A HOOVER INSTITUTION ESSAY

Cyberattacks and the Constitution

MATTHEW C. WAXMAN

Aegis Series Paper No. 2007

The United States has one of the world's strongest and most sophisticated capabilities to launch cyberattacks against adversaries. How does the US Constitution allocate power to use that capability? And what does that allocation tell us about appropriate executive-legislative-branch arrangements for setting and implementing cyber strategy?

The term "cyberattack" is often used loosely. In this essay, I define a cyberattack as action that involves the use of computer code to disrupt, degrade, destroy, or manipulate computer systems or networks or the information on them.[1] I am not including cyber operations that are purely for information gathering or to map foreign networks in preparation for future cyberattacks.

This definition of cyberattack still includes a wide array of operations. On one end are attacks on computer systems that have effects—including kinetic, sometimes violent ones—outside those systems. Examples include the Stuxnet attack that brought down some of Iran's nuclear centrifuges and the 2017 NotPetya attack, widely attributed to Russia, that targeted major Ukrainian companies and government agencies but spread widely and disabled computers—as well as commerce dependent on them—around the globe.[2] At the other end are the types of low-level and often discrete attacks that appear to be contemplated by the United States "Defend Forward" concept. Examples include infiltrating adversary networks and deleting or corrupting data, or US Cyber Command's operations that disrupted the networks of Russia's infamous "Internet Research Agency" troll farm in the run-up to the 2018 US midterm elections.[3] There are of course many possibilities in between.

This essay offers a way to think about the constitutional distribution of powers between the president and Congress governing the use of US cyberattack capabilities. Some commentators and analysts view this problem almost reflexively as a "war powers" issue—a term I use throughout this essay to refer to *the political branches' respective constitutional authority over the hostile use of military force*. That is especially true as one moves up the scale of expected damage.[4] A corollary to that constitutional issue is a statutory question: Namely, how should the 1973 War Powers Resolution, which was intended to restrict extensive military hostilities without congressional approval, be interpreted or amended to account for cyberattacks?[5] The imprecise rhetoric of "cyberwar," "cyber conflict," and "cyberattacks" probably contributes to this legal framing.

But many—and probably almost all—cyberattacks undertaken by the United States cannot plausibly be viewed as exercises of war powers. Indeed, the entire Defend Forward concept appears to involve low-level operations well below the "use of force" threshold under international law and far short of the types of operations that have typically triggered war powers analysis under domestic constitutional law.

This essay argues that as a conceptual and doctrinal matter, cyberattacks alone are rarely exercises of war powers—and they might never be. They are often instead best understood as exercises of other, nonwar military powers, foreign affairs powers, intelligence powers, and foreign commerce powers, among other constitutional powers not yet articulated. Although this more fine-grained and fact-specific constitutional conception of cyberattacks leaves room for broad executive leeway in some operational contexts, this discretion is often the result of congressional delegation or acquiescence as opposed to any inherent constitutional authority on the part of the president. At the same time, these alternative understandings of cyberattacks also contain a strong constitutional basis for Congress to pursue legislative regulation of the procedural and substantive parameters governing cyber operations.

Beyond those descriptive claims, this essay argues that a rush to treat cyberattacks as implicating war powers misguides criticisms about the role Congress is or is not playing in regulating cyberattacks. This is because participants in war powers debates often bring intense and polar normative stances about the appropriate institutional arrangements governing the exercise of those powers. On one end are those who prize executive speed, agility, and secrecy—and therefore presidential freedom from congressional interference. On the other end are those who see formal congressional approval for military campaigns as being of paramount constitutional importance. The latter, who want to roll back presidential unilateralism, often see cyberattacks as yet another problematic means by which presidents can evade proper congressional checks on war. But in their focus on congressional approval for military intervention, and by extension for at least some high-intensity cyberattacks, those critics may overlook other institutional arrangements that are better tailored to US cyber strategy, especially to the sort of lower-intensity activities that make up Defend Forward. They also may overlook the many important ways in which Congress is already actively involved in shaping and facilitating that strategy.

Cyberattacks as Exercising War Powers?

Suppose the executive branch launches an operation that, through infiltration of foreign computer networks and insertion of code, disables an adversary's air defense system, knocks offline parts of its banking system, or takes over control of its intelligence service's social media accounts. Or suppose that a US cyber operation ruins an adversary's ballistic missile test, temporarily shuts down some internal government communications, or disrupts a

state-owned business's operations. These direct effects might be small and temporary, but in some cases they might be large and long term. Assuming that such operations do not take place in the context of an ongoing armed conflict (and putting aside for now any additional statutory authorities or prohibitions), what constitutional powers is the president exercising?

The answer depends a lot on the facts. Cyberattacks, as defined in this essay, encompass a very broad set of possible activities. But a common answer is that this is at least partly a war powers question, and thus the legality of such operations depends on the president's power to use military force in a given instance.

