Clausewitz's Perspective on Deterring Russian Malign Activities in Cyberspace

Lt. Col. Jon V. Erickson, U.S. Army Reserve

In mid-December 2020, Russia was discovered to have pulled off one of the biggest espionage hacks in the world when FireEye, a cybersecurity firm, disclosed that it had suffered an intrusion. FireEye determined that Russian threat actors who compromised the SolarWinds' Orion platform conducted the intrusion. The "hack resulted in attackers reading the email communications at the U.S. Treasury and Commerce departments."[1]

Some questions raised have revolved around why the U.S. Department of Homeland Security's EINSTEIN program was unable to catch these threat actors. Created in 2003, the program provides an automated process to collect, correlate, analyze, and share security information across the federal government.[2] Others have asked why the U.S. Cyber Command's (USCYBERCOM) Defend Forward strategy was unable to identify or detect this activity. While these kinds of questions are helpful for reexamining the U.S. government's assumptions, tactics, and strategies for defending its data, infrastructure, and personnel, it may be more helpful to start with two fundamental questions: What are Russia's political objectives? How does this cyber operation support those objectives?

Carl von Clausewitz's *On War* provides a strong reason for understanding an adversary's political objective. He states that "the political object—the original motive for war—will thus determine both the military objective to be reached and the amount of effort it requires."[3] This article will leverage Clausewitz's insights on expenditure of effort, political repercussions, friction, and people's war to provide a lens through which senior leaders can direct or guide operations in cyberspace in a way that is integrated with operations in other domains in order to conduct multi-domain operations. Additionally, understanding Russia's political objectives with the SolarWinds compromise will allow military strategists to provide a tailored approach to disrupt, deny, degrade, or deter future Russian actions in cyberspace against the United States and its allies.

Russia's Worldview

Before attempting to understand Russia's political objectives with the SolarWinds hack, it is first important to recognize that Russia believes it is at war with the West. Russia views the current U.S.-led international order as posing an existential threat to Russian national interests. One example is the expansion of the North Atlantic Treaty Organization (NATO). While the United States views NATO's strategic role as a stabilizing force throughout the Eurozone, Russia sees NATO's expansion as encirclement and "reflect[s] both real concerns about losing influence in its near abroad and paranoia of a NATO invasion facilitated by NATO's growing military presence on Russia's borders."[4]

Feeding Russian suspicions about NATO's role in the democratization of former Soviet satellite countries were the preceding color revolutions and subsequent NATO membership requests. While the West celebrated these pro-democracy protests for leading to newly democratic states, Russia viewed these color revolutions in its sphere

Next page: A widely circulated meme loosely depicting Russian President Vladimir Putin in the likeness of Prussian General Carl von Clausewitz. Clausewitz is widely respected as a military theorist who described in sophisticated detail the necessary connection between properly conceived acts of war and successfully achieving specific political objectives. (Image courtesy of BakeNecko via Wikimedia Commons)

of influence as "Western-organized coups designed to subvert the legitimate authorities."[5] Additionally, whereas the United States believes in the free flow of information as a major bedrock principle of Western democracies, Russia believes that the United States is conducting a sophisticated information operations campaign against Russia—exposing corruption, nepotism, and abuse of power—"to destabilize the Russian government and political system."[6] Given NATO encirclement and U.S. information warfare, Russia believes it is at war with the West, in particular the United States and NATO, and must overturn the U.S.-led international order.

From the Kremlin's viewpoint, the United States is employing a new form of warfare against Russia in which "long-distance, contactless actions against the enemy are becoming the main means of achieving combat and operational goals."[7] Russia's lesson learned from these color revolutions is that the ability to mobilize a local population to take action under the influence of a foreign power can be just as effective as the foreign power taking military action itself. Gen. Valery Gerasimov, chief of the General Staff of the Armed Forces of the Russian Federation, has stated that in this new form of warfare, "he would consider economic and non-military government targets fair game."[8] This last statement provides an explanation as to why Russian threat actors believe they are justified in hacking businesses used by the U.S. government such as SolarWinds. This begs the question, in support of what political objectives?

Russian Grand Strategy

Russia's grand strategy is to replace the United States as the lone hegemonic power with a multipolar world composed of several power centers, with Russia as one of those powers. Russian "ends" can be broken into three key objectives: exclusive sphere of influence, recognition of and treatment as a great power, and constraint of U.S. global influence.[9] The key objective of Russian grand strategy is to reestablish its own exclusive sphere of influence where it is able to impose control within its near abroad with little interference from outside powers.

