Policy, Strategy, and the President

MILITARY NECESSITY

POLICY-CAPABILITY TENSIONS

Thomas R. Burks

The requirement to conduct cyberspace operations outside of armed conflict but consistent with law-of-armed-conflict principles limits US Cyber Command to a best-tool or whole-of-government approach to national security, creating tension between the command's capabilities and what policy allows it to do. Reframing conflict as strategic competition resolves this tension by restoring military necessity's flexibility, which, in turn, expands what may be considered a military advantage or benefit.

On the eve of the 2018 US midterm elections, US Cyber Command (USCYBERCOM) personnel infiltrated and disrupted networks at the Internet Research Agency (IRA), a civilian corporation headquartered in St. Petersburg, Russia.[1] The operation's apparent purpose was to prevent the IRA from using online resources to interfere with the elections, an objective USCYBERCOM achieved by cutting off the IRA's internet access.

That the United States undertook such a cyberspace operation is unsurprising given Russia's alleged use of the IRA to influence elections in 2016 and the likelihood of a repeat performance.[2] Nor is it surprising the United States would use a military unit this way. The 2017 *National Security Strategy of the United States of America* and 2018 *National Cyber Strategy of the United States of America* contemplate a whole-of-government approach to national security that suggests any number of executive branch organizations might have been chosen as the best tool for the job. The Department of Defense (DoD) is often called upon to conduct activities outside its traditional mission set.[3]

Major Thomas R. Burks, USAF, is the deputy staff judge advocate for the 2nd Bomb Wing, Barksdale Air Force Base, Louisiana. He holds a master of laws in space, cyber, and telecommunications law from the University of Nebraska and a juris doctorate from Indiana University-Indianapolis.

1. Ellen Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms," *Washington Post,* February 27, 2019, https://www.washingtonpost.com/.

2. Council on Foreign Relations (CFR), "Targeting of Internet Research Agency," Cyber Operations Tracker, February 2019, https://www.cfr.org/cyber-operations/.

3. Rosa Brooks, *How Everything Became War and the Military Became Everything: Tales from the Pentagon* (New York: Simon & Schuster, 2016); and Mackenzie Eaglen, "Just Say No: The Pentagon Needs to Drop the Distractions and Move Great Power Competition beyond Lip Service," War on the Rocks, October 28, 2019, https://warontherocks.com/.

Still, it is curious that USCYBERCOM was a viable option given the contents of the DoD law of war policy in effect at that time. The law of war is a body of international law divided into two broad categories: (1) jus ad bellum, which governs whether armed force may be employed, and (2) jus in bello, which regulates the conduct of belligerents once a conflict has begun.[4]

The second category, jus in bello, is generally known as the law of armed conflict (LOAC). As the term LOAC implies, this body of law is applicable only during an armed conflict. But the DoD law of war policy in effect in 2018 required adherence to the law of war in all military operations, even when those operations occurred outside an area of armed conflict.[5] Adherence to the LOAC was required as a matter of policy even when it was not required as a matter of law.

The USCYBERCOM operation would thus have had to comply with LOAC principles, such as the principle of military necessity, even though Russia and the United States were not at war. Applying the principle of military necessity to less-than-war cyberspace operations and meeting its requirements is easier said than done. The reason for this difficulty is that the definition of military necessity presumes the existence of an armed conflict, and the armed conflict itself shapes what is militarily necessary for achieving its ends.

Though the principle is inherently flexible, in the absence of an armed conflict, military necessity must be determined in a vacuum where the military component of the term takes center stage. Focusing on the military component means an operation must include a military benefit or advantage before it may be considered a military necessity.

The USCYBERCOM operation falls short of this standard because it targeted the IRA, a civilian company with no apparent connection to the Russian military, to defend the American electoral process against malicious cyber actors—a worthy national security objective but certainly not a military one. The operation thus included no military benefit or advantage and was not a military necessity.

The Department of Defense might agree with this assessment because in the years following the IRA operation, it changed its policy to require consistency with the law of war rather than strict adherence to the law of war.[6] While this change made the policy more flexible, it did not resolve the issue, since the primary shaper of military necessity (the armed conflict) was still missing. The principle of military necessity as policy must therefore still be judged in a military-focused vacuum, which means USCYBERCOM's operation against the IRA would fail the military necessity test even under today's more relaxed policy standard.