The Constitution's drafters studiously placed the power to declare war in Congress. Throughout American history, a strong current of thought has interpreted this choice to imply that Congress has exclusive (or near-exclusive) power to decide whether or not the country goes to war or initiates armed hostilities beyond cases of, in Madison's words, "repel[ling] sudden attacks."[6]

Several overlapping normative justifications are associated with this view. One is that requiring formal and express congressional approval ensures thorough deliberation and thereby prevents rash military intervention. Another common justification is that no one person ought to be able to bring violent conflict, and hence threats to American blood and treasure, upon the nation absent the most extreme emergency requirement for self-defensive action. For these and other reasons, including concerns that mobilizing military power would threaten republicanism at home, there was strong consensus among the constitutional founders that only Congress—not the president alone—should be able to take the country from peace to war.[7] Some would argue that these reasons have grown stronger over time, as American military power and war's destructive potential have grown. Nevertheless and owing to a variety of factors, over time the president has asserted, sometimes with acquiescence by Congress and the courts, vast power to use military force without congressional approval far beyond the circumstances imagined by Madison.[8]

Modern executive-branch legal precedent and practice generally hold that the president has broad authority to launch military strikes without specific congressional authorization to defend American interests.[9] Indeed, the executive branch's view of expansive presidential powers to use kinetic military force is so well entrenched that putting cyber operations in the same category may be an attractive analytic move for justifying unilateral action in that domain, too (as well as for justifying the president's authority to take kinetic military responses in self-defense against *incoming* cyberattacks).

In a 2020 address, the Defense Department general counsel explained that the legal analysis for the military, in particular, to conduct cyberattacks looks the same as that for kinetic military attacks:

> The domestic legal authority for the DoD to conduct cyber operations is included in the broader authorities of the President and the Secretary of Defense to conduct military operations in defense of the nation. We assess whether a proposed cyber operation has been properly authorized using the analysis we apply to all other operations, including those that constitute use of force.[10]

Importantly, and elaborated below, "military operations in defense of the nation" implicate a much broader set of constitutional categories than just hostile applications of force; most such operations would not be exercises of war powers. The Defense Department general counsel then laid out the overall legal framework and applied it directly to the department's cyber operations:

> The President has authority under Article II of the U.S. Constitution to direct the use of the Armed Forces to serve important national interests, and it is the longstanding view of the Executive Branch that this authority may include the use of armed force when the anticipated nature, scope, and duration of the operations do not rise to the level of "war" under the Constitution, triggering Congress's power to declare war. Furthermore, the Supreme Court has long affirmed the President's power to use force in defense of the nation and federal persons, property, and instrumentalities.[11]

One upshot of this analysis, he concluded, is that "the President has constitutional authority to order military cyber operations even if they amount to use of force in defense of the United States."[12]

Viewing some cyberattacks as the exercise of war powers may seem sensible for several reasons. If they are carried out by US Cyber Command, the organization of the armed forces tasked with conducting offensive cyber operations, the agent is the same one that conducts kinetic attacks. If a cyberattack causes damage that might otherwise be achieved by kinetic violence, or if the target is an adversary's armed forces, the effect is similar. If cyberattacks could foreseeably provoke an armed response, the consequences seem comparable.

It is questionable, though, whether the vast majority of actual and plausible cyberattacks should be understood as exercises of war powers at all. In other words, it may be a category error to analyze many cyberattacks as one would the application of hostile military force abroad, either as to the scope of the president's inherent constitutional authority or as to any constitutional requirement for congressional approval. As mentioned above, this is an area of constitutional law originally conceived for particular concerns about *physically armed* violence—specifically by military forces—including the risks of American bloodshed and escalation.

If war powers are a special constitutional category demanding formal congressional approval because of the risks to American blood, most cyberattacks barely if at all

implicate this concern, because the risks are so tiny and remote. In modern executive-branch practice, as in many criticisms of that practice, risk to American service members is usually considered an affirmative factor in determining whether a military intervention is of such intensity as to amount to "war" in a constitutional sense that might require congressional approval. Low risk to American troops, on the flip side, may help justify presidential unilateralism.[13] Personnel conducting cyberattacks are physically and temporally distant from actions that might seem conceptually analogous to "combat." Of course, it has long been the case that military violence can be carried out remotely, with limited direct risks to American service members. Drone strikes are an obvious modern-day example, but even well before then, advances in aviation and munitions technology made possible massive bombing campaigns with low risk to American pilots. Missiles, of course, can deliver huge payloads from great distances.

Cyberattacks take human remoteness to an extreme, though, by placing no American lives immediately at risk. Except in the most extraordinary circumstances, they rarely even place foreign lives at risk (at least not directly). That human remoteness alleviates some concerns underlying arguments for congressional approval requirements, but it exacerbates others because the relative invisibility of cyberattacks means that political checks function weakly. As Jack Goldsmith and I have argued about "light-footprint" tools, including cyber-operations and drone attacks:

> Light-footprint warfare is still lethal and very consequential warfare, and the lightness of the tools make them relatively easy for a President to deploy extensively. Light-footprint warfare thus has large foreign policy, strategic, and reputational consequences for the United States, akin to much heavier deployments, yet much less public examination. The President's legal theories treat this as a feature of such warfare. But it is also a bug for U.S. democracy, since the stealthy features mean that public debate and political checks—which reduce error as well as excess, and promote legitimacy—function ineffectively.[14]

Another important reason why war powers may be special—and why many argue that requirements of formal congressional approval are needed—is the risk of violent escalation. A common argument is that congressional approval (following careful interbranch deliberation) is especially important for measures that are likely to provoke armed retaliation. In recent decades, executive-branch practice and legal justifications have acknowledged this factor, too, in assessing whether a military intervention rises to the level of "war" perhaps requiring congressional authorization. In its 2018 opinion justifying President Trump's air attacks against Syria, for example, the Justice Department's Office of Legal Counsel considered this variable, noting that steps taken to reduce the probability of military reprisals strengthened the argument that the strikes were within the president's authority.[15] Inversely, if cyberattacks are likely to provoke violent responses, then arguably they ought to require congressional sign-off.