In Russia, preserving Vladimir Putin's power and reestablishing the Russian sphere of influence are very much intertwining interests. When Putin returned to the presidency for a second time in 2012, mass protests greeted him across Russia. This "reinforced his fears of externally-supported opposition as a threat to his rule."[10] As a result, whether it is due to Putin's personal fear of threats to his rule or due to the country's deep-seated geopolitical insecurity, the Kremlin sees constraining U.S. influence as setting conditions that allows Russia to regain its status as a power center in Eurasia.

Reflecting on U.S. actions, Gerasimov wrote, "The scale of the casualties and destruction, the catastrophic social, economic, and political consequences, such new-type conflicts are comparable with the consequences of any real war."[11] Russia's view is that "warfare is more than a simply armed conflict, it's rather the combination of military and non-military means, the result of which is that for each specific tactical objectives and war theater, a different strategy is needed. For example, the tactical base for Ukraine is Low-Intensity Conflict, while in Georgia it was more like conventional linear tactics."[12]

Clausewitz on Russia

In light of Gerasimov's statement, Clausewitz's tenets provide a relevant lens to view how Russia plans to achieve its grand strategy. Gerasimov believes "frontal engagements of large formations of forces at the strategic and operational level are gradually becoming a thing of the past."[13] By utilizing Clausewitz's thought to minimize its expenditure of effort, Russia is pursuing a grand strategy that increases the likelihood of success without requiring defeat of its adversary in battle. Additionally, a student of Clausewitz would also pursue objectives "that have *direct political repercussions*, that are designed in the first place to disrupt the opposing alliances, or to paralyze it, that gain [Russia] new allies, favorably affect the political scene, etc. … [to] form a much shorter route to the goal than the destruction of the opposing armies."[14] Clausewitz posits that if the expenditure of efforts exceeds the political objective, then peace must follow.

Next page: Russian President Vladimir Putin has reputedly used nonstate hackers and other criminal elements to disrupt and degrade U.S. government institutions including the military, private industry, and economic institutions. Collectively, these efforts are weakening the United States' power and influence on the world stage. These same illicit entities have attacked and undermined the governments and economies of Western Europe as well as states that were formerly part of the Soviet Union. (Graphic elements courtesy of Etienne Marais, www.pexels.com; zlatko_plamenov and starline, www.freepik.com. Composite graphic by Arin Burgess, Army University Press)

These efforts can be seen in Russian attacks against Estonia, Georgia, and Ukraine.

To increase the likelihood of achieving its grand strategy of creating a multipolar world, Russia leverages the diplomatic and information instrument of power "to bring about a gradual exhaustion of [the West's] physical and moral resistance."[15] What has amplified the effectiveness of these nonkinetic instruments of power is the cyber domain. Not only has cyberspace provided Russian threat actors the means to penetrate a foreign nation's infrastructure but also influence its population. So far, the risks and costs to Russia of continuing its malign activities are not enough to outweigh the perceived gains. A potential strategic gain relating to Russia's SolarWinds hack is to diminish U.S. influence by making other governments question how the United States can protect them if the United States cannot even protect its own critical infrastructure.

One reason there are more theories than facts to explain the reason for Russian hacking is summarized by Jeremy Hunt, the United Kingdom's foreign secretary, who said, "These cyber attacks serve no legitimate national security interest, instead impacting the ability of people around the world to go about their daily lives free from interference, and even their ability to enjoy sport …. The [Russian] GRU's actions are reckless and indiscriminate."[16] While it is reasonable to assume that Russian malign activities may not serve a strategic purpose, Clausewitz warns not to think of actions as indiscriminate. By "ignoring the fact that they are links in a continuous chain of events, we also ignore the possibility that their possessions may later lead to definite disadvantages" that constrain U.S. global influence.[17]

Russian tactics may instead be introducing the element that Clausewitz calls "friction" to weaken the capacity of international and government institutions to respond to Russian aggression.