---

4. International Committee of the Red Cross (ICRC), *International Humanitarian Law: Answers to Your Questions* (Geneva: ICRC, 2014), 8, https://www.icrc.org/.

5. General Counsel of the Department of Defense (GC DoD), *DoD Law of War Program*, Department of Defense Directive (DoDD) 2311.01E, Incorporating Change 1, November 15, 2010, certified current as of February 22, (Washington, DC: GC DoD, February 22, 2011), 2, https://www.esd.whs.mil/.

6. GC DoD, *DoD Law of War Program*, DoDD 2311.01 (Washington, DC: GC DoD, July 2, 2020), https://www.esd.whs.mil/.

Requiring military operations to comply or be consistent with the principle of military necessity thus creates tension between what the military is capable of and what the DoD law of war policy permits. Fortunately, relieving this tension does not demand revisions to law or policy. All that is required is adjusting how one views the context in which less-than-war cyberspace operations are employed and, in turn, changing how these operations are analyzed for policy compliance.

Stated simply, if the lack of a conflict created the policy-capability tension, a conflict must be added to the analysis. This is not to say that armed conflict should be pursued in the interest of policy clarity, but that conflict must be reframed in a manner that reflects the circumstances where these operations occur, namely, in strategic competition. With conflict thus reframed, the historical flexibility of the principle is restored, and the military necessity of USCYBERCOM operations may be judged by what is necessary to achieve the strategic competition objectives given to the command. Reframing conflict resolves the tension between DoD law of war policy and less-than-war cyberspace operations, which enables the use of the Department of Defense and USCYBERCOM in a best-tool approach to national security.

Principle of Military Necessity

The law of armed conflict is fundamentally a balance between the "necessities of war" that typically require death and destruction and the "requirements of humanity," which require saving lives and reducing human suffering to the extent possible.[7] This balance is achieved by permitting the use of any amount of force in an armed conflict that is militarily necessary, as long as it does not violate the other LOAC components.[8]

Military necessity is thus the starting point for judging the LOAC compliance of belligerent activities in war. Without it, the analysis never proceeds to rules such as distinction, which permits militarily necessary attacks on military objectives but not civilian ones, and proportionality, which prohibits otherwise lawful activities if the incidental loss of civilian life, injury to civilians, or damage to civilian objects is "excessive in relation to the concrete and direct military advantage anticipated."[9] This lynchpin status begs the question, exactly what is military necessity?

The principle of military necessity has its roots in the code of conduct President Abraham Lincoln issued to the US Army during the Civil War.[10] Article 14 of this code, generally referred to as the "Lieber Code," defines military necessity as "those

7. Yoram Dinstein, *War, Aggression, and Self-Defence,* 4th ed. (Cambridge, UK: Cambridge University Press, 2005), 101; and ICRC, *Answers to Your Questions*, 6.

8. Dinstein, *Self-Defence*, 19.

9. Secretariat of the United Nations, "No. 17512, Protocol 1, part 4, sec. 1, chap. 2, art. 51," in *Treaties and International Agreements Registered or Filed with the Secretariat of the United Nations*, vol. 1125 (New York: UN, January 23, 1979), https://treaties.un.org/.

10. Abraham Lincoln, *General Orders No. 100: Instructions for the Government of Armies of the United States in the Field* (Washington, DC: Adjutant General's Office, April 24, 1863), https://avalon.law.yale.edu/.

measures which are indispensable for securing the ends of the war."[11] A key lesson derived from the principle's application during the Civil War is that the principle of military necessity is inherently flexible and shaped by armed conflict. For example, the Lieber Code's definition of military necessity was used to justify the burning of raw cotton to prevent the funds generated by its export from being used to arm and provision the Confederate Army.[12]

Foiling the logistical capabilities of an adversary is an oft-used war measure, but it is noteworthy that military necessity also justifies actions that do not involve force or meet typical military objectives. For example, the "civil chaos" that erupted in reconquered Southern territory made it increasingly difficult to conduct military operations effectively and eventually resulted in the creation of military provost courts to handle civil disputes.[13] This is not a function the US military normally performs, but it was a military necessity in the context of that armed conflict.