Real-world experience is still limited, and the escalation dynamics of cyberattacks are not yet well understood. That said, some studies suggest that cyberattacks are on the whole less likely than are kinetic attacks to provoke violent responses.[16] Some experimental data from crisis simulations indicates that even when they have destructive effects similar to those of conventional attacks, cyberattacks might not have the same political and emotional impacts that create pressures for violent retaliation (or even retaliation in cyberspace).[17] Other empirical and survey data show that, unlike conventional military attacks, cyber operations are not so escalatory and that they also offer escalatory off-ramps by providing response options other than conventional military conflict.[18] At several tense moments in 2019, for example, the United States reportedly chose to hit Iran with cyberattacks on military systems and intelligence facilities, rather than with kinetic strikes, in response to Iranian attacks on Saudi oil refineries and other provocations (including downing an American drone). That reporting suggests that the United States chose cyberattacks over kinetic ones in part because the former were viewed as less likely to drive escalation.[19]

Of course there may be exceptions, especially for devastating cyberattacks. Moreover, cyberattacks can have far-reaching unintended consequences that may magnify resultant international friction or the risk of escalation. For example, as mentioned in the introduction, malicious computer code (widely attributed to the United States) targeted at Iranian nuclear plant control systems accidentally spread around the world.[20] Russian malware targeting Ukraine in 2017 quickly spread, too, and with far greater damage, crippling computer systems across the globe.[21] Furthermore, cyber operations, whether intended to be offensive or defensive, will often be perceived as threatening by targeted states, contributing to instability.[22]

However, evidence does not to date indicate that the risks are high that cyberattacks will provoke conventional military responses. The risk is clearly not zero, and cyberattacks might also result in escalation of other hostile measures, including economic ones or retaliation in cyberspace. But the same is true of so many other instruments of state power—for example, economic sanctions or diplomatic recognition decisions could cause a target state to lash out—that we would never categorize as exercises of constitutional war powers.

Separate from the issues of direct costs and risks, another possible reason why it might make sense to categorize at least *some* cyberattacks as exercises of war powers for constitutional purposes is that states increasingly regard them as hostile military force as a matter of international law. This point is probably applicable only to cyberattacks that directly cause significant and direct physical destruction (say, causing a nuclear meltdown or plane crash) or that produce widespread harm (say, temporarily disabling a major electrical grid). The United States government has repeatedly asserted its right as a matter of international law to respond to some cyberattacks with kinetic military force, on the theory that cyberattacks could qualify as uses of "force" or "armed attacks" under the UN Charter.[23] Many other

powerful states agree with this view, and many academics—myself included—argue that some cyberattacks are appropriately analogized as an international legal matter to kinetic attacks.[24] Defend Forward generally involves US cyber operations well below these levels. Although treating some cyberattacks as uses of force or armed attacks for international law purposes may not be determinative, it at least lends logical support to the idea that very physically destructive cyberattacks (maybe a narrow category) should also qualify as uses of force for constitutional purposes and thus trigger war powers analyses.

The international law and constitutional law analyses need not match up this way, though. Formally, the relevant legal provisions differ: the Constitution obviously predates the UN Charter, for example, and contains an intersecting set of relevant powers that have never been interpreted to map one-for-one onto international law. Normatively, the UN Charter and international self-defense law are almost entirely grounded in preserving international peace and security, whereas constitutional war powers are grounded also in concerns about both accountability and domestic control of military power. And, methodologically, international law and constitutional law draw on different histories and argumentative strategies for filling in legal gaps and ambiguities.

In sum, kinetic military attacks are rarely the correct constitutional analogy for cyberattacks. Rather than a presumption that any cyberattack involves an exercise of war powers, the presumption ought to be the opposite: that it does not. Although this paper is concerned with constitutional issues, it is worth noting that according to this logic it is also doubtful that most cyberattacks alone would or should be considered "hostilities" triggering the statutory limitations of the War Powers Resolution.[25] War powers were carved out as a special constitutional category—one that originally required congressional approval for particular actions and that some argue still ought to—and there should be a strong reason to expand the category to cover new kinds of activities. It is not clear that most cyberattacks make the cut.

Defend Forward and Constitutional Powers

If cyberattacks rarely (if ever) are exercises of war powers, then what constitutional powers are cyberattacks exercises of? The short answer is: it depends.[26] It is a mistake to try to fit them all into any one constitutional category. Cyberattacks, as stated at the outset, make up a broad category of activities. They could range from taking down or even destroying critical infrastructure to spoofing internal communications, and many things in between, like temporarily knocking offline air defense systems. Depending on the facts, cyberattacks could be viewed as exercises of noncombat military powers, foreign affairs powers, intelligence powers, and commerce powers—as well as combinations of these and still other powers. This section uses the US Defend Forward concept to illustrate how those powers can apply, and it also applies them to other hypothetical or past cyberattacks that may even have significant and direct destructive effects.

Defend Forward involves proactively countering malicious adversary cyber campaigns through day-to-day competition. Defend Forward aims to disrupt adversary cyber operations, deter future campaigns, and reinforce favorable international norms through activity conducted beyond US networks—that is, activity inside adversary and third-party networks.[27] According to the 2018 Defense Department Cyber Strategy: "[The Department] will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."[28]

Most operations contemplated by the Defend Forward concept do not involve activities that would count as "cyberattacks." Such operations include establishing a presence in foreign networks, mapping those networks, gathering information, and preparing for future operations. Some Defend Forward activities are cyberattacks, though. These might include interrupting communications from an adversary military facility used to infiltrate US military command and control systems, inserting malware that deletes or encrypts data on servers engaged in malign foreign influence campaigns online, or denying service to networks used by adversary intelligence agencies to conduct industrial espionage. Such operations involve combinations of several constitutional powers.