The combination of Russian foreign policy to provide strategic chances to achieve its interests and gray-zone activities to introduce friction are acting in concert to undermine the functioning of democratic institutions that then leads rivals to perceive Russia as attaining global power status. While friction can be overcome, Clausewitz warns of the danger of friction when it encounters chance, as chance is what "makes everything more uncertain and

> Understanding that Russia's most likely political objective with the SolarWinds hack is part of continued Russian efforts to constrain U.S. influence, efforts to disrupt, deny, degrade, or deter future Russian actions must keep this political objective in mind.

interferes with the whole course of events."[18] By introducing friction coupled with chance, the Russians are creating opportunities where "countless minor incidents—the kind you can never really foresee" gradually wear down their adversaries to produce decisive results.[19] Russian gray-zone tactics places people as the center of gravity as part of an effort to generate those chances. Thus, a large part of Russia's calculation rests on its ability to influence "the character of the people and the government, the nature of the country, and its political affiliations."[20] With the SolarWinds breach, the Russian government may be looking to create doubts among the U.S. population about its own government's ability to protect its infrastructure, to have both Congress and the military spending resources to determine the extent of the hack and potentially rebuild networks, to introduce cybersecurity measures that assure the integrity of the data but at the cost of slowing down the military decision-making process, or all of the above. By introducing friction wherever possible, Russia is introducing a "force that makes the apparently easy so difficult" and creates chances that favor accomplishing Russian objectives.[21]

The SolarWinds hack is an operation that is tied most closely to another Russian means to achieve its political objective and that is to brandish its cyberattack capabilities as another form of power. As Clausewitz states, "When one force is a great deal stronger than the other … there will be no fighting; the weaker side will yield at once."[22] Thus, Russia may in fact secretly desire to be unmasked "and hope it is passed forward to national decisionmakers … [to] force the target to recalculate its correlation of forces against the attacker."[23] By demonstrating its capabilities, Russia is posing a dilemma upon the West. Slow down or stop the acceptance of new NATO members such as Ukraine or Georgia; alternatively devote substantially more resources towards strengthening the resiliency of its members to resist and recover from hybrid or armed attack. Case in point, when Ukraine sought integration with NATO, Russia annexed Crimea. Ukraine must now deal with irregular forces that seek to create conditions that further favor Russian political objectives while NATO determines an appropriate response. Russia's success in Ukraine sends a signal to countries in Russia's near abroad that the NATO, and indirectly the United States, security umbrella may not be enough to deter Russian actions, leading these countries to rethink their political alignments.

Another way for Russia to achieve its political objective of constraining U.S. influence globally is to use the hacks to sow suspicion and fear about an open internet, which undermines U.S.-led conversations around information security to instead conform more closely to Russia's information security doctrine. During the Cold War, Putin saw how Western countries could influence the local population by broadcasting into Soviet territory and today sees similar results with recent pro-democracy color revolutions.[24] The Kremlin may see the United States attempting to do the same against Putin's regime by exposing corruption, nepotism, and abuse of power, which motivates the Kremlin's desire to control information distribution within Russia. Therefore, by executing cyber operations such as SolarWinds, Russia may be creating conditions where other countries may call for the creation of international laws on information security that may align more closely to Russian desire for a more closed off internet. Not only could this insulate

Russia from real or imagined threats, but it could also create international digital rules of engagement that will limit the ability of the United States to threaten Russia or those in Russia's perceived sphere of influence.

Understanding that Russia's most likely political objective with the SolarWinds hack is part of continued Russian efforts to constrain U.S. influence, efforts to disrupt, deny, degrade, or deter future Russian actions must keep this political objective in mind. Countering Russian aggression or provocation will require all national instruments of power-diplomatic, information, military, and economic. While recognizing that the full levers of national power must be exercised to counter Russian aggression, the rest of this article is limited to actions that the United States can employ in cyberspace as part of a broader military strategy.

Defending Forward

Before starting down the road of taking military action, leaders need to understand that misperception and miscalculation are two major risks in cyberspace. In any domain, especially in cyber, deciphering intent and attributing actions are two difficult issues to tackle. The definition of attribution can be many things—a machine, a location, the person who pressed the keys, the organization that supports the person, the person's motivation, and more—but also carries a certain amount of uncertainty such as the possibility of misdirection. The same can be said with miscalculating whether an intent was malicious, in self-defense, or somewhere in between. Taking action prematurely based on false information "is as likely to lead to ill-timed action as to ill-timed inaction and is no more conducive to slowing down operations than it is to speeding them up."[25] This leads into the crux of the issue when it comes to developing a military strategy for cyberspace.