Additionally, in freeing the slaves in the areas of rebellion, the 1863 Emancipation Proclamation was justified as a measure for reducing the South's labor force and the Confederacy's ability to provision and equip its armed forces. The Emancipation Proclamation was thus a "fit and necessary war measure" by which President Lincoln could "suppress [the] rebellion."[14] This made Lincoln's edict a military necessity even though it did not involve traditional military force and met a national security objective (preserving the Union) rather than a tactical or operational one.

As applied in the Civil War, the principle of military necessity was inherently flexible and expansive enough to include measures necessary for achieving the aims of that conflict, even if those measures were atypically military or nationally focused. After the Civil War, the principle of military necessity and the humanitarian limitations also found in the Lieber Code quickly gained international recognition and over time became a part of the LOAC.[15]

Today, the Department of Defense defines military necessity as the "principle that justifies the use of all measures needed to defeat the enemy as quickly and efficiently as possible that are not prohibited by the law of war."[16] The DoD definition is consistent with that used by the American Tribunal at Nuremberg, which found that military necessity "permits a belligerent, subject to the laws of war, to apply any amount

11. Lincoln, *General Orders*, art. 14.

12. Burrus M. Carnahan, "Lincoln, Lieber and the Laws of War: The Origins and Limits of the Principle of Military Necessity," *American Journal of International Law* 92, no. 2 (April 1998): 226, https://blogs.loc.gov/.

13. Carnahan, "Lincoln, Lieber," 224.

14. Abraham Lincoln, Emancipation Proclamation, January 1, 1863, presidential proclamations, 1791-1991; record group 11; general records of the United States Government; National Archives, https://www.archives.gov/.

15. Lincoln, *General Orders*, arts. 14, 16; and Gary D. Solis, *The Law of Armed Conflict: International Humanitarian Law in War* (Cambridge, UK: Cambridge University Press, 2010), 259–60.

16. GC DoD, *DoD Law of War Manual*, (Washington, DC: GC DoD, December 2016), 52, https://www.hsdl.org/.

and kind of force to compel the complete submission of the enemy with the least possible expenditure of time, life, and money."[17]

These modern definitions of military necessity retain the core aspects of the original, which suggests the principle and its key characteristics—flexibility and shaped by armed conflict—remain unchanged even though the LOAC humanitarian components that restrain military necessity have changed considerably.

Limitations of Military Necessity as Policy

Applying the principle of military necessity in an armed conflict is often not simple or easy, but after decades of experience, the Department of Defense is accustomed to its requirements and the other LOAC principles that accompany it. When military necessity is applied as a matter of policy outside the context of armed conflict, that application can become problematic. The USCYBERCOM operation against the Internet Research Agency ably demonstrates this point.

Operation against the IRA

In 2014, Russian nationals working for the IRA embarked on a two-year disinformation campaign aimed at influencing US elections. As detailed in a subsequent federal indictment, the IRA adopted the personas of real and fake American persons and used these personas to spread various messages. Some messages were designed to favor one candidate or disadvantage another, while other messages sought to suppress some voting blocs and to influence the votes of others.[18] The evidence suggests these were not the activities of independent actors but rather the actions of a Russian Federation proxy and thus the actions of the Russian Federation. This was certainly Congress's conclusion.[19]

Exactly how well the IRA's campaign worked is impossible to tell. What can be said is that a Russian government proxy influenced the 2016 election to some degree and cast doubt on the veracity of the American electoral process and its results. Not to be outmaneuvered again, the United States took a more proactive approach for the 2018 midterm election. Part of this effort reportedly involved USCYBERCOM personnel accessing IRA systems and shutting them down shortly before Election Day, thereby removing the so-called trolls from the internet and their access to American voters.[20]

---

17. United States v. Wilhelm List et al., United States Military Tribunal at Nuremberg, Germany, 1948, 11 *NMT* 1230, 1253.

18. United States v. Internet Research Agency LLC, et al., Case 1:18-cr-00032-DLF (Washington, DC, February 16, 2018), 3–4, https://www.justice.gov/.

19. S. Rep. No. 116-290 vol. 2 at 4-5 (2020), https://www.congress.gov/.

20. Nakashima, "Cyber Command Disrupted;" and Zachary Fryer-Biggs, "The Pentagon Has Prepared a Cyber Attack against Russia," The Center for Public Integrity (website), November 2, 2018, https://publicintegrity.org/.

