it. Operational effectiveness concerns the capacity to produce desired effects against a target set. As I will show, cyberwar and cyber revolution scholars expect three key properties of information technologies to provide superior operational effectiveness: the speed of communication, the global scope and scale of computer networks, and the ease of online anonymity.[10] Information technology has produced significant economic efficiencies, and revolutionary scholars expect comparable gains in effectiveness by employing the technology in conflict. A key instrument of utilizing information technology in security competition is cyber operations, which I define as the exploitation of vulnerabilities in information and communications technologies (ICTs) to produce desired outcomes against adversaries.[11] Because the revolutionary thesis posits that information technology increases effectiveness, its adherents expect cyber operations to expand the independent strategic utility of instruments short of war. As Richard Harknett and Max

6. Pape, *Bombing to Win*, p. 56.
7. Ibid., p. 57. See also Phil Haun, "Foundation Bias: The Impact of the Air Corps Tactical School on United States Air Force Doctrine," *Journal of Military History*, Vol. 85, No. 2 (April 2021), pp. 453–474.
8. Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security*, Vol. 38, No. 2 (Fall 2013), pp. 41–73, doi.org/10.1162/ISEC_a_00136; Thomas Rid, *Cyber War Will Not Take Place* (New York: Oxford University Press, 2013); Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (New York: Oxford University Press, 2015); Jon R. Lindsay, "Restrained by Design: The Political Economy of Cybersecurity," *Digital Policy, Regulation, and Governance*, Vol. 19, No. 6 (2017), pp. 493–514, doi.org/10.1108/DPRG-05-2017-0023; and Erica D. Borghard and Shawn W. Lonergan, "Cyber Operations as Imperfect Tools of Escalation," *Strategic Studies Quarterly*, Vol. 13, No. 3 (Fall 2019), pp. 122–145, https://www.jstor.org/stable/26760131.
9. Lucas Kello, *The Virtual Weapon and International Order* (New Haven, Conn.: Yale University Press, 2017), pp. 75–78.
10. I discuss these assumptions and their origins in detail in this article.
11. Exploitation enables both passive information collection and active effects. This study focuses on active effects (i.e., manipulation, disruption, or damage of targeted computer systems).

Smeets conclude, "cyber operations and campaigns can be pivotal in world affairs by independently . . . supporting the maintenance or alteration of the balance of power . . . without having to resort to military violence."[12] Just as cyberwars failed to manifest in practice, however, empirical evidence for this cyber revolution remains scarce. On the contrary, a growing body of research shows how cyber operations seem to fall short of their promise, both in warfare and conflict short of war.[13]

I argue that the reason for this shortfall lies at the operational level of conflict, whereby actors deploy combinations of tactics to attain strategic goals.[14] Stephen Biddle has shown how operational mechanisms are crucial for determining the strategic utility of new technologies in conventional war, and I contend the same applies to cyber conflict.[15] Prevailing expectations tend to focus on the strategic promise of new technology, but they overlook the operational mechanisms required to fulfil it. In this article, I show that the mismatch between promise and practice is the consequence of the subversive nature of cyber operations, whose operational trilemma limits strategic utility. Cyber operations produce outcomes by exploiting vulnerabilities in computer systems and the way they are embedded in modern societies.[16] This mechanism is commonly known as hacking.[17] Hacking may appear to be a novel instrument, yet its primary reliance on exploitation reveals its parallels to subversion.[18]

Subversion is an understudied instrument of power used in nonmilitary covert operations. Consequently, the field of international relations lacks a theory

12. Richard J. Harknett and Max Smeets, "Cyber Campaigns and Strategic Outcomes," *Journal of Strategic Studies* (2020), p. 24, doi.org/10.1080/01402390.2020.1732354.
13. Erica D. Borghard and Shawn W. Lonergan, "Cyber Operations as Imperfect Tools of Escalation," *Strategic Studies Quarterly*, Vol. 13, No. 3, (Fall 2019), pp. 122–145, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-13_Issue-3/Borghard.pdf; Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies*, Vol. 22, No. 3 (2013), pp. 365–404, doi.org/10.1080/09636412.2013.816122; Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Vienna, Va.: Cyber Conflict Studies Association, 2013); and Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security*, Vol. 41, No. 3 (Winter 2016/17), pp. 72–109, doi.org/10.1162/ISEC_a_00267.
14. Edward N. Luttwak, "The Operational Level of War," *International Security*, Vol. 5, No. 3 (Winter 1980/81), p. 61, doi.org/10.2307/2538420.
15. Stephen Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton, N.J.: Princeton University Press, 2010).
16. Jon Erickson, *Hacking: The Art of Exploitation* (San Francisco, Calif.: No Starch, 2003), pp. 115–116.
17. Franklin Kramer notes that "cyber attacks—hacking of various kinds—are a fact of modern life." Kramer, "Cyberpower and National Security: Policy Recommendations for a Strategic Framework," in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, eds., *Cyberpower and National Security* (Washington, D.C.: Potomac, 2009), p. 15. See also Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge, Mass.: Harvard University Press, 2020), p. 3; and David J. Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power* (Abingdon, UK: Routledge, 2011), pp. 26–31.
18. Buchanan, *The Hacker and the State*.

of subversion. Building on existing work in intelligence studies, this article develops such a theory and shows why cyber operations rely on subversion. It demonstrates that the defining characteristic of subversion is its reliance on the secret exploitation of vulnerabilities in a system of rules. Accordingly, I define subversion as exploiting vulnerabilities to secretly infiltrate a system of rules and practices in order to control, manipulate, and use the system to produce detrimental effects against an adversary. In traditional subversion, states target social systems. Typically, states have used undercover spies to infiltrate groups and institutions, establish influence within the latter, and then use this influence to produce desired outcomes against an adversary.[19] Although cyber operations target a different kind of system, I show that the mechanism of exploitation has the same subversive characteristics.

Subversion's reliance on exploitation distinguishes it from warfare and diplomacy, the two classic instruments of power in security competition. Subversion holds great strategic promise because of two key properties of exploitation: its secrecy and indirect reliance on adversary systems. Secrecy can be either covert (the identity of the actor is obscured) or clandestine (the activity itself is obscured).[20] Existing research identifies two strategic benefits of secrecy: it lowers states' escalation risks and reputation costs for intervening in the affairs of their adversaries.[21] The indirect nature of exploitation also lowers resource costs compared to the use of force. It is indirect because subversive actors produce effects through exploited systems. Subversion leverages an adversary's own capabilities against its own systems to produce effects. These effects range from influencing government policies and public opinion to degrading material capabilities through sabotage to undermining institutional efficiency and effectiveness.[22] In short, subversion promises a less expensive and less risky alternative to warfare that states can use to actively interfere in

19. Paul W. Blackstock, *The Strategy of Subversion: Manipulating the Politics of Other Nations* (Chicago: Quadrangle, 1964); and Lawrence W. Beilenson, *Power through Subversion* (Washington, D.C.: Public Affairs, 1972).

20. Michael E. DeVine, *Covert Action and Clandestine Activities of the Intelligence Community: Selected Definitions in Brief* (Washington, D.C.: Congressional Research Service, June 14, 2019).

21. Austin Carson, *Secret Wars: Covert Conflict in International Politics* (Princeton, N.J.: Princeton University Press, 2018); and Michael Poznansky, "Feigning Compliance: Covert Action and International Law," *International Studies Quarterly*, Vol. 63, No. 1 (March 2019), pp. 72–84, doi.org/10.1093/isq/sqy054.

22. Howard L. Douthit III, "The Use and Effectiveness of Sabotage as a Means of Unconventional Warfare: An Historical Perspective from World War I through Vietnam," master's thesis, Air Force Institute of Technology, January 21, 1988, https://apps.dtic.mil/sti/pdfs/ADA188034.pdf; Beilenson, *Power through Subversion*, p. 80; Eckard Michels, *Guillaume, der spion: Eine deutsch-deutsche karriere* [Giullaume, the spy: A German career] (Berlin: Links Christoph Verlag, 2013); and Christopher Andrew and Vasili Mitrokhin, *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB* (New York: Basic Books, 1999), pp. 364, 473.

their adversaries' affairs and attempt to shift the balance of power when diplomacy falls short. Cyber operations share this promise. Because various social, political, and physical processes are increasingly computerized, subverting these computer systems can produce a range of physical, political, and economic effects. Cyber revolutionary theory accordingly expects cyber operations to offer a low-risk and low-cost, yet highly effective, instrument for conducting sabotage, political interference, and economic disruption.

Yet, I identify an operational trilemma that tends to prevent subversion from fulfilling this promise, and this article shows why cyber operations also face this trilemma. The same characteristics that enable the promise of subversion (i.e., its secret and indirect nature) require significant efforts to establish and maintain. These efforts constrain operational effectiveness across three key variables. First, they slow operational speed, defined as the time required from starting an operation until it produces effects. Second, they constrain the intensity of effects, determined by both scope and scale. Scope concerns the severity of effects against individual targets, and scale comprises the number of targets affected and thus the scale of societal impact.[23] Third, efforts to maintain secrecy and exploit systems limit control, defined as the extent of control over a targeted system, and over the effects produced through this system.

These constraints pose a trilemma for actors because the three variables (i.e., speed, intensity of effects, and control) are negatively correlated—a gain in one variable tends to produce losses across the other two variables. For example, the higher the operational speed, the less intensity and control actors tend to achieve. As mentioned, the revolutionary thesis expects information technology to enable high-speed cyber operations with large-scale effects under a mantle of secrecy. In practice, however, the trilemma prevents actors from achieving these properties all at once. Consequently, in most circumstances cyber operations fall short of their strategic promise and provide, at best, limited strategic utility.

I test this theory through an in-depth case study of the ongoing Russo-Ukrainian conflict. This protracted conflict started in 2013, and it includes five major disruptive cyber operations that attempted election interference, sabotage, and economic dislocation. As a paradigmatic example of cyber-enabled low-intensity conflict involving one of the world's leading cyber powers, Russia, against a much weaker adversary, one would most expect to observe the utility of cyber operations. With its long duration and multiple cyber operations in a real-world "test lab" of cyber conflict, the constraints of the

23. This definition builds on Herman Kahn's definition of conflict intensity. Kahn, *On Escalation: Metaphors and Scenarios* (Westport, Conn.: Greenwood, 1986 [1965]).

trilemma are least likely to apply.[24] Consequently, the Russo-Ukrainian conflict is a crucial case.[25] I introduce and use a systematic framework to measure operational effectiveness across the variables of speed, intensity, and control, and I triangulate strategic utility. The case study leverages rich original data from field interviews with experts in Ukraine, leaked Russian documents and emails, and forensic reports. Evidence from these sources supports my theory that the subversive trilemma constrains operational effectiveness and limits strategic utility.

This article makes three main contributions. First, it furthers the current debate in cybersecurity between cyber revolutionaries and an emerging rival thesis of "cyber evolution," whose proponents point out the general strategic continuity between cyber conflict and intelligence contests.[26] The theory of the subversive trilemma clarifies what types of intelligence operations cyber operations reproduce, and how operational constraints limit their strategic utility. Second, the theory contributes to security studies by clarifying the strategic role of cyber operations as instruments of subversion that promise an effective alternative to force yet offer limited utility in practice. The theory of subversion also contributes to international relations, which has neglected the topic. Third, the article adds rich empirical evidence on the mechanisms, constraints, and utility of cyber operations that will be useful for both cybersecurity and international security scholars.

The argument proceeds as follows. First, I outline how expectations about the strategic utility of cyber operations have evolved. Second, I develop the theory of subversion from which I derive a set of expectations and hypotheses. This section also specifies the research design and empirical strategy. Third, I present the case study, which examines the operational effectiveness and strategic utility of cyber operations in the Russo-Ukrainian conflict. I conclude with a discussion of alternate explanations and potential limitations of the study before laying out the implications for international security.

24. Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar," *Wired*, June 20, 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/.
25. A "crucial case" is one "in which a theory that passes empirical testing is strongly supported and one that fails is strongly impugned." Alexander L. George and Andrew Bennett, *Case Studies and Theory Development in the Social Sciences* (Cambridge: Massachusetts Institute of Technology Press, 2005), p. 9.
26. Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies*, Vol. 24, No. 2 (2015), pp. 316–348, doi.org/10.1080/09636412.2015.1038188; Aaron Franklin Brantly, *The Decision to Attack: Military and Intelligence Cyber Decision-Making* (Athens: University of Georgia Press, 2016), pp. 43–62, http://muse.jhu.edu/book/45365; and Joshua Rovner, "Cyber War as an Intelligence Contest," *War on the Rocks* blog, September 16, 2019, https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/.

Existing Literature on the Strategic Utility of Cyber Operations

Cybersecurity scholars' expectations concerning the strategic utility of cyber operations have shifted from warfare to conflict short of war. Initial research expected cyber operations to provide independent utility in warfare, enabling strategic cyber strikes and offering an offensive advantage.[27] Such cyberwar theorizing rested on three assumptions about the effectiveness of cyber operations: information technology enabled unrivaled operational speed compared to conventional warfare,[28] while the Internet's design facilitates anonymity[29] and its global scale allows actors to disrupt or damage targets at massive scale.[30] Accordingly, other scholars assumed that the same three properties also offered strategic utility as complements to the use of force.[31] But scenarios of cyberwar and escalation did not manifest in practice. Instead, the intensity of cyber conflict has remained below the threshold of war.[32]

Cyber revolution theory proposes, accordingly, that cyber operations offer

27. Arquilla and Ronfeldt, "Cyberwar Is Coming!"; Kramer, "Cyberpower and National Security"; Clarke and Knake, *Cyber War*; William J. Lynn III, "Defending a New Domain," *Foreign Affairs*, September/October 2010, https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain; Joseph S. Nye Jr., "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly*, Vol. 5, No. 4 (Winter 2011), pp. 18–38, https://www.jstor.org/stable/26270536; and Wirtz, "The Cyber Pearl Harbor."

28. Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in Kramer, Starr, and Wentz, eds., *Cyberpower and National Security*, p. 28; Nye, "Nuclear Lessons for Cyber Security?" p. 18; Lynn, "Defending a New Domain"; James C. Mulvenon and Gregory J. Rattray, eds., *Addressing Cyber Instability* (Vienna, Va.: Cyber Conflict Studies Association, August 2012), p. 23; Jacquelyn Schneider, "Cyber and Crisis Escalation: Insights from Wargaming," United States Naval War College, 2017, p. 1, https://paxsims.files.wordpress.com/2017/01/paper-cyber-and-crisis-escalation-insights-from-wargaming-schneider.pdf; and Clarke and Knake, *Cyber War*, p. 34.

29. Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, Calif.: RAND, 2009), p. 43; Gregory J. Rattray, "An Environmental Approach to Understanding Cyberpower," in Kramer, Starr, and Wentz, eds., *Cyberpower and National Security*, p. 272; Lynn, "Defending a New Domain"; Joseph S. Nye Jr., *Cyber Power* (Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010), p. 6, https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf; Chris C. Demchak and Peter Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly*, Vol. 5, No. 1 (Spring 2011), pp. 32–61, https://www.jstor.org/stable/26270509; and Farwell and Rohozinski, "Stuxnet and the Future of Cyber War," p. 35.

30. Rattray, "An Environmental Approach to Understanding Cyberpower," pp. 266–268; Lynn, "Defending a New Domain," p. 1; Nye, "Nuclear Lessons for Cyber Security?" p. 21; and Peter Dombrowski and Chris C. Demchak, "Cyber War, Cybered Conflict, and the Maritime Domain," *Naval War College Review*, Vol. 67, No. 2 (Spring 2014), p. 73, https://www.jstor.org/stable/26397758.

31. Libicki, *Cyberdeterrence and Cyberwar*, p. 139; Max Smeets, "The Strategic Promise of Offensive Cyber Operations," *Strategic Studies Quarterly*, Vol. 12, No. 3 (Fall 2018), pp. 90–113, https://www.jstor.org/stable/26481911; and Jon R. Lindsay and Erik Gartzke, "Coercion through Cyberspace: The Stability-Instability Paradox Revisited," in Kelly M. Greenhill and Peter Krause, eds., *Coercion: The Power to Hurt in International Politics* (New York: Oxford University Press, 2018).

32. Valeriano and Maness, *Cyber War versus Cyber Realities*.

states a newly effective instrument in competition short of war, revolutionizing the way states compete.[33] Although they consider different types of conflict, revolutionary scholars and cyberwar theorists base their arguments on remarkably similar assumptions. Cyber revolution scholars emphasize how information technologies increase the speed,[34] scale,[35] and relative ease of anonymity[36] of instruments short of war, enhancing their effectiveness and elevating their strategic utility. In particular, Michael Fischerkeller and Richard Harknett suggest that technological change has expanded the scope and scale of intelligence operations to such an extent that it constitutes a "difference in kind" in strategic utility,[37] while Michael Warner suggests that information technology may have "fixed covert action's problem of scale."[38] Ben Buchanan goes as far as proclaiming the advent of a "new form of statecraft," whereby "one of the primary ways governments shape geopolitics is by hacking other countries."[39] The underlying assumptions about the strategic promise of information technology continue to be widely shared yet rarely tested empirically. Moreover, the scarce empirical work on key cases indicates the limited effectiveness and utility of cyber operations.[40]

A rival set of scholars argues that cyber operations are merely an evolution of covert operations.[41] While this perspective specifies the larger strategic space (i.e., intelligence contests), it still lacks a theory about the operational mechanisms and strategic utility of cyber operations. Intelligence operations encompass a broad range of activities, from passive information collection to active interference,[42] and cyber operations cannot likely reproduce all of them equally well. As Loch Johnson has shown, covert operations have been de-

33. Kello, *The Virtual Weapon and International Order*; Michael Warner, "A Matter of Trust: Covert Action Reconsidered," *Studies in Intelligence*, Vol. 63, No. 4 (December 2019), pp. 33–41, https://www.cia.gov/static/d61827122b5a1b8023e0f11678c2edce/Covert-Action-Reconsidered.pdf; Buchanan, *The Hacker and the State*; Harknett and Smeets, "Cyber Campaigns and Strategic Outcomes"; and Michael P. Fischerkeller and Richard J. Harknett, *Cyber Persistence Theory, Intelligence Contests, and Strategic Competition* (Alexandria, Va.: Institute for Defense Analyses, June 2020), https://apps.dtic.mil/sti/pdfs/AD1118679.pdf.
34. Kello, *The Virtual Weapon and International Order*, p. 2; and Harknett and Smeets, "Cyber Campaigns and Strategic Outcomes," p. 9.
35. Warner, "A Matter of Trust," p. 38; and Buchanan, *The Hacker and the State*, p. 290.
36. Buchanan, *The Hacker and the State*, p. 1; Kello, *The Virtual Weapon and International Order*, p. 154; and Harknett and Smeets, "Cyber Campaigns and Strategic Outcomes," p. 24.
37. Fischerkeller and Harknett, *Cyber Persistence Theory, Intelligence Contests, and Strategic Competition*, p. 10.
38. Warner, "A Matter of Trust," p. 38.
39. Buchanan, *The Hacker and the State*, p. 7.
40. Lindsay, "Stuxnet and the Limits of Cyber Warfare"; and Slayton, "What Is the Cyber Offense-Defense Balance?"
41. Gartzke and Lindsay, "Weaving Tangled Webs"; Rovner, "Cyber War as an Intelligence Contest"; and Brantly, *The Decision to Attack*.
42. Michael Warner, "Wanted: A Definition of 'Intelligence'," *Studies in Intelligence*, Vol. 46,

ployed to produce a wide range of effects, from influencing public opinion to sabotage to full-blown secret wars.[43] Importantly, evolution theory does not clarify which of these effects cyber operations can and cannot produce, and thus their strategic utility remains unclear. Current scholarship on covert operations focuses primarily on military operations.[44] Yet, the premise of the current shift in scholarly attention toward conflict short of war is the emerging consensus that cyber operations are relatively ineffective and irrelevant in warfare.[45] Hence, cyber operations are not likely to be useful substitutes for military covert operations. Rather, as the next section shows, cyber operations are nonmilitary instruments of subversion.

Why Cyber Operations are Subversive

In this section, I develop the theory of subversion. I show how both subversion and cyber operations rely on secret exploitation and face an operational trilemma that limits their strategic promise. There is no general theory about subversion, and the scholarly work on the topic is scarce. Existing studies either tie their definition of subversion to a specific goal, the overthrow of governments from within,[46] or they examine its use in specific contexts, such as using nonstate proxies to undermine state authority[47] or great power competition.[48] But Cold War scholar Paul Blackstock identified a common operational mechanism used in subversive operations regardless of specific goals or context that offers a foundation for a general theory: the secret exploitation of political or social vulnerabilities.[49] While Cold War subversion primarily targeted entire political systems, any system of rules and practices is potentially vulner-

No. 3 (2002), https://www.cia.gov/resources/csi/studies-in-intelligence/volume-46-no-3/wanted-a-definition-of-intelligence/.

43. Loch K. Johnson, "On Drawing a Bright Line for Covert Operations," *American Journal of International Law*, Vol. 86, No. 2 (April 1992), pp. 284–309, doi.org/10.2307/2203235.

44. Austin Carson, "Facing Off and Saving Face: Covert Intervention and Escalation Management in the Korean War," *International Organization*, Vol. 70, No. 1 (Winter 2016), pp. 103–131, doi.org/10.1017/S0020818315000284; Poznansky, "Feigning Compliance"; and Rory Cormac and Richard J. Aldrich, "Grey Is the New Black: Covert Action and Implausible Deniability," *International Affairs*, Vol. 94, No. 3 (May 2018), pp. 477–494, doi.org/10.1093/ia/iiy067.

45. Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies*, Vol. 35, No. 1 (2012), pp. 5–32, doi.org/10.1080/01402390.2011.608939; Gartzke, "The Myth of Cyberwar"; and Borghard and Lonergan, "Cyber Operations as Imperfect Tools of Escalation."

46. Beilenson, *Power through Subversion*, p. v; and Frank Kitson, *Low Intensity Operations: Subversion, Insurgency, and Peacekeeping* (London: Faber and Faber, 1971), p. 3.

47. Melissa M. Lee, *Crippling Leviathan: How Foreign Subversion Weakens the State* (Ithaca, N.Y.: Cornell University Press, 2020).

48. William C. Wohlforth, "Realism and Great Power Subversion," *International Relations*, Vol. 34, No. 4 (December 2020), pp. 459–481, doi.org/10.1177/0047117820968858.

49. Blackstock, *The Strategy of Subversion*, p. 50.

able to subversion because it contains flaws that allow subversive actors to infiltrate and manipulate the system in unexpected ways. The main system of rules targeted by traditional subversion are institutions, and recent research has examined the use of subversion against institutions of all kinds.[50] If exploitation is successful, subversive actors can use the targeted systems to produce detrimental effects against an adversary, without revealing either their identity or the subversive activity itself.[51] Subversion is thus covert and clandestine. For example, a spy might become an employee at an industrial facility and gain access to machinery that they manipulate to damage the facility and possibly surrounding areas, but they hide the subversion by making it look like an accident.

Cyber operations rely on the same mechanism of secret exploitation, but they target computer systems rather than political systems. Exploitation is possible because the behavior of computer systems is determined by different layers of code, consisting of logical rules and instructions.[52] Hacking, the central instrument used in cyber operations as commonly defined, involves secretly exploiting flaws in these rules to make computer systems behave in unintended ways.[53] In practice, hackers establish undetected and unauthorized access and control over an adversary's computer systems, which they manipulate to produce detrimental effects against the adversary. For example, hackers might target computer systems that control physical machinery and manipulate their operation in a way that damages or destroys the machinery. The 2010 Stuxnet operation that sabotaged Iranian nuclear enrichment centrifuges with a computer virus offers a key example.[54] In addition to targeting technical vulnerabilities in computer systems, hackers also use "social engineering" to exploit pathologies in human behavior to get people to unwittingly provide access to systems.[55] Phishing emails are a classic example.[56] Cyber operations

50. Jan Olsson, "Subversive Action," in *Subversion in Institutional Change and Stability: A Neglected Mechanism* (London: Palgrave Macmillan, 2016), pp. 39–61, doi.org/10.1057/978-1-349-94922-9_3; and James Mahoney and Kathleen Thelen, eds., *Explaining Institutional Change: Ambiguity, Agency, and Power* (Cambridge: Cambridge University Press, 2010).
51. Blackstock, *The Strategy of Subversion*, p. 68.
52. Thomas Dullien, "Weird Machines, Exploitability, and Provable Unexploitability," *IEEE Transactions on Emerging Topics in Computing*, Vol. 8, No. 2 (April–June 2020), pp. 391–403, doi.org/10.1109/TETC.2017.2785299.
53. Erickson, *Hacking*, p. 115.
54. Ralph Langner, *To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve* (Arlington, Va.: Langner Group, November 2013), http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf.
55. Pekka Tetri and Jukka Vuorinen, "Dissecting Social Engineering," *Behaviour & Information Technology*, Vol. 32, No. 10 (2013), pp. 1014–1023, doi.org/10.1080/0144929X.2013.763860.
56. Prashanth Rajivan and Cleotilde Gonzalez, "Creative Persuasion: A Study on Adversarial Be-

Table 1. Key Instruments of Power in International Relations

	Warfare	Diplomacy	Subversion
Relation	direct	direct	indirect
Interaction Mode	overt/covert	overt	covert/clandestine
Mechanism	force	persuasion/bargaining	exploitation

thus share the core characteristics of subversion, namely the reliance on secret exploitation and the indirect use of adversary systems to produce effects. Accordingly, cyber operations are an instrument of subversion—and technical experts routinely refer to hacking as subversion.[57]

The secret and indirect nature of exploitation distinguishes subversion from the two classic instruments of power in world politics: warfare and diplomacy (see table 1). In the words of Carl von Clausewitz, war is "the use of physical force to compel an enemy to one's will."[58] It shifts the balance of power by destroying adversaries' material capabilities. Warfare typically involves direct interaction, but states can also covertly pursue "secret wars."[59] In contrast, diplomacy relies on direct and overt forms of communication to exert influence through reasoned discourse, bargaining, or signaling.[60] Diplomacy shifts the balance of power through alliances and international law.[61]

Strategically, subversion promises a way for states to intervene in adversary affairs when diplomacy falls short to produce results, and yet at lower risks and costs than going to war. The secret and indirect nature of exploitation enables this promise. As discussed, secrecy reduces escalation risks and lowers reputational costs. The indirect nature of exploitation adds a third benefit:

haviors and Strategies in Phishing Attacks," *Frontiers in Psychology*, February 21, 2018, doi.org/10.3389/fpsyg.2018.00135.

57. See, for example, Philip A. Myers, "Subversion: The Neglected Aspect of Computer Security," master's thesis, Naval Postgraduate School, 1980, https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/myer80.pdf; and Susan Young and Dave Aitel, *The Hacker's Handbook: The Strategy behind Breaking into and Defending Networks* (Boca Raton, Fla.: CRC, 2004), pp. 15–29.

58. Carl von Clausewitz, *On War*, abr., ed. Beatrice Heuser, trans. Michael Howard and Peter Paret (Oxford: Oxford University Press, 2006), p. 13.