As Military Activity

Assuming the operation is conducted by the military (presumptively, Cyber Command), one possibility is to treat it as an exercise of presidential power to engage in military activities, but not, for constitutional purposes, the hostile application of armed force. The president, as commander in chief of the armed forces, can take many steps using military forces—forces provided by Congress—that impose costs on adversaries or involve risks of retaliation or escalation, including moving combat forces into foreign theaters or engaging in military exercises.[29] US Attorney General Robert Jackson offered a classic formulation of this view in a 1941 opinion concluding that the president had constitutional authority to order the instruction of British pilots by American military service members at US training facilities. As commander in chief of the armed forces, Jackson noted, the president "has supreme command over the land and naval forces of the country and may order them to perform such military duties as, in his opinion, are necessary or appropriate for the defense of the United States. These powers exist in time of peace as well as in time of war."[30]

Cyberattacks carried out by the US military inside foreign networks to, for example, prevent or deter adversary efforts to infiltrate US information systems could be understood much like the training of British pilots aimed at undermining German air superiority; without physical destruction, they deny or degrade an adversary's cyber capability. For that matter, looking beyond Defend Forward, cyberattacks to degrade an adversary's offensive or defensive military capability might also be treated as analogous. Such cyberattacks include the reported 2019 US cyber operation that wiped out information systems used by Iranian forces to target ships.[31] Yes, these examples may involve electronic transgression of territorial

borders—and that may have international law implications—but any argument drawing constitutional conclusions from this fact just begs the question whether and how digital intrusion is constitutionally significant.

Importantly, although the president has wide latitude as commander in chief to engage in military activities other than force absent statutory restrictions, Congress restricts such types of military activities all the time. For example, Congress regulates the US military's training and equipping of foreign armed forces with substantive, procedural, and fiscal restrictions,[32] and Congress has historically imposed various types of restrictions on peacetime deployments of troops abroad.[33] Congress could likewise do more to limit military cyber activities but has so far chosen not to.

As Foreign Relations

If a cyberattack is intended more for its communicative impact than its military impact, it might better be thought of as modern-day "gunboat diplomacy." This framing draws heavily on both the president's general powers as chief executive to conduct foreign relations, including communicating threats, and his commander-in-chief powers to control military forces.[34] Temporarily taking offline an enemy's digital infrastructure might be analogized to overflying its territory, for example, as a show of capability that demonstrates adversary vulnerability.

One might object that comparing cyberattacks that destroy or degrade adversary systems to coercive diplomacy is inapt because the latter activities lack any direct contact with the adversary and its assets. After all, most uses of military force that would unquestionably implicate war powers—for example, punitive air strikes—are also intended more for their communicative impact than their direct damage. But drawing constitutional conclusions from this distinction again begs the question of what type of "contact" with the adversary moves an action into the constitutional category of war powers.

As Intelligence Activities

Many cyberattacks of the sort envisioned by Defend Forward also involve exercises of constitutional intelligence powers.[35] This is a blurry area of constitutional law because secrecy precludes the sort of public articulation of government legal analysis that often accompanies military intervention. The executive branch has argued that the president possesses broad authority, implicitly derived from the president's power to conduct foreign relations as well as his commander-in-chief powers, to engage in clandestine intelligence activities to undermine enemy political, economic, and military systems. Another view is that much of this power comes from statutory delegations from Congress, both express and implied.[36] Cyber operations designed only to collect information would clearly fit within the category of intelligence powers, but this essay is concerned with those intended to have disruptive or damaging effects.

The executive branch has at times taken the view that the president's power to engage in intelligence activities includes directing some quasi-military activities, such as paramilitary support to proxy groups or physical sabotage operations, as well as propaganda campaigns and other political manipulation when conducted covertly (that is, so that the hidden hand of the United States is plausibly deniable).[37] Whether some of those intelligence activities, particularly those involving physical violence, are really just a subset of war powers or a different constitutional category altogether—and one that did not become important until the Cold War—is unclear. Congress, for its part, has regulated covert intelligence activities by enacting procedural and reporting requirements, such as the covert action statute's requirements of presidential sign-off and notification to congressional intelligence committees.[38] Oversight statutes of this nature can be understood either as recognizing and limiting the president's broad inherent intelligence powers or as implicitly authorizing the president to engage in covert intelligence activities in the first place. Either way, the resulting institutional model is one in which the president has not been required to seek formal congressional approval for specific operations, but is required to meet other congressionally imposed requirements.[39]

Cyberattacks conducted as part of Defend Forward will often involve the exercise of intelligence powers, or perhaps can well be analogized to them. For starters, the means of cyberattacks—surreptitiously entering and mapping foreign information networks for vulnerabilities—is mostly an intelligence activity;[40] the difference between "defensive" intrusions and mapping of enemy networks and "offensive" disruptions of such networks may be relatively small pieces of computer code. Furthermore, even some cyber operations with damaging effects—such as altering data or implanting malware to disable or destroy digital systems—are akin to black bag jobs, propaganda operations, or covert support for proxy paramilitary forces, activities traditionally carried out by US intelligence agencies. A cyber operation like Stuxnet, which targeted militarily significant and sensitive sites and had significant, destructive physical effects, comes closer to an exercise of war powers but bears an even stronger resemblance to past exercises of intelligence powers, such as physical sabotage operations carried out by intelligence operatives or their proxies. Such operations are usually treated as a different constitutional category.