The involvement of USCYBERCOM was officially acknowledged in 2020 when then-President Donald Trump confirmed he had ordered the operation.[21] As the "sole organ of the federal government in . . . international relations" and in their role as the ultimate military commander, US presidents have substantial constitutional authority to determine which elements of the executive branch are employed to achieve national security objectives.[22]

Congress also has foreign policy responsibilities and in exercising its constitutional authority has long indicated approval of the use of USCYBERCOM for this type of clandestine operation.[23] From an international law perspective, the operation against the IRA was not a use of force, does not appear to have violated the principle of nonintervention, and because it occurred outside of an armed conflict and did not constitute an attack, LOAC rules did not apply as a matter of law.[24]

Accordingly, from international and domestic law perspectives, the cyberspace operation against the IRA appears to have been completely legal, and Trump was well within his authority to choose USCYBERCOM for its execution. (Incidentally, cyberspace operations must also comply with domestic statutes such as the Wiretap Act, Computer Fraud and Abuse Act, and the Hatch Act. Compliance is assumed for this article's purposes.)

Compliance with Policy

Legality notwithstanding, the question remains whether the IRA operation was consistent with DoD policy, which at the time required all military operations to comply with the LOAC.[25] Judging the LOAC compliance of the IRA operation must begin with the principle of military necessity, which again permits "the use of all measures needed to defeat the enemy as quickly and efficiently as possible that are not prohibited by the law of war."[26]

The available information indicates the IRA operation did not meet this standard for two reasons. First, the cyberspace operation was conducted outside of an armed conflict, which means no objectives or end state existed to define what winning the conflict looked like. Consequently, there was no way to determine whether the operation was necessary for achieving those ends.

---

21. Nakashima, "Cyber Command Disrupted;" and Marc Thiessen, "Trump Confirms, in an Interview, a U.S. Cyberattack on Russia," *Washington Post,* July 10, 2020, https://www.washingtonpost.com/.

22. US Const., art. II, §§ 1, 2; and United States v. Curtiss-Wright Corp, 299 U.S. 304, 320 (1936).

23. National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, § 954 (2011); and Authorities Concerning Military Cyber Operations, 10 USC § 394(a), amended Pub. L. 115–232, div. A, title XVI, §§ 1631(a), 1632, 132 Stat. 2123 (2018).

24. Charter of the United Nations, Articles 2(4), 2(7), https://legal.un.org/, and https://legal.un.org/; Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Merits, Judgment International Court of Justice. Reps. 1986, 14, ¶ 205, https://www.icj-cij.org/; and Secretariat of the United Nations, Protocol 1, art. 49.

25. GC DoD, DoDD 2311.01E, 2.

26. GC DoD, *Law of War Manual*, 52.

Second, in the absence of an armed conflict that might expand military necessity, one must look to the military aspect of the principle to determine whether its requirements have been met. In a military-focused analysis, the IRA operation would have to have offered a military benefit or advantage, criteria that an operation targeting a civilian corporation staffed by civilians and owned by a civilian oligarch did not meet.[27]

Additionally, the operation did not target Russian military capability but the broader Russian Federation's ability to influence US elections. Consequently, while USCYBERCOM's protection of US elections helped achieve a national security objective and may even have foiled a component of Russian grand strategy, its operation achieved no military benefit or advantage and was not a military necessity.

There are counterarguments to this assessment. It could be argued, for example, that the IRA operation was a military necessity because it was ordered by the commander-in-chief and executed by a military unit under the orders of the secretary of defense. Actions necessary for meeting the task's objectives are therefore a military necessity. This line of reasoning is attractive because it is easy to apply and permits the broad use of USCYBERCOM.

But this argument is flawed for two reasons. First, it only applies to subordinate forces; personnel at the highest levels of government that determine whether a proposed order meets legal and policy requirements must determine whether military necessity exists before the order is ever issued. Second, the act of issuing military orders does not itself create legal and policy compliance. The opposite is true, meaning compliance with law and policy must be established before the order may be carried out. This is why military personnel have an affirmative duty to disobey unlawful orders.[28] Therefore, the existence of military necessity is a conditional precedent for order issuance, not its result.