59. Carson, *Secret Wars*.

60. Hedley Bull, *The Anarchical Society: A Study of Order in World Politics* (New York: Columbia University Press, 1977), p. 163; Thomas Risse, "'Let's Argue!': Communicative Action in World Politics," *International Organization*, Vol. 54, No. 1 (Winter 2000), pp. 1–39, https://www.jstor.org/stable/2601316; Thomas C. Schelling, *Arms and Influence* (New Haven, Conn.: Yale University Press, 2008); and Barbara Koremenos, Charles Lipson, and Duncan Snidal, "The Rational Design of International Institutions," *International Organization*, Vol. 55, No. 4 (Autumn 2001), pp. 761–799, https://www.jstor.org/stable/3078615.

61. Henry Kissinger, *Diplomacy* (New York: Simon and Schuster, 1995), pp. 17–29.

lower resource costs, since effects are produced through adversary systems, rather than one's own material capabilities. Subversion can provide independent strategic utility by undermining, manipulating, or disrupting the institutions that modern societies depend on, weakening adversaries or influencing their foreign policy. Cyber subversion holds the same promise, as revolutionary scholars emphasize.

THE SUBVERSIVE TRILEMMA

In practice, subversion tends to fall short of its promise. Blackstock noted in 1964 that scholars and policymakers have "greatly overestimated" the effectiveness and utility of subversion,[62] and more recent quantitative studies document the high failure rate of subversive operations.[63] The reason for this failure, I argue, is a subversive trilemma that constrains effectiveness and limits strategic utility. As this section shows, cyber subversion faces the same trilemma.

The indirect and secret nature of exploitation that enable the strategic promise of subversion require significant efforts to establish and maintain. In general, secrecy in covert operations requires extra "time, skills, an money."[64] Subversion requires further efforts because it depends on secrecy to succeed. Whereas secret warfare operates on a spectrum of secrecy and can continue even when the cover has been blown,[65] discovery of a subversive operation typically means failure. I argue that this constraint applies to cyber subversion as well. In traditional subversion, the victim can arrest the spy involved;[66] in cyber subversion, victims can delete computer viruses and "patch" vulnerabilities.[67]

To fulfil the promise of secret exploitation, I find that actors must meet four distinct challenges that constrain operational effectiveness. They must identify suitable vulnerabilities in a system designed by others, exploit them without being detected, establish access and control over the system without detection, and maintain control to produce effects through this system that achieve their desired outcomes. As detailed below, these four challenges constrain opera-

62. Blackstock, *The Strategy of Subversion*, p. 304.
63. Lindsey A. O'Rourke, *Covert Regime Change: America's Secret Cold War* (Ithaca, N.Y.: Cornell University Press, 2018); and Sarah-Jane Corke, *US Covert Operations and Cold War Strategy: Truman, Secret Warfare, and the CIA, 1945–53* (New York: Routledge, 2008).
64. Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 4th ed. (Washington, D.C.: CQ, 2009), p. 177.
65. Cormac and Aldrich, "Grey Is the New Black."
66. Beilenson, *Power through Subversion*, p. 63.
67. Erickson, *Hacking*, p. 320.

tional effectiveness across three variables: operational speed, intensity of effects, and control.

First, speed is limited because identifying vulnerabilities and developing means of exploitation requires reconnaissance and learning how target systems function. Both processes take time. Spies have had to learn new languages or skills to infiltrate institutions.[68] Hackers similarly study how complex computer systems function and write code to exploit them, which can take months.[69] Moreover, cyber subversion may require more time than traditional subversion because hackers cannot use force to override logic in programming code if their means of exploitation fails.[70] In contrast, spies can use limited force to gain access, such as by blackmailing individuals or forcing open a door.

Second, the need to establish access to target systems without detection limits the intensity of effects. In general, only effect types for which suitable target systems exist are possible. If there are no vulnerable institutions that control physical machinery within a targeted state, traditional subversion cannot produce physical effects. This constraint applies to cyber subversion as well, whereby only those social and physical processes controlled by computers are within reach. Even for vulnerable targets, the scope and scale of effects that actors can produce through a target system depend on the scope and scale of their access to the system. Expanding the scope and scale of access increases discovery risks, however, thus limiting the maximum intensity that can be achieved without discovery. In traditional subversion, for example, Lindsey O'Rourke identifies a resulting dilemma between the scale of an operation and the need for secrecy.[71] I expect the same to apply to cyber subversion. Undoubtedly, cyber operations facilitate a greater scale of effects compared to traditional subversion because computer viruses can multiply and spread automatically.[72] This capacity does not negate the dilemma between secrecy and scale, however; the more systems that are affected, the more likely one of the affected victims will discover the compromise. Moreover, automated proliferation may spread beyond its intended targets. Accordingly, the infamous Stuxnet malware was discovered by a Belarusian antivirus firm because it

68. Christopher Andrew and Vasili Mitrokhin, *The Mitrokhin Archive: The KGB in Europe and the West* (London: Allen Lane, 1999), pp. 192–193, 220.
69. Lillian Ablon and Andy Bogart, *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits* (Santa Monica, Calif.: RAND, 2017), https://www.rand.org/pubs/research_reports/RR1751.html.
70. Libicki, *Cyberdeterrence and Cyberwar*, p. 16.
71. O'Rourke, *Covert Regime Change*, p. 8.
72. Jürgen Kraus, "On Self-Reproducing Computer Programs," trans. and ed. Daniel Bilar and Eric Filiol, *Journal in Computer Virology*, Vol. 5 (February 2009), pp. 9–87, doi.org/10.1007/s11416-008-0115-z.

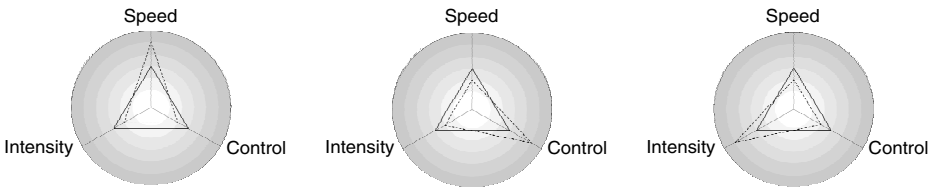
spread, apparently accidentally, far beyond the targeted nuclear enrichment plant in Natanz.[73]

Third, the need to avoid discovery and the indirect production of effects via manipulation of a target system limit control, both over the system itself and the effects produced through it. A subversive actor's control over a target system is never absolute because, as discussed, upon discovery the victim can neutralize it. Even if it remains undiscovered, however, subversive actors can only establish control over those parts of the system with which they have become familiar. A spy may be unable to gain access to a targeted organization or may lack the language skills required for infiltration.[74] Likewise, hackers may be unfamiliar with certain computer systems and find no way to access them. Most importantly, subversive actors do not have full control over effects for two reasons. First, they may lose control over the subversive agent. Pressure from undercover work may prompt spies to behave erratically or defect.[75] Although they don't have feelings, computer viruses used in cyber subversion may similarly go rogue. The Morris Worm of 1988, for example, was designed as a harmless network mapping tool, but its automated spread combined with bandwidth-consuming activity caused massive unintended disruptions across the early Internet.[76] Finally, because actors have limited control over target systems, these systems may respond unexpectedly to manipulation, which risks causing the subversion to either fail to produce the desired effect or create negative and unintended consequences.

Crucially, these constraining variables of speed, intensity, and control are negatively correlated, producing a subversive trilemma. As illustrated in figure 1, holding all else equal, improving one variable tends to produce corresponding losses across the remaining variables. Increasing operational speed means less time for reconnaissance and development, which increases the risk of making mistakes and that targets will discover the subversion, both of which decrease control. Increasing intensity requires actors to expand the scope or scale of access to systems, which increases discovery risks. Lowering discovery risks for a given effects intensity tends to increase development time requirements, which reduces speed. Moreover, increasing control usually reduces speed because hackers need more time for reconnaissance and develop-

73. The anti-virus software vendor VirusBlokAda in Belarus detected the malware used in the Stuxnet operation on computers in Belarus on June 17, 2010, and initially named it "Rootkit .TmpHider." "Rootkit.TmpHider," *VirusBlokAda*, http://www.anti-virus.by/en/tempo.shtml.
74. Andrew and Mitrokhin, *The Mitrokhin Archive*, pp. 200–201.
75. Michael Herman, *Intelligence Power in Peace and War* (Cambridge: Cambridge University Press, 1996), p. 65.
76. Charles Schmidt and Tom Darby, "The What, Why, and How of the 1988 Internet Worm," *Snowplow*, revised July 2001, https://web.archive.org/web/20051020030056/http://snowplow.org/tom/worm/worm.html.

Figure 1. The Subversive Trilemma



NOTE: In each diagram, the dotted triangle shows how increasing one of these three variables tends to decrease the others compared with a given state in which all are balanced, which is represented by the solid triangle.

ment plus extra efforts to avoid collateral damage by limiting the scale of effects and, thus, intensity.

This subversive trilemma constrains operational effectiveness and thus severely limits the strategic utility that subversion can achieve in practice. Speed, intensity, and control are essential components of operational effectiveness, yet each of these variables can lead to mission failure and no more than two can be maximized at once. Increasing both speed and intensity proportionally "doubly" decreases control, for example, because the more intense the possible effects are, the more sensitive the target and the more challenging the undetected exploitation is likely to be. Hence, pursuing both maximum intensity and speed makes it highly likely that an operation either fails to produce a strategically significant outcome or produces unintended consequences that impose further costs. Conversely, maximizing both control and speed is likely to constrain intensity to such a degree that it is extremely unlikely to produce a strategically significant outcome. Maximizing both intensity and control in turn tends to reduce speed to a glacial pace. Accordingly, forensic evidence indicates that the carefully calibrated Stuxnet operation took five years to develop.[77] In theory, operations that maximize intensity and control are most likely to produce significant strategic gains, but in practice, their glacial pace renders them mostly useless in urgent crises and makes premature discovery probable. If high speed is necessary, such operations are likely unable to go after the most sensitive targets because they require significant reconnaissance and development time, and the scope of control that they have over a given target system is also limited. Meanwhile, more intense effect types, such as damage or disruption, involve greater risk of collateral damage or unintended

77. Geoff McDonald et al., "Stuxnet 0.5: The Missing Link," *Symantec Security Response* (Mountain View, Calif.: Symantec Corporation, 2013), https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-088.pdf.

consequences. Maximizing control requires either avoiding such effect types or restricting use to fewer and less sensitive targets—both of which reduce effect intensity.

Because of this trilemma, like traditional subversion, cyber subversion is unlikely to deliver on its strategic promise except in "unicorn" scenarios in which hackers are both exceptionally skilled and exceptionally lucky. Otherwise, in line with the different configurations of the trilemma outlined above, cyber operations will tend to be too slow, too low in intensity, or too unreliable to provide significant utility.

hypotheses and research design

My theory refines cyber evolution theory by specifying a distinct set of operational characteristics that shape strategic utility. It produces three expectations and three corresponding hypotheses for the case analysis. First, like cyber revolution theory, I expect states to primarily deploy cyber operations independently from diplomacy and warfare. Unlike cyberwar theories, I expect states to primarily use cyber operations as part of subversive campaigns against nonmilitary targets. Second, I expect the operational variables of speed, intensity, and control to be negatively correlated. Specifically, the different permutations of this trilemma produce the following hypotheses: increasing speed tends to decrease intensity and control (H1); increasing intensity tends to decrease speed and control (H2); increasing control tends to decrease intensity and speed (H3); and increasing two variables tends to doubly decrease the remaining variable (H4). Evidence supporting these hypotheses across different cyber operations would support my theory, whereas evidence of operations scoring high across all three variables, or actors achieving simultaneous increases across all three variables would support cyber revolution theory or cyberwar theory (for operations deployed for warfare). Third, I expect most cyber operations to fall short of providing measurable strategic utility, and I expect the subversive trilemma to be a key limiting factor.

I test these expectations in a case study of the Russo-Ukrainian conflict, which started in 2013. The five cyber operations within the case provide internal variation and allow within-case comparison. The Russo-Ukrainian conflict is a paradigmatic case of cyber-enabled limited conflict that occupies the gray zone between peace and conventional war, in which cyber revolution theorists expect cyber operations to provide added utility.[78] Four of the cyber operations

78. Oliver Fitton, "Cyber Operations and Gray Zones: Challenges for NATO," *Connections*, Vol. 15, No. 2 (Spring 2016), p. 109, http://www.jstor.org/stable/26326443; and James J. Wirtz, "Life in the 'Gray Zone': Observations for Contemporary Strategists," *Defense & Security Analysis*, Vol. 33, No. 2 (2017), p. 108, doi.org/10.1080/14751798.2017.1310702.

in this case are attributed to Sandworm, which is an advanced hacker group that is in turn attributed to Russia's Glavnoye Razvedyvatelnoye Upravlenie (GRU) intelligence service.[79] Russia is a leading cyber power that is known for having a high tolerance for risk,[80] and the Sandworm group is one of the world's most skilled and most dangerous hacking groups.[81] I expect the constraints of the subversive trilemma to be less pronounced in this case for several reasons. In addition to the linguistic and cultural similarities between the two countries, Russian spies have penetrated Ukrainian institutions, and many Ukrainian industrial facilities rely on Russian technologies.[82] Moreover, Sandworm had seven years to adapt and improve its tradecraft. Hence, the conditions render cyber operations most likely to demonstrate their effectiveness and utility, while the constraints of subversion I identify are least likely to apply compared to conflicts with less favorable conditions.