The main issue is that "it is estimated that up to 90 per cent of the infrastructure that compromises cyberspace is privately owned, with the remaining 10 per cent or so owned by governments."[26] This is problematic with regard to what actions the military or any government organization can legally take in cyberspace. Therefore, USCYBERCOM's Defend Forward strategy must be one of many tools that the U.S. government employs in its efforts to counter Russian malign activities in cyberspace. Given that cyberspace is essential for nearly every basic function of modern society, the U.S. military must be careful of gray-zone encroachment where the United States attempts a Sisyphean effort to turn the neutral and open internet into either blue or red space.

To achieve Russian political objectives, several elements of Russian gray-zone activities utilize what Clausewitz called "the people's war" to create the conditions for regime change. He states that "any nation that uses it intelligently will, as a rule, gain some superiority over those who disdain its use."[27] For too long, Russia was one of a small group of countries to strategically harness this element of warfighting because Russia had a much broader definition of war. In contrast, the United States and other Western countries had a dichotomous definition of either being at war or not. However, the U.S. *2021 Interim National Security Strategic Guidance* remedies this by recognizing the need to compete across the spectrum of conflict to deter gray-zone actions.[28] This need for the United States to compete and win in activities below the level of armed conflict lends itself well to an important Clausewitzian thought that USCYBERCOM is beginning to deploy with its Defend Forward strategy.

Clausewitz's concept of a people's war does not have to be limited to the Russian use of overthrowing or compelling regime change. It can also be a tool to deter Russian aggression toward NATO allies and other European partners, as well as other countries in its near abroad. Further building upon Clausewitz's thought on waging a people's war, the United States and its allies could employ state (such as other government organizations) and nonstate actors (e.g., contractors) in cyberspace, "not [to] be employed against the main enemy force … [but] to operate in areas just outside the theater of war—where the invader will not appear

Lt. Col. Jon V. Erickson, U.S. Army Reserve, is a cyber and signal officer serving as the brigade S-3 for the 505th Theater Tactical Signal Brigade. He holds a bachelor's degree from the United States Military Academy, a master's degree in information technology from the University of Maryland University College, an MBA from the University of California-Los Angeles, and is attending the Army War College. His previous assignments include battalion commander in the Army Reserve Cyber Protection Brigade and deputy chief of staff, G-6, for the 79th Theater Sustainment Command. Erickson has three combat deployments—Iraq, Afghanistan, and Kuwait—and one overseas tour in Germany.

U.S. Cyber Command (USCYBERCOM) members work 2 April 2021 in the Integrated Cyber Center, Joint Operations Center at Fort George G. Meade, Maryland. USCYBERCOM is the military's frontline force engaged in mitigating Russian as well as other adversarial cyberattacks against the United States. (Photo by Josef Cole)

in strength—in order to *deny him these areas altogether*."[29] With the ever-looming threat of attack, ambush, or denial, Russia's only answer is to send out "frequent escorts as protection for his convoys, and as guards on all his stopping places, bridges, defiles, and the rest."[30] This is, in essence, the goal of the Defend Forward strategy of narrowing sanctuaries and turning the neutral, open gray space of the internet into more contested space from the Russian perspective. The goal is to "persistently contest malicious cyberspace actors to generate continuous tactical, operational, and strategic advantage."[31]

An analogy that may help explain the concept of conducting a "people's war" in cyberspace is to think about how the U.S. military conducted counterinsurgency (COIN) operations. In COIN, "the insurgent wins if he does not lose. The counterinsurgent loses if he does not win."[32] The same can be applied to hackers. Just as in a COIN environment, the Defend Forward strategy is about demonstrating long-term commitment to bolster the public's faith in the government to protect and defend its citizens in cyberspace. Just as a military cannot win in a COIN environment by applying an offensive approach, USCYBERCOM has taken the same approach in cyberspace. Part of the reason is that cyberattacks are essentially single-use attacks. They alert the target to a previous unknown vulnerability that later gets closed or mitigated against. This exposes a paradox of cyberattacks where its use diminishes future cyberattack capabilities of the instigator rather than deter bad behavior by the target. Circling back to the COIN analogy, the United States does not have to win every time, but it must continually reaffirm its commitment to enforcing the rule of law in order to gain the trust and support of the population. This is what the Defend Forward strategy is ultimately about: separating hackers from their cause and support, gathering intelligence to drive operations, placing listening posts as close to the hackers to understand the environment, and more.