It could also be argued that even if this assessment was once correct, it is now irrelevant because DoD policy was revised, and it no longer requires adherence to the law of war but rather only consistency with its principles. Under this more flexible regime, a purely military advantage or benefit may not be required for policy compliance.

Still, before concluding the new policy's flexibility has freed military necessity of its military-centric focus, one should consider how closely related components of the LOAC inform the meaning of military necessity. The rule of distinction requires distinguishing between civilians and military personnel and between military objects and civilian objects to ensure civilians and their objects are not targeted. Under the law of armed conflict, an object is considered a military object if its "nature, location, purpose, or use make[s] an effective contribution to military action and whose total

27. United States v. Internet Research Agency, 2; Maxim Trudolyubov, "Vladimir Putin's Parallel State," The Russia File (blog), February 21, 2018, https://www.wilsoncenter.org/; and Zack Beauchamp, "Meet the Shady Putin Crony Funding Russia's Troll Farm and Mercenary Army," Vox, February 26, 2018, https://www.vox.com/.

28. GC DoD, DoDD 2311.01, 3, 12; Uniform Code of Military Justice, 10 U.S.C. §§ 890, 892 (2019); and Joint Service Committee on Military Justice (JSCMJ), *Manual for Courts-Martial*, "Article 90," 16.c.(2)(a) (Washington, DC: JSCMJ, 2019), https://jsc.defense.gov/.

or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage."[29]

This definition clearly contemplates a military advantage before an object can be targeted. The USCYBERCOM operation against the IRA fares just as poorly under the rule of proportionality, which prohibits damage to civilian objects when the damage is "excessive in relation to the concrete and direct military advantage anticipated."[30] Given that distinction and proportionality are derived from and predicated on military necessity, it follows that the existence of a military benefit or advantage is still necessary even under the revised policy.

The increased flexibility of the Department's current law of war policy thus did not resolve the problems of its predecessor. This means that unless "military" is read out of that principle, a draconian step not contemplated by either version of the DoD policy, the principle of military necessity remains predicated on achieving a military advantage or benefit.

But as the Lieber Code's application in the Civil War demonstrates, even operations that do not involve force or traditional military objectives can meet the requirements of military necessity as long as the operation is necessary for achieving the ends of the conflict in which it is employed. Therefore, it is the lack of a conflict, not per se the military focus of military necessity, that locks the principle into a military-focused vacuum. The key to unlocking military necessity's inherent flexibility, and thus expanding the types of operations that can meet its requirements, lies in having a conflict against which the military necessity of less-than-war cyberspace operations may be judged.

Reframing the Conflict

Strategic Competition

Unless an actual war is to be pursued in the interest of easier analysis, something not suggested or advisable, giving these operations a conflict means reframing conflict as something other than armed conflict. The current state of international affairs—the state in which it has existed for most of the last few centuries—suggests strategic competition is the leading candidate. Such reframing is not possible in the case of an actual armed conflict, which is a status defined by international law.[31]

But flexibility in terms and in their application is permissible in policy spaces that seek to occupy areas the law does not. There is no set definition for strategic competi-

29. Secretariat of the United Nations, Protocol 1, art. 52.2; National Defense Authorization Act for Fiscal Year 2010, 10 U.S.C. § 950p(a)(1).

30. Secretariat of the United Nations, Protocol 1, art. 51 (emphasis added).

31. "Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field," arts. 2–3, August 12, 1949, 6 UST 3114; and 75 UNTS 31, https://treaties.un.org/.

tion, and the United States has not chosen a unified approach.[32] For this discussion, it is enough to observe its foundational principles and understand how they can be used to formulate a new way of looking at conflict.