I proceed in three steps. First, I verify whether and how Russia deployed cyber operations in coordination with its diplomatic and military efforts. Second, I measure relative operational speed, intensity, and control to assess whether and how the subversive trilemma constrained effectiveness. I base my measurement for speed on how much time elapses between when the hackers start to develop the cyber operation and when it concludes. To measure intensity, I track both scope (i.e., degree of intrusiveness) and scale (i.e., number of affected devices and individuals). I follow Loch Johnson's escalation ladder of covert operations, which ranks thirty-eight different types of operations according to their intrusiveness (the lower the rank, the higher the intrusiveness) and groups them according to risk.[83] Finally, I use four key indicators to meas-

79. Sandworm is also known as "TeleBots," "Electrum," "Quedagh,"and "BlackEnergy." See the online resource "APT Groups and Operations," established by Florian Roth and maintained by several threat intelligence researchers for further background: https://docs.google.com/spreadsheets/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/edit#gid=1636225066.

80. Mark Galeotti, *Putin's Hydra: Inside Russia's Intelligence Services* (London: European Council on Foreign Relations [ECFR], May 2016), http://www.ecfr.eu/page/-/ECFR_169_-_PUTINS_HYDRA_INSIDE_THE_RUSSIAN_INTELLIGENCE_SERVICES_1513.pdf; and "Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed," *National Cyber Security Centre*, October 3, 2018, https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed.

81. Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (New York: Doubleday, 2019); and Robert Lemos, "Suspected Russian 'Sandworm' Cyber Spies Targeted NATO, Ukraine," *Ars Technica*, October 14, 2014, https://arstechnica.com/security/2014/10/suspected-russian-sandworm-cyber-spies-targeted-nato-ukraine/.

82. Vitalii Usenko and Dmytro Usenko, "30% of Ukrainian SBU Officers Were Russian FSB and GRU Agents," ed. Olena Wawryshyn, *Euromaidan Press*, April 24, 2014, http://euromaidanpress.com/2014/04/24/30-of-ukrainian-sbu-officers-were-russian-fsb-and-gru-agents/; and Tomila Lankina and Alexander Libman, "Soviet Legacies of Economic Development, Oligarchic Rule, and Electoral Quality in Eastern Europe's Partial Democracies: The Case of Ukraine," *Comparative Politics*, Vol. 52, No. 1 (October 2019), pp. 127–176, doi.org/10.5129/001041519X15624348215945.

83. Johnson, "On Drawing a Bright Line for Covert Operations."

ure control: premature discovery, failure to produce effects, time to neutralize effects, and collateral damage.

Third, to evaluate strategic utility I analyze whether and how cyber operations contribute to Russia's strategic goals and/or cause a shift in the balance of power. It is challenging to determine strategic utility for conventional weapons let alone for secret cyber operations.[84] Indeed, for all five cyber operations Russia has neither publicly acknowledged its involvement nor clearly stated its goals. To determine the strategic utility of these cyber operations despite these constraints, I follow established practice in intelligence studies to draw inferences using triangulation among multiple sources of data.[85]

In this case study, I use process-tracing[86] and leverage mostly original data from four main primary sources: field interviews with Ukrainian cybersecurity experts and witnesses,[87] leaked documents and emails,[88] forensic reporting, and social media posts and local media reporting.[89] I primarily measure utility through impacts on the balance of power defined as the distribution of material capabilities.[90] I also examine whether and how the subversive trilemma limits the strategic utility of each operation.

Case Study: The Russo-Ukrainian Conflict

The Russo-Ukrainian conflict has its origins in Ukraine's pursuit of closer relations with the European Union and the West. Despite President Viktor Yanukovych's close ties with Russia, in February 2013, the Ukrainian

84. James G. Roche and Barry D. Watts, "Choosing Analytic Measures," *Journal of Strategic Studies*, Vol. 14, No. 2 (1991), p. 172, doi.org/10.1080/01402399108437447.
85. Loch K. Johnson, ed., *Handbook of Intelligence Studies* (New York: Routledge, 2007), p. 81.
86. Jeffrey T. Checkel, "Mechanisms, Process, and the Study of International Institutions," in Andrew Bennett and Jeffrey T. Checkel, eds., *Process Tracing: From Metaphor to Analytic Tool* (Cambridge: Cambridge University Press, 2014), pp. 74–97, doi.org/10.1017/CBO9781139858472.006.
87. The author traveled to Ukraine in 2018 to conduct interviews with twenty-three key individuals, while adhering to a strict ethics protocol approved by the University of Toronto's Research Ethics Board (Protocol No.: 00034827).
88. Email inboxes of separatist leader Kirill Frolov and Russian advisor Vladimir Surkov provide unique insights into Russian perceptions and coordination of separatist movements in Ukraine. Daria Goriacheva, the author's research assistant and a native Russian speaker, carefully analyzed and translated these sources. The Ukrainian hacker collective Ukrainian Cyber Alliance obtained these emails and has made them publicly available at the following links: https://ordilo.org/wp-content/uploads/2016/12/frolov_moskva@mail.ru.rar (last accessed May 17, 2019) and https://drive.google.com/drive/folders/0BxCzAWE6sxSfRXVjdm1pV2c3WXc (last accessed July 15, 2021). Henceforth, email citations from this source will include the sender and recipient names, date, and time.
89. Collected and translated by the author's research assistant, Daria Goriacheva.
90. Kenneth N. Waltz, *Theory of International Politics* (Reading, Mass: Addison-Wesley, 1979).

Parliament voted to commit to an EU-Ukraine Association Agreement.[91] This vote threatened Russian interests of maintaining Ukraine within its sphere of influence. A key part of the Kremlin's Ukraine strategy has been spreading "rumour, speculation, half-truth, conspiracy, and outright lie, to obscure the realities of Russian activities."[92] Consequently, the drivers of foreign policy continue to be hotly debated.[93] Yet, even amidst these acrimonious debates, there is broad consensus that Russia has pursued two complementary strategic goals.[94] It wants to prevent and reverse Ukraine's realignment toward the European Union and the West as well as maintain Ukraine within its sphere of influence. Accordingly, Russian scholars highlight Russia's priority to "stop the pro-Western Kiev government"[95] and explain that "Russia looks at the former USSR states as creating arcs of safety in Eastern Europe."[96] Public statements by Russia's leadership warn Ukraine against the "inevitable financial catastrophe"[97] that would result from EU integration, and President Vladimir Putin has repeatedly emphasized the shared history of Ukraine and Russia and their "sameness"[98] as "one people."[99]

To achieve these goals, Russia leveraged diplomacy, (semi-covert) warfare, and subversion. Initially, Russia applied increasing diplomatic pressure on the Yanukovych government while mobilizing a network of subversive proxy actors, comprised of church organizations such as the "Union of

91. Interfax-Ukraine, "Parliament Passes Statement on Ukraine's Aspirations for European Integration," *Kyiv Post*, February 22, 2013, https://www.kyivpost.com/article/content/ukraine-politics/parliament-passes-statement-on-ukraines-aspirations-for-european-integration-320792.html.

92. Mark Galeotti, *Controlling Chaos: How Russia Manages Its Political War in Europe* (Berlin: ECFR, September 2017), p. 6, http://www.ecfr.eu/publications/summary/controlling_chaos_how_russia_manages_its_political_war_in_europe.

93. Elias Götz, "Russia, the West, and the Ukraine Crisis: Three Contending Perspectives," *Contemporary Politics*, Vol. 22, No. 3 (2016), pp. 249–266, doi.org/10.1080/13569775.2016.1201313.

94. See section 1 of the online appendix, doi.org/10.7910/DVN/IZ65MC.

95. Vladimir V. Shtol, "Geopoliticheskiye zadachi Rossii na postsovetskom prostranstve" [Geopolitical tasks for Russia in post-Soviet space], *Vestnik Moskovskogo Gosudarstvennogo Oblastnogo Universiteta* [Moscow National Regional University Press], No. 3S (2014), p. 176.

96. E. Shturba and M. Makhalkina, "Territorial'nyye anklavy byvshego SSSR v kontekste natsional'noy bezopasnosti sovremennoy Rossii" [Territorial enclaves of the former USSR in a context of national safety of contemporary Russia], *Istoricheskaya i sotsial'no-obrazovatel'naya mysl* [Historic and socially-educated thoughts],Vol. 2, No. 1C (2016), p. 26.

97. Shaun Walker, "Ukraine's EU Trade Deal Will Be Catastrophic, Says Russia," *Guardian*, September 22, 2013, https://www.theguardian.com/world/2013/sep/22/ukraine-european-union-trade-russia.

98. "Putin Says Russia, Ukraine Torn Apart to Prevent Major Rival from Emerging," *TASS*, February 21, 2020, https://tass.com/politics/1122727.

99. Vladimir Putin, "Address by President of the Russian Federation: Vladimir Putin Addressed State Duma Deputies, Federation Council Members, Heads of Russian Regions, and Civil Society Representatives in the Kremlin," *President of Russia*, March 18, 2014, http://en.kremlin.ru/events/president/news/20603.

Orthodox Citizens" and other separatist groups, to stimulate pro-Russian sentiment. A leaked document in 2013 outlines Russia's goals to "create a network of Russian influence . . . [to] prevent the signing of association agreements between Ukraine and the EU . . . [and] neutralizethe political and media influence of European integrators."[100] This campaign involved some curious measures, such as a series of rock concerts,[101] which unsurprisingly failed to produce measurable results.[102] Russia's diplomatic efforts, however, were successful. Following a secret meeting with Putin, Yanukovych unilaterally withdrew from EU association negotiations in November 2013, prompting tens of thousands of Ukrainians to gather at Maidan square to protest.[103] In February 2014, Yanukovych's government collapsed. In response, Russia utilized its subversive proxies to conduct a regime change operation in Crimea. Subsequently, Russia's proxies organized protests around government institutions in the regional capital Sevastopol, which Russia supported with unmarked military forces.[104] These proxies then helped organize a referendum, coordinated from Moscow, deciding secession before Ukraine could react and producing a fait accompli.[105] In the Donbass region, Russia deployed similar tactics, but pockets of local resistance allowed the Ukrainian government to launch a countercampaign in May 2014.[106] Russia and Ukraine remain in a protracted stalemate with ongoing, significant bloodshed.

Although Russia has (thus far) failed to achieve its two core strategic goals,

100. "O komplekse mer po vovlecheniyu Ukrainy v Yevraziyskiy integratsionnyy protsess" [About the set of measures to involve Ukraine in the Eurasian integration process], *ZN.Ua*, August 16, 2013, https://zn.ua/internal/o-komplekse-mer-po-vovlecheniyu-ukrainy-v-evraziyskiy-integracionnyy-process-_.html.
101. Sergey Glazyev, email to Kiril Frolov, September 13, 2013, 9:45 a.m.
102. Sanshiro Hosaka, "The Kremlin's Active Measures Failed in 2013: That's When Russia Remembered Its Last Resort—Crimea," *Demokratizatsiya: The Journal of Post-Soviet Democratization*, Vol. 26, No. 3 (Summer 2018), pp. 321–364, muse.jhu.edu/article/699570.
103. Oksana Grytsenko and Ian Traynor, "Ukraine U-turn on Europe Pact Was Agreed with Vladimir Putin," *Guardian*, November 26, 2013, https://www.theguardian.com/world/2013/nov/26/ukraine-u-turn-eu-pact-putin.
104. Michael Kofman et al., *Lessons from Russia's Operations in Crimea and Eastern Ukraine* (Santa Monica, Calif.: RAND, 2017); Dmytro Lisunov, Oleh Baturin, and Serhiy Petrenko, "Why Surkov Needs Private Army: Union of Donbas Volunteers (UDV) as Reserve of National Guard of Russia," *InformNapalm English* blog, April 30, 2017, https://informnapalm.org/en/surkov-needs-private-army-union-donbas-volunteers-reserve-russian-guard/; and Alya Shandra, "Glazyev Tapes, Continued: New Details of Russian Occupation of Crimea and Attempts to Dismember Ukraine," *Euromaidan Press*, May 16, 2019, http://euromaidanpress.com/2019/05/16/glazyev-tapes-continued-ukraine-presents-new-details-of-russian-takeover-of-crimea-and-financing-of-separatism/.
105. Kremlin, "Podpisan ukaz o priznanii Respubliki Krym" [Decree on recognition of the Republic of Crimea was signed], *Prezident Rossii* [President Of Russia], March 17, 2014, http://kremlin.ru/events/president/news/20596; and David M. Herszenhorn and Andrew E. Kramer, "Ukraine Plans to Withdraw Troops from Russia-Occupied Crimea," *New York Times*, March 19, 2014, https://www.nytimes.com/2014/03/20/world/europe/crimea.html.
106. Vladimir A. Kalamanov, "Ukraina v geopoliticheskom izmerenii sovremennoy mirovoy

these efforts have produced significant strategic gains. First, the balance of power shifted in Russia's favor as it expanded its territory into Crimea and gained partial control over Donbass.[107] Despite prevailing conceptualizations of a cyber-enabled "hybrid war" in Ukraine, however, cyber operations played no role in attaining these gains.[108] Existing research shows cyber operations were irrelevant to military action in the Donbass or Crimea, and there is also no evidence that any cyber operations attributed to Russia contributed to the regime change operation in Crimea.[109] This absence is particularly surprising considering that Russian "information warfare" doctrine includes cyber operations as being relevant to the objectives it pursued in Ukraine.[110] Instead, Russia deployed its cyber operations independently of the warfare effort as part of a larger subversive campaign targeting the remaining territory of Ukraine.