While threat hunting and defending forward is a way to increase friction upon Russia malign activities in cyberspace, it is no guarantee of preemptively disrupting ongoing operations—made apparent by the SolarWinds hack. Another issue is that the U.S. *National Defense Strategy* does not impose clearly signaled costs on the adversary to dissuade them from conducting cyber operations against the United States and its allies. Costs need to be imposed to deter further action that puts our adversaries "in a situation that is even more unpleasant than the sacrifice you call on him to make. … Otherwise, the enemy would not give in but wait for things to improve."[33] The costs have to be high enough to force American rivals to reassess their cost-benefit calculus, which "means leveraging Western strengths in areas such as finance, soft power in third nations, intelligence gathering, and even cyberwarfare."[34] Worst case, the United States and its allies *must* pose dilemmas that will regardless increase risk or pose some kind of cost to Russia.

"The U.S. *National Defense Strategy* does not impose clearly signaled costs on the adversary to dissuade them from conducting cyber operations against the United States and its allies."

Responding to Russian Cyber and Gray-Zone Activities

More important is keeping in mind the larger U.S. grand strategy vis-à-vis China, to develop some kind of partnership with Russia to peel it away from China's influence and not upset the European balance of power. There are a couple ways to do so in the domain of cyber. The first is supporting NATO's extension of its core task of collective defense further into the cyber domain by providing our NATO allies and other European partners with training and capabilities to expose, attribute, and deter Russian aggression. Doing so helps those member nations build cyber resilience in their own countries in line with NATO's Article 3, a growing area of importance for the alliance. Second is increasing friction between Russia and China by sharing intelligence regarding Chinese activities in cyberspace that impact Russia such as stealing intellectual property, conducting espionage, or misinformation activities. Military sales, like energy, undergirds the Kremlin's geopolitical influence. Exposing and attributing the full extent of previously unknown Chinese intellectual property theft activities against Russian companies can expose the Russian-China alliance as more of an opportunistic alliance that impairs one of Russia's key objectives of becoming a global power. Finally, Western countries can look for common interests to create avenues for cooperation such as in the realm of information security. Russia's foreign minister, Sergey Lavrov, has stated Russian openness to wide cooperation with the West but clarifies that cooperation "would be on Russian terms of a 'universal feeling of equality and equally guaranteed security.'"[35] It is important to pair deterrence activities with compromises that dissuade Russia from seeing the need or opportunity for aggression.

Russia has been refining and escalating its gray-zone tactics to achieve its ultimate objective of creating an uncontested sphere of influence. For the United States to maintain the current rules-based international order, it must reexamine what is required to maintain strategic primacy in this complex global security environment. USCYBERCOM's 2018 Command Vision provide a framework to develop a long-term strategic approach for the military in cyberspace.[36] Most important is that this document provides a cyber strategy that aligns with U.S. regional interests in Russia.

Operating in this kind of environment may constitute one of the most demanding challenges for military planners and leaders since World War II. They have to think beyond purely military action and develop objectives that consider all national power elements to shape the strategic environment where a rival's motivations to engage in malign activity are disrupted, denied, degraded, or deterred. Rather than engage in reprisal actions that escalate situations like the SolarWinds hack to crisis

or conflict, the United States must impose cost in a way that requires a change to Russia's cost-benefit calculus. Additionally, Russia has a strong desire to be seen as a global power and be engaged as equals. Thus, future military strategy should keep this in mind.

As a military organization, being able to manage conflict and preserve peace through strength are two core means by which the military deters war. The application of many of Clausewitz's tenets can be used by senior leaders to integrate operations in cyberspace with the other domains. Understanding and applying Clausewitz's concepts can also be used to devise a tailored deterrence approach that prevents future SolarWinds-like hacks. While the character of war is changing, the fundamental teachings of Clausewitz still remain applicable because the nature of war has not changed. Understanding the political objectives of American adversaries will minimize the risk of military decision-makers falling into the trap of mismatching political-military objectives in deterring future malign activities in cyberspace by Russia. ■

Notes

1. Brian Krebs, "SolarWinds Hack Could Affect 18K Customers," Krebs on Security, 15 December 2020, accessed 19 April 2021, https://krebsonsecurity.com/2020/12/solarwinds-hack-could-affect-18k-customers/.