The modern state, born in seventeenth-century Europe, was founded on two key principles: (1) states are abstract and enduring entities that exist in their own right; and (2) states have national interests that each state has a sovereign right to pursue.[33] Of course, activities that further one state's interests do not necessarily promote the interests of others and can be at cross-purposes with those of other states. These actions inevitably lead to friction and rivalry as states seek to further their interests and provide themselves a comparative advantage in the pursuit of "nationalist ambitions [and] passions."[34]

The competitive pursuit of national interests is often referred to as great power or strategic competition.[35] This article will use the term strategic competition since not all states against which the United States competes can rightly be considered a great power. In centuries past, strategic competition frequently resulted in the use of war as a means of furthering state interests.[36] But the adoption of the UN Charter and its prohibition on the "threat or use of force" except under narrow circumstances greatly limited the ease with which states could choose armed force to achieve state interests.[37]

The removal of force as an option did not eliminate armed conflict, but it made force less easily resorted to and consequently made the less-than-war tools of international relations even more important than they already were. Modern strategic competition is characterized by states preparing for military conflict as a deterrent to armed force while using less-than-war options, including diplomacy, economic policy, sanctions, espionage, cyberspace operations, and influencing through information, to pursue their national interests. This strategic competition is the battle in which the United States is presently engaged, making it the conflict relevant to the reframing discussion.

Pros and Cons

Reframing the conflict as strategic competition has three key benefits. One, it adopts a conflict in which the United States is already engaged and for which it has

32. Alexander Boroff, "What is Strategic Competition Anyway?," Modern War Institute, April 4, 2020, https://mwi.usma.edu/; and Ali Wynn, "The Need to Think More Clearly About Great-Power Competition," RAND Corporation, February 11, 2019, https://www.rand.org/.

33. Henry Kissinger, *World Order* (New York: Penguin Books, 2014), 22.

34. Robert Kagan, *The Return of History and the End of Dreams* (New York: Vintage Books, 2008), 3.

35. Donald J. Trump, *National Security Strategy of the United States of America* (Washington, DC: White House, December 2017), 27, https://trumpwhitehouse.archives.gov/; and James N. Mattis, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Office of the Secretary of Defense, January 2018), 1, https://dod.defense.gov/.

36. Dinstein, *Self-Defence*, 176; and James Turner Johnson, *Ethics and the Use of Force: Just War in Historical Perspective* (Farnham, England: Ashgate Publishing Limited, 2011), 39.

37. UN Charter, art. 2(4), 44, 51.

identified national interests and objectives. There is thus no new ground to be broken to enable the reframing. Two, reframing the conflict as strategic competition has the potential to expand what type of less-than-war operations can be considered a military necessity. Indeed, once military necessity is freed from its military-centric focus, the Department of Defense and USCYBERCOM may be used for operations (within legal limits) that meet broad national security objectives without regard to an operation's purely military benefit or advantage.

Three, reframing conflict as strategic competition provides the Department of Defense with a policy framework to which it is accustomed and through which LOAC-as-policy seamlessly transitions into LOAC-as-law should an armed conflict break out. Reframing the conflict thus enables a best tool or whole-of-government approach to national security that familiarly cuts across the full spectrum of military operations.[38]

It must be acknowledged, however, that reframing conflict may have its detractors. For instance, one could argue that if military necessity is broadened to include more than military-centric objectives, there will be no practical limitation on what USCYBERCOM can undertake. But the legal limits of international and domestic law still exist in a reframed conflict, as does the rigorously interagency nature of the US national security apparatus. It is only the DoD law of war policy that becomes more flexible and able to adapt to the state of strategic competition in which it is employed.

Furthermore, it must be remembered that military necessity is only the first step in the policy analysis; cyberspace operations must still be "consistent with" the other LOAC rules.[39] Accordingly, there are ample legal and policy checks on USCYBERCOM's actions.

It could also be argued that strategic competition is not an appropriate candidate for a reframed conflict because it is not possible to win interstate relations. This point is well taken, as strategic competition is what might be called an "infinite game," meaning a state of competition that never actually ends.[40]

Still, while it may not be feasible to win strategic competition, it is possible to identify national interests and the adversaries that threaten them and set discrete national security objectives designed to further those interests. Accordingly, while the game may never be truly won, it is possible to determine what is militarily necessary for achieving national security objectives and furthering the comparative advantage of the United States.

Practical Application

Reframing conflict as strategic competition is useful only if it can be practically applied. While details about the USCYBERCOM operation remain classified, using publicly

38. Donald J. Trump, *National Cyber Strategy of the United States of America* (Washington, DC: The White House, September 2018), 20.