EVALUATING CYBER OPERATIONS IN UKRAINE

The final phase of the Russo-Ukrainian conflict is characterized by slow-paced Russian efforts to weaken Ukraine. Although cyber operations have remained irrelevant in the military clashes in Donbass, in Ukraine's remaining territory, Russia used election interference, sabotage, disinformation, propaganda, and

sistemy i vozvrashcheniye Rossiyskogo liderstva" [Ukraine in the geopolitical dimension of the modern world system and the return of Russian leadership], *Vestnik Rossiyskogo Universiteta Druzhby Narodov* [Press of Peoples' Friendship University of Russia], *Politologiya* [Political Science], No. 4 (n.d.), p. 14; and Tom McCarthy and Alan Yuhas, "Ukraine Crisis: Kiev Launches 'Anti-terror Operation' in East—Live Updates," *Guardian*, April 15, 2014, https://www.theguardian.com/world/2014/apr/15/ukraine-military-forces-russia-live-blog.

107. Andrew S. Bowen, "Coercive Diplomacy and the Donbas: Explaining Russian Strategy in Eastern Ukraine," *Journal of Strategic Studies*, Vol. 42, No. 3–4 (2019), pp. 312–343, doi.org/10.1080/01402390.2017.1413550.

108. András Rácz, *Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist*, FIIA Report No. 43 (Helsinki: Finnish Institute of International Affairs [FIIA], June 16, 2015), https://www.fiia.fi/wp-content/uploads/2017/01/fiiareport43.pdf; and Fitton, "Cyber Operations and Gray Zones."

109. Nadiya Kostyuk and Yuri M. Zhukov, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?" *Journal of Conflict Resolution*, Vol. 63, No. 2 (February 2019), pp. 317–347, doi.org/10.1177/0022002717737138; and Aaron F. Brantly, Nerea M. Cal, and Delvin P. Winkelstein, *Defending the Borderland: Ukrainian Military Experiences with IO, Cyber, and EW* (West Point, N.Y.: Army Cyber Institute, December 1, 2017), https://vtechworks.lib.vt.edu/handle/10919/81979. See also section 2 of the online appendix, doi.org/10.7910/DVN/IZ65MC.

110. Keir Giles and William Hagestad II, "Divided by a Common Language: Cyber Definitions in Chinese, Russian, and English," paper presented at the 5th International Conference on Cyber Conflict, Tallinn, Estonia, June 4–7, 2013, https://ieeexplore.ieee.org/document/6568390; and Sergei Chekinov and Sergei Bogdanov, "Vliyanie nepriamykh deistvii na kharakter sovremennoi voiny" [The influence of indirect actions on the nature of modern warfare], *Voennaya Mysl* [Military Thought], No. 6 (2011), pp. 3–4, quoted and translated in Mark Galeotti, "Hybrid, Ambiguous, and Non-linear? How New Is Russia's 'New Way of War'?" *Small Wars & Insurgencies*, Vol. 27, No. 2 (March 2016), p. 288, doi.org/10.1080/09592318.2015.1129170.

Table 2. A Comparison of Five Cyber Operations

	Speed	Intensity	Control	Strategic Utility
election interference (2014)	3 months	low scale, high scope	• no premature discovery • disruptive effect on target partially produced • disruptive effect neutralized within 20 hours, preventing impact	negligible
power grid I (2015)	19 months	high scale, high scope	• premature discovery • disruptive effect on target produced • disruptive effect neutralized within 6 hours	negligible
power grid II (2016)	31 months	high scale, highest scope	• premature discovery • disruptive effect on target partially produced • disruptive effect neutralized within 75 minutes	negligible
"NotPetya" (2017)	6 months	highest scale, medium scope	• premature discovery • disruptive effect on targets produced • lasting effect (i.e., data destruction) • collateral damage and unintended consequences	measurable, significant impact on balance of power
"BadRabbit" (2017)	12 months	low scale, low scope	• no premature discovery • disruptive effects on target produced • controlled proliferation	negligible

economic warfare to conduct a long-term, slow-burning subversive campaign to weaken Ukraine and keep it within its sphere of influence.[111] Five major cyber operations attributed to Russian-sponsored actors contributed to this campaign, and the analysis in this section examines their operational mechanisms and strategic utility. Table 2 summarizes key findings.

ELECTION INTERFERENCE (2014). The first cyber operation attempted to disrupt Ukraine's 2014 presidential elections by sabotaging the computer systems of the Central Elections Commission (CEC). It moved fast and pursued intense effects by disrupting a core political process in democracies, yet it failed to influence the elections because the hackers missed a security measure that the

111. Alya Shandra and Robert Seely, "The Surkov Leaks: The Inner Workings of Russia's Hybrid War in Ukraine" (London: Royal United Service Institute [RUSI], July 2019), https://static.rusi.org/201907_op_surkov_leaks_web_final.pdf.

CEC used to neutralize the compromise. This outcome provides support for the subversive trilemma and is congruent with H4. Consequently, as I expect, the operation provided Russia—whose military intelligence agency GRU most likely sponsored it—with little measurable strategic utility. Furthermore, I find circumstantial evidence that Russia deployed this cyber operation as part of its larger subversive campaign rather than to support its diplomatic and military initiatives.[112] This finding confirms the expected independent strategic role of cyber operations.

The group behind this cyber operation to sabotage the CEC's computers developed it within only two months, which is very fast compared with the five years it took to develop Stuxnet.[113] The hackers had to work quickly because Ukraine's elections announcement in March 2014 was unexpected. Forensic evidence indicates the initial compromise of Ukraine's CEC occurred shortly after.[114] Although the vulnerability and means of exploitation remain unknown, on May 21 the hackers deployed malware (i.e., a computer virus) that disrupted the CEC's computer systems for at least several hours.[115] The CEC successfully restored service before election day on May 25.[116]

The hackers moved fast while pursuing intense effects that were low in scale yet high in scope because they aimed to disrupt a core democratic process.[117] Yet, as predicted by the trilemma, they had insufficient control over the CEC's computer system. The intended effect of the cyber operation became clear on May 23, when the hacker collective Cyber Berkut boasted to have "destroyed PC and network infrastructure of the Ukrainian CEC," and challenged the elections' legitimacy as being under "total U.S. control."[118] Cyber Berkut is a front organization for GRU[119] and is likely linked to high-profile threat actor

112. See section 3 in the online appendix, doi.org/10.7910/DVN/IZ65MC.
113. McDonald et al., "Stuxnet 0.5."
114. Author interview with Victor Zhora, Kyiv, April 7, 2018; and Nikolay Koval, "Revolution Hacking," in Kenneth Geers, ed., *Cyber War in Perspective: Russian Aggression against Ukraine* (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015), p. 57, https://ccdcoe.org/library/publications/cyber-war-in-perspective-russian-aggression-against-ukraine/.
115. Nikolay Koval, then head of Ukraine's Computer Emergency Response Team (CERT), indicates the outage lasted around twenty hours. Koval, "Revolution Hacking," p. 57. Cybersecurity expert Victor Zhora, who was personally involved in the mitigation efforts, noted that the outage lasted only "a few" hours; personal correspondence with the author via online messaging service, May 19, 2019.
116. Author interview with Zhora, 2018.
117. According to Johnson's escalation ladder, election interference is a "high risk option" (rung 18 of 38). Johnson, "On Drawing a Bright Line for Covert Operations," pp. 286–288.
118. "The Ministry of Finance of Ukraine Is Cracked: In the Country There Were Only Debts," *CyberBerkut*, May 23, 2015, http://www.cyber-berkut.ru/en/index_02.php.
119. "Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed," October 3, 2018.

APT 28.[120] Contrary to its claims, however, the vote counting remained unaffected because the hacker's reconnaissance overlooked the fact that the CEC could use its backups to restore service.[121] This evidence supports H4. Consequently, the cyber operation failed to help Russia disrupt Ukraine's election or to shift the balance of power. The elections proceeded unhindered, and their integrity was widely accepted.[122]

POWER GRID I (2015). The second Russian-sponsored cyber operation sabotaged equipment by the energy providers Prykarpattyaoblenergo, Chernovtsoblenergo, and Kievoblenergo, causing a power outage in Western Ukraine on December 23, 2015, that affected 230,000 people and lasted six hours. These highly intense effects featured both high scope and scale and required substantial time to develop, yet the hackers failed to produce strategically significant lasting effects because they had insufficient control over the targeted systems. Although the hackers successfully exploited the power grid infrastructure, ultimately the companies used a simple switch to neutralize the disruption. The outage affected less than 1 percent of Ukraine's population and comprised only about 0.015 percent of Ukraine's daily energy consumption.[123] According to a senior advisor to the Ukrainian government, its short duration and timing on the day before Christmas caused minimal economic disruption.[124] In contrast to sensationalist Western coverage naming this an "act of cyberwar,"[125] only a few local Ukrainian outlets covered it, and none on the front page.[126] This outcome supports the subversive trilemma (specifically H2) and its constraining influence on strategic utility.

120. Koval, "Revolution Hacking," p. 58.
121. Author interview with Zhora, 2018.
122. Organization for Security and Co-operation in Europe (OSCE) et al., *International Election Observation Mission: Ukraine—Early Presidential Election, 25 May 2014: Statement of Preliminary Findings and Conclusions* (Kyiv: OSCE, May 26, 2014), https://www.osce.org/odihr/elections/ukraine/119078?download=true.
123. Sych, "Zillya! Antivirus provela analiz kiberatak na infrastrukturnyye obyekti Ukrainy" [Zillya! Antivirus has analyzed cyber attacks on infrastructure facilities in Ukraine], *Zillya! Antivirus*, February 17, 2016, https://zillya.ua/ru/zillya-antivirus-provela-analiz-kiberatak-na-infrastrukturnye-obekti-ukrainy.
124. Author interview with senior Ukrainian government advisor, Kyiv, April 5, 2018. The official has asked to remain anonymous.
125. Jose Pagliery, "Scary Questions in Ukraine Energy Grid Hack," *CNN*, January 18, 2016, https://money.cnn.com/2016/01/18/technology/ukraine-hack-russia/index.html; Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/; and Elias Groll, "Did Russia Knock Out Ukraine's Power Grid?" *Foreign Policy*, January 8, 2016, https://foreignpolicy.com/2016/01/08/did-russia-knock-out-ukraines-power-grid/.
126. "SBU predupredila khakerskuyu ataku Rossiyskikh Spetssluzhb na energoob'yekty Ukrainy—112 Ukraina" [SBU prevented hacker attack of Russian Special Services on power facilities of Ukraine—112 Ukraine], *112.Ua*, https://112.ua/kriminal/sbu-predupredila-hakerskuyu-ataku-rossiyskih-specsluzhb-na-energoobekty-ukrainy-281811.html; "Pislya kibera-

I also find no evidence that this cyber operation was linked to Russia's military or diplomatic efforts at the time. Military clashes continued throughout December 2015 despite a truce.[127] There were no major diplomatic events. It is plausible, as some have argued, that this cyber operation was retaliation for sabotage to Crimea's power supply in November 2015 that destroyed the power lines linking it to the mainland, but there is no conclusive evidence.[128] This sabotage operation against the power grid was more intense than the effort to disrupt the CEC's computer systems. A power blackout can cause both physical damage and possibly death, particularly in winter.[129] As the subversive trilemma would predict, this relative increase in intensity correlated with a significant decrease in speed (see table 2). On May 12, 2014, one day after the Donbass referendum, Sandworm used a Portuguese university's compromised server[130] to send phishing emails to employees of the targeted energy firms.[131] Curiously, the sender address was a Portuguese university, and these emails contained general information on Ukraine's railway system.[132] This cyber operation therefore relied on the unlikely scenario of the victims being sufficiently interested in Ukraine's railway system to click on the malicious attachment. Somebody did, though, providing Sandworm access to corporate systems.[133]

Forensic evidence indicates that hackers needed another five months to access the physical control systems in order to exploit its technical vulnerabili-

taky na 'Prykarpattyaoblenerho' v SSHA perehlyanut' zakhyst enerhomerezh" [After the cyberattack on Prykarpattyaoblenerho, the protection of power grids will be reviewed in the United States], *Obozrevatel*, https://www.obozrevatel.com/ukr/news/58420-pislya-kiberataki-na-prikarpattyaoblenergo-v-ssha-pereglyanut-zahist-energomerezh.htm; and Sergey Martynets, "SSHA pidozryuyut? Rosiyu u prychetnosti do kiberatak na ukrayins'ki elektromerezhi" [The United States suspects Russia of involvement in cyberattacks on Ukrainian power grids], *Ukrainian National News* (UNN), January 7, 2016, https://www.unn.com.ua/uk/news/1536191-ssha-pidozryuyut-rosiyu-u-prichetnosti-do-kiberatak-na-ukrayinski-elektromerezhi.

127. "Deadly Clashes in Ukraine despite Holiday Truce," *RadioFreeEurope/RadioLiberty*, December 27, 2015, https://www.rferl.org/a/deadly-clashes-in-ukraine-despite-holiday-truce/27452015 html.

128. Kim Zetter, "Everything We Know about Ukraine's Power Plant Hack," *Wired*, January 20, 2016, https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/; Ivan Nechepurenko and Neil MacFarquhar, "As Sabotage Blacks Out Crimea, Tatars Prevent Repairs," *New York Times*, November 23, 2015, https://www.nytimes.com/2015/11/24/world/europe/crimea-tatar-power-lines-ukraine.html.

129. Johnson's ladder does not include critical infrastructure sabotage, but the scope of effects places it within the riskiest, "extreme options." Johnson, "On Drawing a Bright Line for Covert Operations," pp. 286, 292.

130. "Kyberuhroza BlackEnergy2/3" [Cyber threat BlackEnergy2/3], *CysCentrum*, January 16, 2016, https://cys-centrum.com/ru/news/black_energy_2_3.