As Foreign Commerce

Yet another possibility is that cyberattacks are a form of meddling with international commerce, implicating the Constitution's allocation of foreign commerce powers. Domestically, telecommunications and other uses of the internet are uncontroversially understood to fall under Congress's Commerce Clause regulatory authority. Internationally, too, operations to halt, redirect, or otherwise interfere in digital information flows could be viewed as interventions into foreign commerce. I highlight this possibility because unlike the categories above, intervention in the flow of commerce is expressly Congress's domain: Article I assigns to Congress the power to regulate foreign commerce. International

commerce is also another arena in which the US government often wields tools—in the form of economic and financial sanctions—that impose damage on foreign states, organizations, and individuals in order to advance US foreign policy objectives. Indeed, it is in part because foreign commerce is so connected with national defense that Congress exercises much of its power in this area through broad delegations; it has granted the president wide discretion to take economic measures to deal with foreign emergencies or trade disputes, for example.[41]

For constitutional purposes it might seem like a stretch to analogize manipulating computer code or digital information flows across borders to manipulating trade in goods or services. So is analogizing such activities to dropping bombs or deploying troops, though. Moreover, whereas kinetic military attacks may have incidental effects on private, commercial property, some cyber operations use commercial infrastructure as an integral feature of attack.

Of course, cyberattacks might involve several or even all of these constitutional powers (noncombat military powers, foreign affairs powers, intelligence powers, commerce powers, and perhaps others). Indeed, depending on the specific facts, cyberattacks should be understood to involve various combinations of them. The main upshot is that while there could perhaps be instances where cyberattacks are exercises of war powers, such instances are exceedingly rare and limited to specific extreme cases. Most cyberattacks, especially ones that do not rise to the level of uses of force or armed attacks under international law, could fit in other categories. They could also form a new constitutional category altogether, for which the respective roles of Congress and the president are not yet established.

Congress and Cyber Strategy

As stated at the outset, one reason to resist categorizing cyberattacks as exercises of war powers is that the doctrinal fit is poor. That is not just rigid formalism; cyberattacks do not implicate the main concerns underlying war powers law, at least not to the same degree as does kinetic force. Another reason to resist that categorization is that it tends to limit thinking about institutional arrangements. In particular, critics of presidential war powers unilateralism tend to focus on specific congressional approval for actions, at least those beyond a certain threshold. It may seem natural, under that view, to demand specific congressional approval for cyberattacks or cyber campaigns beyond a certain threshold, too. Proponents of presidential war powers unilateralism, meanwhile, tend to see congressional regulation of such powers as dangerous, if not constitutionally suspect, meddling.

By contrast, the catalog of constitutional powers in the previous section, each of which involves potent tools of international competition and conflict, brings along a wide array of institutional arrangements. Moreover, to those who worry about executive unilateralism with regard to cyber operations—and who therefore seek to bolster congressional

checks and oversight—that catalog offers many more and stronger legal justifications for congressional involvement than does a legal framework rooted primarily in war powers. Congress shapes the use of noncombat military powers through, among other things, legislating military force structures and organizational arrangements, annual appropriations and authorization bills, and oversight processes. The president has a very free hand in exercising some foreign affairs functions, but Congress can shape most of them using powers of its own. Congress regulates intelligence largely through special oversight and statutory procedural requirements, and, especially when national security is involved, it often regulates international commerce through broad delegations of authority to the executive branch.

As Robert Chesney has shown, Congress is already quite engaged in shaping US cyber strategy, including pushing and facilitating more assertive uses of military cyber operations against particular adversaries.[42] That congressional involvement includes a wide range of institutional arrangements typical of coercive tools besides military force.

Congress has pressed the Defense Department to build up its offensive cyber capacity through annual National Defense Authorization Acts (NDAAs),[43] for example. It has clarified the Defense Department's authority to conduct offensive cyber operations,[44] thereby strengthening its position within the executive branch. Congress has also tried to streamline the internal executive-branch approval of cyber operations while setting outer boundaries on how those operations should be conducted. For example, it has provided clearer statutory authority for the Defense Department to conduct wide-ranging clandestine cyber operations considered short of hostilities, including in areas where hostilities are not occurring, thereby enabling quicker and more flexible Defense Department action in countering cyber adversaries outside US computer networks.[45]

Congress has acted to enhance oversight of cyberattacks, mandating special reporting requirements to the armed services committees for offensive and "sensitive" military cyber operations.[46] Cyberattacks conducted as covert action by the CIA are reported separately to the intelligence committees under long-standing arrangements, as are other intelligence activities that might fit within this essay's definition of cyberattacks. Such reporting is foundational to other congressional roles, because it keeps Congress—or at least certain committees—informed of executive-branch actions that would otherwise be largely invisible. As discussed above, cyberattacks are especially invisible compared to other methods of international conflict, so robust congressional oversight is arguably extra-important as a stand-in for public scrutiny. One continuing challenge for Congress, then, is to design more meaningful reporting requirements, especially ones that get at results of cyber operations—that is, that emphasize the outputs (which are difficult to assess) rather than just the inputs of US cyber activities themselves. Congress might partly address this issue by requiring notification of committees not only of operations and targets but also of certain types of collateral damage or effects.