39. GC DoD, DoDD 2311.01, 3.

40. Simon Sinek, *The Infinite Game* (New York: Portfolio/Penguin, 2019), 259–60.

available information regarding USCYBERCOM's operation against the IRA as a case study sufficiently demonstrates the viability of this proposed reframing.

The first step of the analysis is to determine US national interests and the threats to those interests during the 2018 midterm elections. The 2017 *US National Security Strategy*, for instance, asserts four broad national interests, one of which is "protect[ing] the American people, the homeland, and the American way of life."[41]

When elaborating on this national interest, the Strategy identified cyberspace operations as a threat to American political interests and marked foreign governments for "swift and costly consequences" should those governments engage in malicious cyber activities against the United States. The 2018 *US National Cyber Strategy* identifies the Russian government as an adversary using cyberspace to undermine American democracy and "sow discord" in democratic processes and further explains that countering, disrupting, degrading, and deterring such activities is a national security objective.[42]

With objectives and the adversary defined, Trump would have been well within his constitutional authority to choose the Department of Defense and USCYBERCOM as the instrument of national security best positioned to "protect the American . . . way of life" by foiling Russian attempts to influence the midterm elections. Once the task was given to the Department of Defense and USCYBERCOM, those organizations could use the same objectives and adversary to identify actions necessary to meet those objectives, such as shutting down the systems of a Russian government proxy being used to influence and undermine the American democratic process. Reframing the conflict as strategic competition would thus have made USCYBERCOM's operation against the IRA a military necessity.

While the national security policy landscape has changed somewhat under the Biden administration, reframing conflict as strategic competition would likely produce the same result as in 2018. In March 2021, the Biden administration issued interim national security guidance that identifies Russia as a chief rival. Further, this guidance articulates defending democracy against cyberattacks and disinformation and imposing "real costs" on those who "interfer[e] with our democratic processes" as key national security initiatives.[43]

The adversary is the same, and the stated objectives are essentially so. The objectives suggest that had the interim guidance been in place in 2018, the Department of Defense and USCYBERCOM could still have been the best tools for election defense, and the administration could have used them to determine which actions were necessary to meet its national security objectives. Reframing conflict as strategic competition is thus more than a one-off instance of policy compliance; it is a viable model for continued use and application to less-than-war cyberspace operations.

41. Trump, *National Security Strategy*, 4.

42. Trump, *National Cyber Strategy*, 2–3, 20.

43. Joseph R. Biden, *Interim National Security Strategic Guidance* (Washington, DC: The White House, March 2021), 6, 8, 19–20.

Conclusion

Before 2016, USCYBERCOM and the Department of Defense were reportedly focused on issues other than election defense but have since broadened the scope of their concerns to include issues affecting the greater national security of the United States.[44] This shift is consistent with the whole-of-government and best-tool approach contemplated in US strategic documents. The national security strategy is being revised at the time of this writing; however, the Biden administration's interim guidance indicates defending American democratic institutions from various threats, including actors in cyberspace, remains a key US national interest.[45]

Further, holding cyberspace actors accountable for their malicious activities by "imposing substantial costs" remains an option for pursing such interests.[46] These factors suggest the whole-of-government approach to national security, including DoD and USCYBERCOM involvement in such measures, is here to stay.

In the interest of maturing how USCYBERCOM is used and ensuring a consistent analysis of its operations, it is necessary to address the difficulty of applying the DoD law of war policy, and particularly the principle of military necessity, to less-than-war cyberspace operations. One option is to eliminate the portions of the policy applicable outside of armed conflict or perhaps to exempt less-than-war cyberspace operations from the policy's reach permanently. But as discussed, the Department's familiarity with LOAC as law suggests applying LOAC as policy to these operations has its advantages.

The second and better option is to relieve the tension between what the Department of Defense can do and what its policy permits by reframing conflict as strategic competition, thereby giving less-than-war cyberspace operations the conflict qualification needed for military necessity analysis. Reframing conflict in this way expands what is militarily necessary to meet the reframed conflict's objectives, thus enabling rather than stymying the use of the Department of Defense and USCYBERCOM as instruments of national security. **Æ**

---

44. Todd Lopez, "For 2020 Election, Threat is Bigger than Russia," Department of Defense News, August 8, 2020, https://www.defense.gov/.

45. Biden, *Strategic Guidance*, 9.

46. Biden, 18.