131. Ibid.

132. Oleg Sych, "Zillya! Antivirus provela analiz kiberatak na infrastrukturnyye obyekti Ukrainy."

133. "Kyberuhroza BlackEnergy2/3," *CysCentrum*.

ties. In October 2014, threat intelligence vendor iSight reported that Sandworm was exploiting a "zero-day" vulnerability (a previously unknown vulnerability about which the software vendor is unaware) in Microsoft Windows to target energy providers.[134] Subsequent analysis showed that the hackers had identified a vulnerability in an industrial control system that establishes an interface for human-machine interaction (HMI).[135] HMI systems themselves, however, cannot cause physical effects (i.e., disrupting the power supply).[136] The hackers needed another fourteen months to learn how to operate a power plant.[137] At 3:30 p.m. on December 2015, Sandworm operatives manually entered commands that caused the temporary blackout, using built-in functionality to cause an unexpected outcome.[138]

The cyber operation disrupted power service by remotely disconnecting approximately thirty power substations and delayed restoration by simultaneously inundating phone support centers with calls.[139] Ninety minutes later, the hackers attempted to prevent the power companies from restoring service by deleting all data on the affected computers.[140] Yet, employees at these Soviet-era power plants neutralized the disruption and restored power within six hours by switching to manual control.[141] Although it later became clear that all the affected utility providers discovered the compromise months before Sandworm attempted to disconnect the power substations, none of the victims reported or acted upon the premature discovery.[142] It was primarily

134. Stephen Ward, "iSIGHT Discovers Zero-Day Vulnerability CVE-2014-4114 Used in Russian Cyber-Espionage Campaign," *iSight Partners* blog, October 14, 2014, https://web.archive.org/web/20141015001101/https://www.isightpartners.com/2014/10/cve-2014-4114/.
135. Kyle Wilhoit and Jim Gogolinski, "Sandworm to Blacken: The SCADA Connection," *Trend Micro: Security Intelligence Blog*, October 16, 2014, https://blog.trendmicro.com/trendlabs-security-intelligence/sandworm-to-blacken-the-scada-connection/.
136. Dragos, *Crashoverride: Analysis of the Threat to Electric Grid Operations* (Hanover, Md.: Dragos, 2017), p. 10, https://dragos.com/blog/crashoverride/CrashOverride-01.pdf.
137. As Dragos explains, access to an HMI enabled the hackers to "learn the industrial process and gain the graphical representation of that ICS [industrial control system] through the HMI." Dragos, *Crashoverride*, p. 10.
138. Robert M. Lee, Michael J. Assante, and Tim Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid* (Washington, D.C.: Electricity Information Sharing and Analysis Center, March 18, 2016), https://africautc.org/wp-content/uploads/2018/05/E-ISAC_SANS_Ukraine_DUC_5.pdf; and Dragos, *Crashoverride*, p. 10.
139. Sych, "Zillya! Antivirus provela analiz kiberatak na infrastrukturnyye obyekti Ukrainy"; and Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid."
140. "Kiberugroza BlackEnergy2/3," *CysCentrum*; Sych, "Zillya! Antivirus provela analiz kiberatak na infrastrukturnyye obyekti Ukrainy"; and Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid."
141. Sych, "Zillya! Antivirus provela analiz kiberatak na infrastrukturnyye obyekti Ukrainy"; and Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid."
142. "Kiberugroza BlackEnergy2/3," *CysCentrum*.

luck rather than stealth that enabled the hackers to control the system long enough to attempt to produce effects.

POWER GRID II (2016). One year after it disrupted power substations in Western Ukraine, Sandworm targeted the power grid in Kyiv, Ukraine's capital. The hackers had developed an advanced technique capable of more intense effects than its predecessor, which could, in theory, inflict lasting damage to Ukrenergo's power plant machinery.[143] But this capability failed, and Ukrenergo was able to neutralize the outage even faster than before. Maximizing intensity correlates with reduced speed and control—confirming H2. Like its predecessor in 2015, there is no evidence linking this cyber operation to Russia's ongoing military and diplomatic efforts in Ukraine. The key military events in October 2016 were infighting among the pro-Russian rebels in the Donbass region and the assassination of rebel leader Arsen "Motorola" Sergeyevich Pavlov.[144] Given the timing of this sabotage operation (days before Christmas), a Ukrainian government official speculated that its primary purpose was to inflict psychological distress rather than to advance Russia's military or diplomatic agenda.[145]

Sandworm required an additional twelve months (thirty-one months total) to develop this cyber operation compared with its 2015 predecessor. The hackers used this time to deepen their knowledge about power substations and to develop a more advanced and, theoretically, more effective malware. According to industrial cybersecurity experts Dragos, the hackers attempted to trigger an automated protective system that would take targeted substations offline (i.e., "islanding") by rapidly activating and deactivating power circuits.[146] This malware was theoretically capable of "coordinated targeting of multiple electric sites and could result in a few days of outages."[147] Forensic analysis revealed that the malware could cause lasting physical damage by deactivating Siemens's protective relays.[148]

The additional time that it took Sandworm to develop this sabotage operation against the power grid in Kyiv correlates with an increased potential in-

143. Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid."
144. Jack Losh, "Ukrainian Rebel Leaders Divided by Bitter Purge," *Washington Post*, October 3, 2016, https://www.washingtonpost.com/world/europe/ukrainian-rebel-leaders-divided-by-bitter-purge/2016/10/03/2e0076ac-8429-11e6-b57d-dd49277af02f_story.html; and Andrew E. Kramer, "Bomb Kills Pro-Russian Rebel Commander in Eastern Ukraine," *New York Times*, October 17, 2016, https://www.nytimes.com/2016/10/18/world/europe/ukraine-rebel-arsen-pavlov-motorola-killed.html.
145. Author interview with an anonymous government advisor, Kyiv, April 21, 2018.
146. Dragos, *Crashoverride*, p. 23.
147. Ibid., p. 23.
148. Ibid., p. 24.

tensity of effects, confirming expectations of the subversive trilemma. This cyber operation qualifies as an "extreme option" in Johnson's escalation ladder, given its potential physical damage.[149] At 11:53 p.m. on December 17, 2016, Sandworm's malware deenergized the Severyana power substation near Kyiv, resulting in a loss of 202.9 megawatts—enough to power around 600,000 Ukrainian households according to average consumption statistics by the International Energy Agency.[150] Ukrenergo had learned from the 2015 sabotage, however, and swiftly switched to manual control, so that "within an hour and fifteen minutes, power was restored in full."[151] In practice, this operation thus achieved less intense effects than its predecessor.

Dragos's analysis of this cyber operation underlined that deploying the advanced technique to damage targets "would be very difficult to do at scale."[152] Yet, the hackers never got that far. The networking protocol of the targeted industrial control systems reversed Internet protocol (IP) addresses when executing commands, but Sandworm had missed this and entered the wrong addresses, which resulted in "nonsensical communication."[153] When I interviewed Volodymyr Styran, a cybersecurity expert at Berezha Security, he concluded that Sandworm hackers are "just people" who "screwed it up at some point, as they did in previous incidents."[154] The triangulation of evidence indicates that this cyber operation neither contributed to Russia's strategic goals nor achieved a shift in the balance of power, which confirms my expectations. The economic and psychological impacts of this second sabotage operation

149. Johnson, "On Drawing a Bright Line for Covert Operations," p. 186.
150. "Prichinoy obestochivaniya chasti Kiyeva mozhet byt' ataka khakerov" [The reason for the blackout in part of Kiev may be an attack by hackers], *Fakty.ua*, December 18, 2016, https://fakty.ua/227538-prichinoj-obestochivaniya-chasti-kieva-mozhet-byt-ataka-hakerov. In the United States, one megawatt typically provides enough power for about 750 households. California Energy Commission, "California ISO Glossary," https://www.energy.ca.gov/resources/energy-glossary. Hence, an outage of 202.9 megawatts would equal power loss for 152,175 standard U.S. households. In 2016, IEA data shows average energy consumption per capita in Ukraine was only approximately one quarter of that in the United States (3.2MWh vs 12.8MWh), and thus the number of households affected would be up to 608,700. For data on electricity consumption per capita per country, see "Electricity," IEA, accessed August 21, 2021, https://www.iea.org/fuels-and-technologies/electricity.
151. Vsevolod Kovalchuk, "Tsiyeyi nochi na pidstantsiyi 'pivnichna' vidbuvsya zbiy—Vsevolod Kovalchuk" [That night at the northern substation a failure has been—Vsevolod Kovalchuk], Facebook, December 18, 2016, https://www.facebook.com/permalink.php?story_fbid=1798082313797621&id=100007876094707.
152. Dragos, *Crashoverride*, p. 25.
153. Joe Slowik, *Crashoverride: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack* (Hanover, Md.: Dragos, 2019), p. 11, https://dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf.
154. Author interview with Volodymyr Styran, Kyiv, April 19, 2018. The incident that Styran refers to is Sandworm's 2015 attempt to compromise the media firm Starlight Entertainment, during which it committed a similar basic error. See section 4 of the online appendix, doi.org/10.7910/DVN/IZ65MC.

against Ukraine's power infrastructure were even less significant than in 2015. The outage occurred overnight when most businesses were closed and most people were asleep. Although some U.S. media outlets covered the event, the incident barely registered in Ukrainian media.[155] Accordingly, security researcher Marina Kratofil concluded that the operation "should not have long and serious consequences."[156]

NOTPETYA (2017). Sandworm's fourth operation, NotPetya, used data-destroying self-proliferating malware to cause a massive disruption that measurably affected Ukraine's GDP. The hackers took much less time to prepare this operation (see table 2), opting to reduce the scope of the effects in order to maximize scale. Although at first glance NotPetya appears to provide evidence that supports cyber revolution theory about the scale advantage of cyber operations, I argue that NotPetya's scale resulted from a loss of control. Indeed, NotPetya's collateral damage and follow-on costs highlight the operational perils of maximizing scale, providing further evidence of the subversive trilemma and H4.

There is no evidence suggesting that Russia orchestrated the NotPetya cyber operation in coordination with its military and diplomatic efforts. On the diplomatic front, Ukrainian President Petro Poroshenko banned several high-profile Russian websites in May 2017,[157] while military clashes continued between Russia and Ukraine despite agreeing to another ceasefire agreement on June 24.[158] There is no indication that NotPetya was linked to any of these events.

Sandworm started to develop NotPetya in December 2016, when it released

155. "Prychynoy obestochyvanyya chasty Kyeva mozhet byt' ataka khakerov" December 18, 2016; "V 'Ukrenerho' ne vyklyuchayut' kiberataku na pidstantsiyu 'Pivnichna', cherez yaku chastynu Kyyevu bulo znestrumleno" [Ukrenergo does not rule out a cyberattack on the Pivnichna substation, because of which part of Kyiv was de-energized], *UNN*, December 18, 2016, https://www.unn.com.ua/uk/news/1628435-v-ukrenergo-ne-viklyuchayut-kiberataku-na-pidstantsiyu-pivnichna-cherez-yaku-chastinu-kiyevu-bulo-znestrumleno; and Informatsiyne ahentstvo Ukrayins'ki Natsional'ni Novyny (UNN) [Ukrainian National News (UNN) news agency reported], Vsi onlayn novyny dnya v Ukrayini za s'ohodni—naysvizhishi, ostanni, holovni [All online news of the day in Ukraine for today—the latest, latest, main], https://www.unn.com.ua/uk/news/1628435-v-ukrenergo-ne-viklyuchayut-kiberataku-na-pidstantsiyu-pivnichna-cherez-yaku-chastinu-kiyevu-bulo-znestrumleno.

156. "Vidklyuchennya elektroenerhiyi v Ukrayini bulo khakers'koyu atakoyu—eksperty" [Power outage in Ukraine was a hacker attack—experts], *Hromadske*, January 11, 2017, https://hromadske.ua/posts/vidkliuchennia-elektroenerhii-v-ukraini-bulo-khakerskoiu-atakoiu.

157. Cassandra Allen, "Mapping Media Freedom: Ukrainian Journalists Subjected to Malicious Cyber-Attacks," *Index on Censorship* blog, July 11, 2017, https://www.indexoncensorship.org/2017/07/journalists-ukraine-cyber-attacks/.