In short, concern that cyber is an area of executive unilateralism is misplaced, especially when it comes to cyber operations conducted by the US military. Congress and the executive are already collaborating on a system built through interbranch deliberation, and invoking war powers—either along with a belief in broad inherent executive-branch authority or along with insistence on case-by-case congressional approval—is neither appropriate nor useful. As Chesney writes: "With little fanfare and less public notice, Congress and the executive branch have cooperated effectively over the past decade to build a legal architecture for military cyber operations."[47]

It is true that this legal architecture leaves the president with a lot of discretion to engage in cyber operations or cyberattacks, at least those that fall below a very high threshold constituting war (if one takes the view that cyberattacks alone could ever meet that bar), without getting additional congressional approval. That discretion is a product of both inherent constitutional power and delegated power from Congress.

At least with regard to Defend Forward, there is a powerful strategic logic to that vast zone of discretion. When it comes to using hostile kinetic military force, strategy usually involves specific breakpoints in time and conflict intensity: as tensions with a specific adversary rise, the United States sustains a military attack, or as a threat grows, the United States moves from not using force to using it. It is often an on/off switch. Normally, the military force switch is off, and at a particular moment the government turns it on. At that moment, constitutional war powers are activated.

In contrast to the on/off nature of most kinetic military intervention, Defend Forward involves a constant level of cyber conflict; the United States must be continually prosecuting it.[48] Cyber Command's chief and a top adviser recently described its implementation this way:

> Cyber Command implements this defend forward strategy through the doctrine of persistent engagement. The idea behind persistent engagement is that so much of the corrosive effects of cyber attacks against the United States occur below the threshold of traditional armed conflict. . . . This doctrine of persistent engagement reflects the fact that one-off cyber operations are unlikely to defeat adversaries. Instead, U.S. forces must compete with adversaries on a recurring basis, making it far more difficult for them to advance their goals over time.[49]

"There is also consensus across the U.S. government that great-power competitors are making strategic gains in and through cyberspace with persistent, targeted campaigns that never rise to the level of a catastrophic cyber attack," writes Emily Goldman, a policy official at Cyber Command and the National Security Agency. Therefore, "Competing below the level of armed conflict and contesting malicious cyber activity in day-to-day competition are consistent themes across the *National Defense Strategy*, the *National Military Strategy*, and the 2018 *Department of Defense Cyber Strategy*."[50]

The type of continuous agility called for in such situations matches especially poorly with the sort of rigid requirements for case-by-case congressional approval critics of unilateral presidential war powers often call for. The case-by-case model is workable when there is a clear and visible initiation point, or a break from baseline dormancy. The vast majority of US cyberattacks, however, will be part of constant and largely invisible campaigns against multiple adversaries simultaneously. Indeed, in recent years the executive branch has also instituted reforms to delegate decision making on cyber operations to lower levels of command, too, in order to better achieve that continuous agility.[51]

It may well be that Congress and future presidential administrations will move toward a different strategy. There may also be rare US offensive cyberattacks that look more like discrete applications of military force. For now, though, a war powers framing matches poorly the way the United States actually conducts cyberattacks.

Conclusion

Cyberattacks are a national capability the exercise of which usually involves no direct risk to American lives, is largely invisible to the public eye, could possibly but is relatively unlikely to escalate to conventional military conflict, and for which international law and norms are uncertain and evolving. At the most general level, this essay is about constitutional analogies: What exercises of power are cyberattacks most like? Constitutional categorization by analogy is important in this case not just for doctrinal reasons but because how one categorizes cyberattacks triggers certain conventions, practices, and political arguments regarding how overlapping executive and legislative power is shared.

Cyberattacks-as-war-powers is one possible answer, but it is rarely—and maybe never—a good fit. There are many other categories that, in combination, better fit most cyberattacks, including operations conducted as part of Defend Forward. Those categories provide better doctrinal justifications for executive action, as well as for congressional regulation. Viewing cyberattacks through those alternative lenses also helps to open up a wider array of institutional arrangements that more appropriately match emerging cyber strategy.

NOTES

1 This is similar to the way the Defense Department's Joint Publication 3–12 defines "cyberspace attack": "Cyberspace attack actions create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial effects in the physical domains." Joint Chiefs of Staff, Joint Pub. 3-12, Cyberspace Operations Core Activities II-7 (2018).

2 See Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, Wired (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world; David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. Times (June 1, 2012), https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

3 *See* Ellen Nakashima, *U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms*, Wash. Post (Feb. 27, 2019), https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

4 *See, e.g.*, Lyle Denniston, *Constitution Check: Is the War Powers Clause a Dead Letter in the Cyberspace Age?*, Nat'l Const. Ctr. (Feb. 5, 2013), https://news.yahoo.com/constitution-check-war-powers-clause-dead-letter-cyberspace-113217808.html; Stephen Dycus, *Congress's Role in Cyber Warfare,* 4 J. Nat'l Sec. L. & Pol'y 155 (2010); Jason Healey & A.J. Wilson, *Cyber Conflict and the War Powers Resolution: Congressional Oversight of Hostilities in the Fifth Domain*, 5 Geo. J. Int'l Aff. 59 (2012); Tyler K. Lowe, *Mapping the Matrix: Defining the Balance Between Executive Action and Legislative Regulation in the New Battlefield of Cyberspace*, 17 Scholar 63 (2015).