2. *Privacy Impact Assessment EINSTEIN Program: Collecting, Analyzing, and Sharing Computer Security Information across the Federal Civilian Government* (Washington, DC: Department of Homeland Security National Cyber Security Division, U.S. Computer Emergency Readiness Team, September 2004), 4, accessed 19 April 2021, https://www.cisa.gov/sites/default/files/publications/privacy_pia_eisntein.pdf.

3. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 81.

4. Andrew Radin and Clint Reach, *The Russian Views of the International Order* (Santa Monica, CA: RAND Corporation, 2017), 39, accessed 19 April 2021, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1800/RR1826/RAND_RR1826.pdf.

5. Ibid., 68.

6. Robert Person, "Russian Grand Strategy in the 21st Century," in *Russian Strategic Intentions*, A Strategic Multilayer Assessment (SMA) White Paper, ed. Nicole Peterson (Boston: NSI Inc., May 2019), 33, accessed 19 April 2021, https://nsiteam.com/social/wp-content/uploads/2019/05/SMA-TRADOC-Russian-Strategic-Intentions-White-Paper-PDF-1.pdf.

7. Valery Gerasimov, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations," *Military Review* 96, no. 1 (January-February 2016): 24, accessed 19 April 2021, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art008.pdf.

8. Patrick Tucker, "Russian Military Chief Lays Out the Kremlin's High-Tech War Plans," Defense One, 28 March 2018, accessed 22 June 2021, https://www.defenseone.com/technology/2018/03/russian-military-chief-lays-out-kremlins-high-tech-war-plans/147051/.

9. Daniel Goure, "Russian Strategic Intentions," in Peterson, *Russian Strategic Intentions*, 7.

10. Person, "Russian Grand Strategy in the 21st Century," 10.

11. Gerasimov, "The Value of Science Is in the Foresight," 24.

12. "Making the Kremlin Believe That It's More Advantageous to Cooperate Is Quite Difficult," New Generation Warfare Centre, 6 June 2017, accessed 26 April 2021, https://ngwcentre.com/new-blog/2018/10/5/making-the-kremlin-believe-that-its-more-advantageous-to-cooperate-is-quite-difficult.

13. Gerasimov, "The Value of Science Is in the Foresight," 24.

14. Clausewitz, *On War*, 75.

15. Ibid., 93.

16. "UK Exposes Russian Cyber Attacks," Gov.UK, 4 October 2018, accessed 21 April 2021, https://www.gov.uk/government/news/uk-exposes-russian-cyber-attacks.

17. Clausewitz, *On War*, 182.

18. Ibid., 101.

19. Ibid., 119.

20. Ibid., 569.

21. Ibid., 121.

22. Ibid., 96.

23. Martin C. Libicki, *Brandishing Cyberattack Capabilities* (Santa Monica, CA: RAND Corporation, 2013), viii, accessed 19 April 2021, https://www.rand.org/content/dam/rand/pubs/research_reports/RR100/RR175/RAND_RR175.pdf.

24. Radin and Reach, *The Russian Views of the International Order*, 73.

25. Clausewitz, *On War*, 84.

26. John P. Sheldon, "The Rise of Cyberpower," in *Strategy in the Contemporary World: An Introduction to Strategic Studies*, ed. John Baylis et al., 6th ed. (New York: Oxford University Press, 2019), 298.

27. Clausewitz, *On War*, 479.

28. White House, *Interim National Security Strategic Guidance* (Washington, DC: White House, 2021), 14, access 22 June 2021, https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

29. Clausewitz, *On War*, 481.

30. Ibid., 481

31. United States Cyber Command (USCYBERCOM), *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command* (Washington, DC: USCYBERCOM, 2018), 4, accessed 19 April 2021, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf.

32. Eliot Cohen et al., "Principles, Imperatives, and Paradoxes of Counterinsurgency," in *Conflict after the Cold War: Arguments on Causes of War and Peace*, ed. Richard K. Betts, 4th ed. (New York: Routledge, 2016), 584.

33. Clausewitz, *On War*, 77.

34. Richard Weitz, "Moscow's Gray Zone Toolkit," in Peterson, *Russian Strategic Intentions*, 24.

35. Radin and Reach, *The Russian Views of the International Order*, 47.

36. USCYBERCOM, *Command Vision for US Cyber Command*, 4.