158. Patrice Hill, "Monitor Says Ukraine Cease-Fire, Weapons Withdrawal Not Being Honored," *RadioFreeEurope/RadioLiberty*, February 22, 2017, https://www.rferl.org/a/monitor-osce-says-ukraine-cease-fire-heavy-weapons-withdrawal-not-honored/28324012.html.

the "Moonraker worm," which could self-proliferate across networks and disrupt systems through data encryption.[159] It took Sandworm only six months to adapt the generic "Green Petya" malware upon which NotPetya was based.[160] Between January and March 2017, Sandworm targeted two unnamed financial institutions to test a new supply-chain malware propagation mechanism with a new malware called Python/TeleBot.A.[161] NotPetya used a similar supply-chain mechanism as the hackers compromised the software update server of a popular accounting software provider and hid malware within automated updates that would be sent to customers. This server update thus automatically spread the malware to its entire user population. According to Styran, NotPetya was "technically simple," but the hackers showed a spark of "genius" by exploiting the victims' trust in the automated server update.[162]

By May 2017, Sandworm had figured out how to compromise its key target, the Ukrainian software firm Intellect Services, which produces the popular M.E.Doc accounting software.[163] Ukrainian hacker Sean Townsend noticed that at least one of the firm's servers had not been updated since 2012,[164] and Ukrainian authorities confirmed that the last update occurred in February 2013.[165] Before deploying NotPetya, Sandworm propagated another newly developed piece of malware called "Xdata" through this server. XData infected 134 victims and caused some minor disruptions, but it did not significantly affect Ukraine.[166] Ukrainian cybersecurity expert Victor Zhora speculates that XData was a "proof of concept" aimed to "map the network" of victimized firms.[167] Sandworm finally deployed NotPetya, propagated it to M.E.Doc clients via a compromised software update on June 22, and activated it across all

159. Anton Cherepanov, *GreyEnergy: A Successor to BlackEngergy*, GreyEnergy White Paper (Bratislava, Slovakia: ESET, October 2018), https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf.
160. Ibid.
161. Anton Cherepanov, "TeleBots Are Back: Supply-Chain Attacks against Ukraine," *WeLiveSecurity* blog, ESET, June 30, 2017, https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/.
162. Author correspondence with Volodymyr Styran via online messaging service, May 14, 2019.
163. Jack Stubbs and Pavel Polityuk, "Family Firm in Ukraine Says It Was Not Responsible for Cyber Attack," Reuters, July 3, 2017, https://www.reuters.com/article/us-cyber-attack-ukraine-software-idUSKBN19O2DK.
164. Author interview with Sean Townsend, Kyiv, April 15, 2018.
165. Catalin Cimpanu, "M.E.Doc Software Was Backdoored 3 Times, Servers Left without Updates since 2013," *BleepingComputer*, July 6, 2017, https://www.bleepingcomputer.com/news/security/m-e-doc-software-was-backdoored-3-times-servers-left-without-updates-since-2013/.
166. MalwareHunterTeam (@malwarehunterteam), "Here is an IDR based heatmap for past 24 hours of XData ransomware. 91% of victims from Ukraine, ~3% from RU. @BleepinComputer @demonslay335," Twitter, May 19, 2017, 1:56 p.m., https://twitter.com/malwrhunterteam/status/865627306794008578.
167. Author interview with Zhora, 2018.

infected machines on June 27. NotPetya self-proliferated across networks from all affected machines before executing a disk encryption program that irreversibly destroyed all data on targeted computers. The ransom demand that NotPetya displayed on hacked computers turned out to be deception, because neither the bitcoin address it listed for payments nor the decryption key existed.[168]

NotPetya's economic disruption ranks in the middle of Johnson's escalation ladder (rung nineteen of thirty-eight).[169] It achieved massive scale, however, disabling an estimated 500,000 computers in Ukraine alone.[170] Its automated proliferation ultimately affected organizations across sixty-five countries,[171] including targets in Russia such as the state-owned oil company Rosneft.[172] NotPetya's speed and apparent success in producing intense effects suggest that Sandworm successfully bypassed the subversive trilemma. But I show that this cyber operation confirms H4, because the increase in speed and intensity of effects correlate with a decrease in control. The hackers could neither predict nor control NotPetya once they had set it in motion. Days before NotPetya's automated proliferation and encryption was activated on infected computers, M.E.Doc had sent another clean update to its customers, which Anton Cherepanov suggests was "an unexpected event for the attackers."[173] It is exceedingly unlikely that Sandworm could map the near-instantaneous spread of NotPetya across hundreds of thousands of systems just a few weeks later.[174] Forensic evidence indicates that Sandworm had "underestimated the malware's spreading capabilities," which then "went out of control."[175] The result was significant collateral damage.

NotPetya's economic disruption decreased Ukraine's gross domestic product (GDP) by approximately 0.5 percent in 2017, which shifted the balance of

168. David Maynor et al., "The MeDoc Connection," *Talos* blog, Cisco, July 5, 2017, http://blog.talosintelligence.com/2017/07/the-medoc-connection.html; and Anton Ivanov and Orkhan Mamedov, "ExPetr/Petya/NotPetya Is a Wiper, Not Ransomware," *Securelist* blog, AO Kaspersky Lab, June 28, 2017, https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/.

169. Johnson, "On Drawing a Bright Line for Covert Operations," p. 286.

170. This estimate by an anonymous expert at a leading cybersecurity vendor in Ukraine is based on the number of compromises he observed personally while involved in mitigation efforts at multiple large enterprises in Ukraine. Author interview with anonymous cybersecurity expert, Kyiv, April 19, 2018.

171. Author interview with anonymous government advisor.

172. "Maersk, Rosneft Hit by Cyberattack," *Offshore Energy*, June 28, 2017, https://www.offshore-energy.biz/report-maersk-rosneft-hit-by-cyberattack/.

173. Anton Cherepanov, "Analysis of TeleBots' Cunning Backdoor," *WeLiveSecurity* blog, ESET, July 4, 2017, https://www.welivesecurity.com/2017/07/04/analysis-of-telebots-cunning-backdoor/.

174. Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar."

175. Cherepanov, "TeleBots Are Back."

power in Russia's favor and provided it with independent strategic utility.[176] Unlike Sandworm's previous cyber operations, NotPetya was prominently reported in Ukrainian media.[177] Leaders from Ukraine, the United States, the United Kingdom, and Australia condemned Russia for the destructive cyber operation, underlining its significance.[178] Yet, I argue that NotPetya's loss of control indicates the scale of its impact was accidental and produced unintended consequences. The United States imposed sanctions against Russia, particularly the GRU leadership. The U.S. Department of Justice subsequently indicted six GRU officers for deploying destructive malware.[179] These significant unforeseen costs reduce NotPetya's overall strategic utility and confirm the expected constraining influence of the subversive trilemma. More importantly, despite its scale, NotPetya did not measurably contribute to Russia's goals: Ukraine maintained its pro-EU course.

BADRABBIT (2017). When developing NotPetya's successor, BadRabbit, Sandworm used the same technique of disabling targets through encryption, but they added efforts to control its spread and effects. Consequently, it achieved no measurable strategic utility. As predicted by H3, the increase in control decreased intensity and speed. Moreover, I argue that BadRabbit offered little, if any, strategic utility to Russia because the cyber operation only spread to a small number of targets. Its strategic irrelevance provides further support for my hypothesis that the subversive trilemma is a limiting factor.

176. Igor Burdiga, "'Chornyy vivtorok' ukrayins'koho IT: yakykh zbytkiv zavdala kiberataka, ta khto yiyi vchynyv" ["Black Tuesday" of Ukrainian IT: What damage was caused by the cyberattack, and who committed it], *Hromadske*, July 8, 2017, https://hromadske.ua/posts/naslidki-kiberataki.

177. "SBU predupredyla khakerskuyu ataku Rossyyskykh Spetssluzhb na énerhoob'ekty Ukrayny—112 Ukrayna" [SBU prevented hacker attack of Russian Special Services on power facilities of Ukraine—112 Ukraine], *112.ua*, December 28, 2015, https://web.archive.org/web/20160303172015/https://112.ua/kriminal/sbu-predupredila-hakerskuyu-ataku-rossiyskih-specsluzhb-na-energoobekty-ukrainy-281811.html; "Ochil'nyk SBU rozpoviv pro motyv khakeriv, yaki atakuvaly Ukrayinu virusom Petya" [The head of the SBU spoke about the motive of the hackers who attacked Ukraine with the Petya virus], *TSN*, July 4, 2017, https://tsn.ua/ukrayina/ochilnik-sbu-rozpoviv-pro-motiv-hakeriv-yaki-atakuvali-ukrayinu-virusom-petya-955817.html; and "Pidsumky 2017 roku: Nayhuchnishi vbyvstva v Ukrayini" [Results of 2017: The loudest murders in Ukraine], *24tv.ua*, December 5, 2017, https://24tv.ua/news/showNews.do?pidsumki_2017_roku_v_ukrayini_vbivstva_2017&objectId=895499.

178. Mark Landler and Scott Shane, "U.S. Condemns Russia for Cyberattack, Showing Split in Stance on Putin," *New York Times*, February 15, 2018, https://www.nytimes.com/2018/02/15/us/politics/russia-cyberattack.html; and "Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks," *U.S. Department of the Treasury*, March 15, 2018, https://home.treasury.gov/news/press-releases/sm0312.

179. U.S. Department of Justice (DOJ) Office of Public Affairs, *Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace* (Washington, D.C.: DOJ, October 19, 2020), https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

BadRabbit does not appear to be linked to Russia's diplomatic or military initiatives, providing further evidence of the expected independent strategic role of cyber operations. Prior to BadRabbit, the EU-Ukraine Association Agreement entered into full force on September 1, 2017, marking Russia's failure to reverse Ukraine's foreign policy course. Forensic evidence indicates that Sandworm started to develop BadRabbit around September 2016.[180] As the subversive trilemma would predict, increasing control affected BadRabbit's operational speed. Hackers took twelve months to develop BadRabbit compared with only six months for NotPetya. BadRabbit and NotPetya used largely the same code and both cyber operations encrypted data on affected systems before displaying a ransom demand.[181] But Sandworm attempted to "improve upon previous mistakes" by making encryption reversible on BadRabbit and using a manually rather than automatically spreading mechanism.[182] Victims who visited compromised websites (so-called watering holes) manually clicked on "OK/install" when the site offered users fake Adobe Flash Player updates that contained malware.[183]

BadRabbit pursued the same effect type (i.e., economic disruption, or rung nineteen on Johnson's escalation ladder) as NotPetya, but at a fraction of the scale and significantly less intensity. Like NotPetya, it appears that BadRabbit mostly targeted businesses' computer systems, especially banks and media firms but also transport providers. When BadRabbit encrypted compromised systems on October 24, 2017, however, it only affected approximately 200 targets in Russia, Ukraine, Turkey, and Germany.[184] Curiously, most victims (65 percent) were in Russia,[185] whereas 75 percent of NotPetya's targets were in Ukraine.[186] Yet, Sandworm only targeted Ukraine's critical infrastructure.

180. Yonathan Klijnsma, "Down the Rabbit Hole: Tracking the BadRabbit Ransomware to a Long Ongoing Campaign of Target Selection," *RiskIQ*, October 25, 2017, https://www.riskiq.com/blog/labs/badrabbit/.
181. John Leyden, "Hop On, Average Rabbit: Latest Extortionware Menace Flopped," *Register*, October 26, 2017, https://www.theregister.co.uk/2017/10/26/bad_rabbit_post_mortem/; and Orkhan Mamedov, Fedor Sinitsyn, and Anton Ivanov, "Bad Rabbit Ransomware," *Securelist* blog, AO Kaspersky Lab, October 24, 2017 (updated October 27, 2017), https://securelist.com/bad-rabbit-ransomware/82851/.
182. Hasherezade, "BadRabbit: A Closer Look at the New Version of Petya/NotPetya," *Malwarebytes Labs*, October 24, 2017 (updated July 16, 2021), https://blog.malwarebytes.com/threat-analysis/2017/10/badrabbit-closer-look-new-version-petyanotpetya/.
183. Maynor et al., "The MeDoc Connection"; and Eduard Kovacs, "Bad Rabbit Linked to NotPetya, but Not as Widespread," *SecurityWeek*, October 25, 2017, https://www.securityweek.com/bad-rabbit-linked-notpetya-not-widespread.
184. Mamedov, Sinitsyn, and Ivanov, "Bad Rabbit Ransomware."
185. Marc-Etienne M.Léveillé, "Bad Rabbit: Not-Petya Is Back with Improved Ransomware," *WeLiveSecurity* blog, ESET, October 24, 2017, https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/.
186. Burdiga, "Chornyy vivtorok ukrayins'koho IT."

More importantly, forensic evidence shows that critical infrastructure targets were not infected through the malicious Flash Player, indicating that Sandworm "already had a foot inside their [Ukrainian targets] network and launched the watering hole attack at the same time as a decoy."[187]

Consistent with the subversive trilemma, BadRabbit's improved control over the spread of the malware and its effects came at the cost of low speed and low intensity. There are no indications of premature discovery, nor of prior operational missteps that could have compromised the effects. BadRabbit neither auto-proliferated nor produced any significant collateral damage.[188] The available evidence suggests that BadRabbit caused temporary, reversible, and inconsequential disruptions.[189] It received minimal media coverage both within Ukraine and abroad, while Ukraine's newly established "cyberpolice" attributed the operation to "criminals" rather than political operatives.[190] Consequently, BadRabbit neither contributed toward Russia's strategic goals nor shifted the balance of power. Tellingly, since BadRabbit, Sandworm has abandoned any attempts at active effects cyber operations against Ukraine, returning to a focus on pure espionage.[191]

Alternate Explanations for the Lack of Strategic Utility

Because the decision-making processes of the Kremlin and the Russian intelligence agencies who almost certainly sponsored the cyber operations discussed remain inaccessible, alternate interpretations concerning the intentions behind their use abound. This section addresses two alternative interpretations: signaling and experimentation.