5 *See, e.g.*, Eric Talbot Jenson, *Future War and the War Powers Resolution*, 29 Emory Int'l L. Rev. 499 (2015); Oona A. Hathaway, *How to Revive Congress' War Powers*, 3 Tex. Nat'l Sec. Rev. 136 (2019).

6 2 The Records of the Federal Convention of 1787, at 318 (Max Farrand ed., rev. ed. 1966); *see also, e.g.*, John Hart Ely, War and Responsibility: Constitutional Lessons of Vietnam and Its Aftermath 3–10 (1993); Arthur M. Schlesinger, Jr., The Imperial Presidency 1–26 (Mariner Books ed. 2004).

7 *See* 3 Joseph Story, Commentaries on the Constitution of the United States 59–61 (1833).

8 *See generally* Schlesinger, *supra* note 6, at 27–201.

9 *See, e.g.*, Memorandum Opinion from Caroline D. Krass, Principal Deputy Assistant Att'y Gen., Office of Legal Couns., to the Att'y Gen., Authority to Use Military Force in Libya (Apr. 1, 2011); Memorandum Opinion from Steven A. Engel, Office of Legal Couns., to the Couns. to the President, April 2018 Airstrikes Against Syrian Chemical-Weapons Facilities (May 31, 2018).

10 Hon. Paul C. Ney, Jr., DOD General Counsel Remarks at U.S. Cyber Command Legal Conference (Mar. 2, 2020), https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference.

11 *Id*.

12 *Id*.

13 *See* sources cited *supra* note 9.

14 *See* Jack Goldsmith & Matthew Waxman, *The Legal Legacy of Light-Footprint Warfare*, 39 Wash. Q. 7, 18 (2016).

15 *See* Engel, *supra* note 9, at 21.

16 *See* Erica D. Borghard & Shawn W. Lonergan, *Cyber Operations as Imperfect Tools of Escalation*, 13 Strategic Stud. Q. 137 (2019). For an excellent discussion of cyberattacks and crisis stability, see also Jason Healey & Robert Jervis, *The Escalation Inversion and Other Oddities of Situational Cyber Stability*, 3 Tex. Nat'l Sec. Rev. (2020), https://tnsr.org/2020/09/the-escalation-inversion-and-other-oddities-of-situational-cyber-stability/.

17 *See* Jacquelyn G. Schneider, *Deterrence in and through Cyberspace*, *in* Cross-Domain Deterrence: Strategy in an Era of Complexity 95 (Eric Gartzke & Jon R. Lindsay eds., 2019); Jacquelyn G. Schneider, *What War Games Tell Us About the Use of Cyber Weapons in a Crisis*, Council on Foreign Rels. (June 21, 2018), https://www.cfr.org/blog/what-war-games-tell-us-about-use-cyber-weapons-crisis.

18 *See* Benjamin Jensen & Brandon Valeriano, Atlantic Council, What Do We Know About Cyber Escalation? Observations from Simulations and Surveys (2019), https://www.atlanticcouncil.org/wp-content/uploads/2019/11/What_do_we_know_about_cyber_escalation_.pdf; Brandon Valeriano & Benjamin Jensen, *How Cyber Operations Can Help Manage Crisis Escalation with Iran*, Wash. Post (June 25, 2019), https://www.washingtonpost.com/politics/2019/06/25/how-cyber-operations-can-help-manage-crisis-escalation-with-iran/.

19 *See* Idrees Ali & Phil Stewart, *U.S. Carried Out Secret Cyber Strike on Iran in Wake of Saudi Oil Attack: Officials*, Reuters (Oct. 15, 2019), https://www.reuters.com/article/us-usa-iran-military-cyber-exclusive/exclusive-u-s-carried-out-secret-cyber-strike-on-iran-in-wake-of-saudi-oil-attack-officials-idUSKBN1WV0EK; Julian E. Barnes & Thomas Gibbons-Neff, *U.S. Carried Out Cyberattacks on Iran*, N.Y. Times (June 22, 2019), https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html; Sean Lawson, *What Will Be the Effect of the Latest US Cyberattack on Iran?*, Fifth Domain (Oct. 23, 2019), https://www.fifthdomain.com/thought-leadership/2019/10/23/what-will-be-the-effect-of-the-latest-us-cyberattack-on-iran; Anya van Wagtendonk, *Trump Called Off a Military Strike Against Iran. The US Targeted Its Computer Systems Instead*, Vox (June 23, 2019), https://www.vox.com/2019/6/23/18714327/iran-us-donald-trump-cyberattack-drone-strike.

20 Vivian Yeo, *Stuxnet Infections Spread to 115 Countries*, ZDNet (Aug. 9, 2010), https://www.zdnet.com/article/stuxnet-infections-spread-to-115-countries.

21 Greenberg, *supra* note 2.

22 *See generally* Ben Buchanan, The Cybersecurity Dilemma (2017).

23 For a discussion of US government positions on this point, see *Cyber Strategy & Policy: International Law Dimensions: Hearing Before the S. Armed Forces Committee*, 115th Cong. 18 (2017) (statement of Matthew C. Waxman, Liviu Librescu Professor of L., Columbia L. School). The United States and many others also apply *jus in bello* rules to cyberattacks in the course of armed conflict.

24 *See, e.g.*, Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 Yale J. Int'l L. 421 (2011); Michael N. Schmitt, *Noteworthy Releases of International Cyber Law Positions—Part I: NATO*, Articles of War (Aug. 27, 2020), https://lieber.westpoint.edu/nato-release-international-cyber-law-positions-part-i.