The first alternative interpretation holds that Russia deployed cyber operations primarily as signaling tools. Signaling is the core mechanism in coercive diplomacy, in which actors demonstrate and deploy capabilities to signal re-

187. M.Léveillé, "Bad Rabbit."
188. Eduard Kovacs, "Files Encrypted by Bad Rabbit Recoverable without Paying Ransom," *SecurityWeek*, October 27, 2017, https://www.securityweek.com/files-encrypted-bad-rabbit-recoverable-without-paying-ransom.
189. Leyden, "Hop On, Average Rabbit"; and "Kiev Metro Hit with a New Variant of the Infamous Diskcoder Ransomware," *WeLiveSecurity* blog, ESET, October 24, 2017, https://www.welivesecurity.com/2017/10/24/kiev-metro-hit-new-variant-infamous-diskcoder-ransomware/.
190. Cyberpolice of Ukraine, "Kiberpolitsiya rozpovila podrobytsi diyi virusu-shyfruval'nyka 'BadRabbit' (FOTO)—Departament Kiberpolitsiyi" [Cyberpolice tells details of BadRabbit encryption virus (PHOTOS)—Cyberpolice Department], October 25, 2017, https://cyberpolice.gov.ua/news/kiberpolicziya-rozpovila-podrobyczi-diyi-virusu-shyfruvalnyka-badrabbit-foto-2732/.
191. Sandworm's last recorded activity in Ukraine was in October 2018. Anton Cherepanov and Robert Lipovsky, "New TeleBots Backdoor: First Evidence Linking Industroyer to NotPetya," *WeLiveSecurity* blog, ESET, October 11, 2018, https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/.

solve and induce adversary actions.[192] Effective signals have a clear recipient and content, neither of which is the case regarding the five cyber operations that I examine in this article. For example, one interpretation of the two power grid sabotage cyber operations holds that, "Russia is using cyber intrusions to signal the risk of escalation in a crisis" to its rivals (i.e., the United States and NATO).[193] Joseph S. Nye Jr., in contrast, speculates that Russia is signaling to Ukraine, "reminding Ukraine of its vulnerability in a hybrid war with a different level of plausible deniability."[194] Similarly, one interpretation of NotPetya suggests it was "designed to send a political message: if you do business in Ukraine, bad things are going to happen to you."[195] A second interpretation sees Russia "demonstrating its ability to disrupt faith in public institutions."[196] These interpretations are plausible, and so are many others, yet there is little tangible evidence to support them.[197] Ultimately, the existence of multiple interpretations indicates that the signal is unclear. More importantly, even if signaling was the intent, it does not challenge my findings on the limiting role of the subversive trilemma.

The second alternate explanation suggests that Russia deployed cyber operations primarily to test and develop its capabilities. A Dragos report about the power grid sabotage operation in 2016 noted that it was "more of a proof of concept than what was fully capable."[198] Ben Buchanan picks up this point, suggesting that Sandworm perhaps wanted to "see how the code worked in practice so they could refine it for future use," and he quotes Dragos's CEO Robert M. Lee warning of the potential threat to critical infrastructure around the world.[199] There are three key issues with this interpretation. First, it is highly unlikely that an actor will spend years developing a capability and deploy it without pursuing any strategic gains. Moreover, doing so risks losing the capability by allowing potential future victims to remove the vulnerabili-

192. Schelling, *Arms and Influence*.
193. Benjamin Jensen and J.D. Work, "Cyber Civil-Military Relations: Balancing Interests on the Digital Frontier," *War on the Rocks* blog, September 4, 2018, https://warontherocks.com/2018/09/cyber-civil-military-relations-balancing-interests-on-the-digital-frontier/.
194. Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security*, Vol. 41, No. 3 (Winter 2016/17), p. 49, doi.org/10.1162/ISEC_a_00266.
195. Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2010, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
196. Brandon Valeriano, Ryan C. Maness, and Benjamin Jensen, "Cyberwarfare Has Taken a New Turn. Yes, It's Time to Worry," *Monkey Cage* blog, *Washington Post*, July 13, 2017, https://www.washingtonpost.com/news/monkey-cage/wp/2017/07/13/cyber-warfare-has-taken-a-new-turn-yes-its-time-to-worry/.
197. See section 5 of the online appendix, doi.org/10.7910/DVN/IZ65MC.
198. Dragos, *Crashoverride*, p. 11.
199. Buchanan, *The Hacker and the State*, pp. 204–205.

ties it exploits. In the words of Lee, "it would be extraordinarily weird to stage an entire attack as just a proof of concept."[200] Second, there is no empirical evidence supporting this interpretation. Sandworm has not used this toolset again, nor has it pursued other critical infrastructure sabotage using similar methods. Significantly, forensic analysis by Symantec showed that the 2017 intrusions in the U.S. energy grid attributed to Russia were the work of a different actor and shared no tools or techniques.[201] Third, the "proof of concept" interpretation ultimately suggests that cyber operations are instruments of future higher-stakes conflict. Yet as the analysis shows, despite multiple years of experimentation and testing, Sandworm did not overcome the subversive trilemma.

Conclusion

This article has argued that cyber operations are an instrument of subversion whose operational effectiveness is constrained by a subversive trilemma. The demands of the mechanism of secret exploitation that cyber operations rely upon result in actors facing trade-offs between improving either speed, intensity, or control of operations. Increasing the effectiveness of one variable tends to decrease the others. In most circumstances, cyber operations thus tend to be too slow, too low in intensity, or too unreliable to contribute to political goals or shift the balance of power. Consequently, cyber operations tend to fall short of their strategic promise and deliver limited utility. The case study of the Russo-Ukrainian conflict provides strong support for this theory. All five cyber operations that I examine in this article showed clear evidence of the constraining role of the trilemma.

This theory has several implications for the study of cyber conflict. Most importantly, the subversive trilemma significantly hinders the ability of cyber operations to successfully produce independent strategic utility. Success requires alleviating the trilemma without raising costs above those of potential diplomatic or military alternatives. Specifically, effects must be sufficiently intense to contribute to a given goal, while the operation must produce these effects within a timeframe that is short enough to avoid discovery but long enough to increase the likelihood of both achieving the intended effects and avoiding un-

200. Author communication with Robert Lee via online messaging service, February 25, 2021.
201. Threat Hunter Team, "Dragonfly: Western Energy Sector Targeted by Sophisticated Attack Group," *Broadcom* blog, *Symantec Enterprise Blogs: Threat Intelligence*, October 20, 2017, https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks; and Andy Greenberg, "Your Guide to Russia's Infrastructure Hacking Teams," *Wired*, July 12, 2017, https://www.wired.com/story/russian-hacking-teams-infrastructure/.

intended consequences. Furthermore, it requires conditions for success that are rarely present: the availability of systems that control social, economic, or physical processes of strategic significance, yet also contain vulnerabilities that operators can exploit without premature detection. Finally, long development time involving highly skilled operators is expensive; the more intense, physical effects an operation pursues, the less favorable the cost-benefit ratio is likely to be.[202] Moreover, even under ideal conditions, the potential effect on the balance of power is still likely marginal.

Cyber operations are most likely to deliver on their strategic promise in two scenarios. The first scenario is long-term, low-stakes competition between adversaries with a significant power differential. Although most of the conditions above are present in Ukraine, the deployment of multiple cyber operations did not measurably contribute to Russia's strategic goals. Hence, it likely requires decades to develop a successful cyber operation, which makes it difficult to isolate the operation's influence in order to measure its effects. Importantly, the most significant power shift that traditional subversion can achieve is regime change. Cyber operations alone are likely incapable of such effects. Accordingly, cyber operations are most likely to deliver utility if they are integrated with traditional subversion.[203]

The second scenario is high-stakes competition among nuclear-armed peer competitors that expect eventual military confrontation. The tensions between the United States and China are a key example. Potential nuclear escalation renders the risks and costs of using conventional force unacceptably high. Although the subversive trilemma suggests an unfavorable cost-benefit ratio for cyber operations that pursue highly intense effects at the operational level, strategic benefits may still outweigh these costs. The party in a "domain of losses" is especially likely to be more risk-accepting, and thus more likely to accept the limits of control.[204] If states use cyber operations to target military assets for sabotage, cross-domain effects indicate potential inadvertent escalation risks.[205] Because cyber operations can likely achieve only marginal changes to the balance of power over longer-term competition, they are only likely to make a difference when both actors are closely matched and neither side exhibits exponential growth rates.

202. Slayton, "What Is the Cyber Offense-Defense Balance?"
203. The Grugq, "A Short Course in Cyber Warfare," keynote at Black Hat Asia 2018 conference, Marina Bay Sands, Singapore, YouTube, April 10, 2018, https://www.youtube.com/watch?v=gvS4efEakpY.
204. Amos Tversky and Daniel Kahneman, "The Framing of Decisions and the Psychology of Choice," *Science*, January 30, 1981, p. 453.
205. Erik Gartzke and Jon R. Lindsay, "Thermonuclear Cyberwar," *Journal of Cybersecurity*, Vol. 3, No. 1 (March 2017), pp. 37–48, doi.org/10.1093/cybsec/tyw017.

In lower stakes, nonnuclear dyads, capable states can be expected to regularly employ cyber operations even though they have a high failure rate, as has been the case historically with traditional subversion.[206] For the same reason, however, their impact on security competition should not be overestimated because their strategic utility remains limited, barring "unicorn" scenarios in which all favorable conditions align and the subverting actor is extremely lucky.

Three major policy implications follow from this argument. First, it confirms the current shift away from a strategy of cyber deterrence rooted in theories of warfare, whose aim is to avoid costly engagements.[207] Second, alternative emerging strategies of "persistent engagement" and "defend forward" that guide U.S. posture should consider the subversive trilemma as a limiting factor to avoid unintended consequences.[208] These new strategies build on assumptions of cyber revolution theory, and they aim to maximize the utility of cyber operations as instruments of low-intensity strategic competition while minimizing risks by participating in "agreed competition" that adheres to a set of tacit rules of engagement.[209] The findings of this study, however, suggest that the subversive trilemma is the more likely explanation for the observed low intensity of competition. By pursuing more aggressive engagement, the United States may shift adversary cost-benefit calculi toward more risk-taking, such as increasing effects intensity at the cost of control, which inadvertently intensifies cyber competition.[210] Finally, persistence is a key requirement for actors to succeed in exploiting targets. Yet, long-term planning, reconnaissance, and stealth as well as space for creative development are just as if not more important to maximize effectiveness and utility of cyber operations. Privileging persistence, as the current strategy does, risks neglecting these requirements for success. Conversely, defenders in cyber conflict can benefit from exploiting the trilemma and exacerbating its constraining role on adver-

206. O'Rourke, *Covert Regime Change*, p. 8.
207. *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command* (Fort George G. Meade, Md.: U.S. Cyber Command, 2018), https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.
208. Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation," *Cyber Defense Review* (2019), pp. 267–287, https://www.jstor.org/stable/26846132; and Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Force Quarterly*, Vol. 92, No. 1 (2019), pp. 10–14, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_10-14_Nakasone.pdf.
209. Michael P. Fischerkeller and Richard J. Harknett, "Through Persistent Engagement, the U.S. Can Influence 'Agreed Competition,'" *Lawfare* blog, April 15, 2019, https://www.lawfareblog.com/through-persistent-engagement-us-can-influence-agreed-competition.
210. Lennart Maschmeyer, "Persistent Engagement Neglects Secrecy at Its Peril," *Lawfare* blog, March 4, 2020, https://www.lawfareblog.com/persistent-engagement-neglects-secrecy-its-peril.

sary operations. Defensive strategies should prioritize the capacity to detect and neutralize intrusions. If immediate neutralization is impossible, defensive measures should aim to slow adversary speed, limit their control, and maximize the barriers that adversaries must overcome to achieve or intensify effects. The same principles should guide systems design, as well as security rules and practices. Existing counterintelligence strategies provide a useful basis to develop such strategies.

Furthermore, while this study has focused on the utility of cyber operations as independent strategic instruments, its findings also apply to their use as complements to other instruments of power. Just like traditional subversive operations have been deployed to contribute to military goals, such as undermining command structures, so can cyber operations.[211] Regardless of strategic context, any cyber operation that produces effects through hacking relies on the subversive mechanism and is thus bound by its trilemma.[212] Consequently, the trilemma can be expected to apply across multiple strategic contexts.

To verify this theory, further research tracking evidence of the subversive trilemma in varying strategic contexts and by different actors is required. Findings from this study supported H2, H3, and H4, but the cases examined did not produce the configuration of the trilemma predicted by H1. Quantitative research verifying the predicted correlations across a larger universe of cases will be especially useful. Second, historical comparative research is needed to verify the proposition that the quality of subversion has not changed despite the technological advances of the information revolution. In this regard, the integration of cyber operations with traditional subversion is a key topic of interest. While this study has focused on hacking, assessing the impact of new technology on effectiveness and utility requires more empirical examinations of another key instrument of subversion: influence operations that use disinformation and propaganda.

Finally, looking ahead, changes in design features of ICTs may alter the subversive trilemma. The most likely change is simplification and standardization in cyber-physical systems[213] and the rise of the Internet of Things (IoT),[214]

211. Miklós Kun, *Prague Spring, Prague Fall: Blank Spots of 1968*, trans. Hajnal Csatorday (Budapest: Akadémiai Kiadó, 1999), p. 151.
212. There are some exceptions, such as Distributed Denial of Service attacks or Ransomware, yet these are of low relevance in interstate competition.
213. Borja Bordel et al., "Cyber-Physical Systems: Extending Pervasive Sensing from Control Theory to the Internet of Things," *Pervasive and Mobile Computing*, Vol. 40 (September 2017), pp. 156–184, doi.org/10.1016/j.pmcj.2017.06.011.
214. IoT refers to physical devices that have sensors that are linked to the Internet. Philip N. Howard, *Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up* (New Haven, Conn.: Yale University Press, 2015).

which could make it easier for cyber operations to produce physical effects at scale. This change could increase cyber operations' intensity and potential to affect the balance of power, but the perils of losing control over an operation would still exist. Similarly, advances in artificial intelligence may improve control over scale-maximizing operations by facilitating computer network mapping and command-and-control functions.[215] Defenders in cyber conflict (i.e., administrators of computer systems being targeted by cyber operations), however, would likely benefit as well because artificial intelligence promises superior means of detecting exploitation.[216] Consequently, the trilemma will likely remain relevant.

215. See, for example, Zhong Liu et al., "Cyber-Physical-Social Systems for Command and Control," *IEEE Intelligent Systems*, Vol. 26, No. 4 (July/August 2011), pp. 92–96, doi.org/10.1109/MIS.2011.69.

216. Fan Liang et al., "Machine Learning for Security and the Internet of Things: The Good, the Bad, and the Ugly," *IEEE Access*, Vol. 7 (2019), pp. 158126–158147, doi.org/10.1109/ACCESS.2019.2948912.