25 That is especially so if one applies that interpretation of the War Powers Resolution advanced by the Obama administration during the 2011 Libya intervention. In that case, the executive took the position that "hostilities" did not exist because the mission, exposure of US armed forces, risk of escalation, and military means were all limited. *See Libya and War Powers: Hearing Before the S. Comm. on Foreign Relations*, 112th Cong. 89 (2011) (statement of Harold Koh, Legal Adviser, U.S. Dep't. of State).

26 *See* Gary P. Corn, *Cyber National Security: Navigating Gray-Zone Challenges in and through Cyberspace*, *in* Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare 367 (Christopher M. Ford & Winston S. Williams eds., 2019) (explaining that for many offensive cyber operations "the scope of the President's authority is more nuanced as it implicates the full range of Article II authority, not just the commander-in-chief power, and is further complicated by the novelty and uncertainties surrounding the use of cyber operations as a tool of national power").

27 *See* Erica D. Borghard, *Operationalizing Defend Forward: How the Concept Works to Change Adversary Behavior*, Lawfare (Mar. 12, 2020), https://www.lawfareblog.com/operationalizing-defend-forward-how-concept-works-change-adversary-behavior.

28 U.S. Dep't. of Def., Summary: Department of Defense Cyber Strategy 1 (2018).

29 *See* W. Taylor Reveley III, War Powers of the President and Congress: Who Holds the Arrows and the Olive Branch? 15–16 (1981).

30 Training of British Flying Students in the United States, 40 Op. Att'y Gen. 58, 61 (1941).

31 *See* Julian E. Barnes, *U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say*, N.Y. Times (Aug. 28, 2019), https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html.

32 *See* Bolko J. Skorupski & Nina M. Serafino, Cong. Rsch. Serv., R44602, DOD Security Cooperation: An Overview of Authorities and Issues (2016).

33 *See* Jennifer K. Elsea et al., Cong. Rsch. Serv., R41989, Congressional Authority to Limit Military Operations (2013).

34 *Cf.* United States v. Curtiss-Wright Export Corp., 299 U.S. 304, 319 (1936) (discussing the president as the sole organ of the nation in its external relations).

35 *Cf.* Joshua Rovner, *Cyber War as an Intelligence Contest*, War on the Rocks (Sept. 16, 2019), https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest.

36 For a discussion of these perspectives, and a critique of the executive branch view, see Jules Lobel, *Covert War and the Constitution*, 5 J. Nat'l Sec. L. & Pol'y 393 (2011).

37 *See, e.g.*, *Intelligence Oversight Act of 1988 and National Security Reform Act of 1987: Hearing on S. 1721 and S. 1818 Before the S. Select Comm. on Intelligence*, 110th Cong. 93 (1987) (prepared statement of Charles J. Cooper, Assistant Att'y Gen. for the Office of L. Couns.); *Hearings on S. Res. 21 before the S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities*, 94th Cong. 1730–37 (1975) (statement of Mitchell Rogovin, Special Couns., Dir. of Nat'l Intel.); *see also* Richard O.W. Morgan & Jonathan M. Fredman, *The Law of Foreign and National Intelligence*, *in* National Security Law & Policy 1041, 1048 (John Norton Moore, Guy B. Roberts & Robert F. Turner eds., 3rd ed. 2015) (discussing covert action as a category of intelligence activities with a foundation in the president's Article II powers).

38 50 U.S.C. § 3093 (2018).

39 *See* M.E. Bowman, *Secrets in Plain View: Covert Action the U.S. Way*, 72 Int'l L. Stud. 1, 10 (1998) ("Although the precise authority for covert action is debatable, it is clear that both the Congress and the Executive believe it a necessary option. Both presume that legal authority exists to engage in covert action and each presumes to have a Constitutionally authorized, if not precisely defined, role.").

40 Robert Chesney, *Military-Intelligence Convergence and the Law of the Title 10/50 Debate*, 5 J. Nat'l Sec. L. & Pol'y 539, 580 (2012).

41 *See* Christopher A. Casey, Ian F. Ferguson, Dianne E. Rennack & Jennifer K. Elsea, Cong. Rsch. Serv., R45618, The International Emergency Economic Powers Act: Origins, Evolution, and Use (2020).

42 Robert Chesney, *The Domestic Legal Framework for US Military Cyber Operations* 3 (Hoover Working Group on Nat'l Sec., Tech., and Law, Aegis Series Paper No. 2003, 2020).

43 *See, e.g.*, National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114–328, § 923, 30 Stat. 2000, 2357 (2016) (creating a unified combatant command for cyber).

44 *See* National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112–81, § 954, 125 Stat. 1298, 1551 (2011); 10 U.S.C.A. § 111 note; National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115–91, § 1633(a), (b)(5)(B), 131 Stat. 1283, 1738–39 (2017).

45 National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115–232, § 1632, 132 Stat. 1636, 2123–24 (2018); 10 U.S.C. § 394 (2018).

46 The 2013 NDAA required DOD to "provide to the Committees on Armed Services of the House of Representatives and the Senate quarterly briefings on all offensive and significant defensive military operations in cyberspace carried out by the Department of Defense during the immediately preceding quarter." National Defense Authorization Act for Fiscal Year 2013, Pub. L. No. 112–239, § 939, 126 Stat. 1632, 1888 (2013); 10 U.S.C. § 484 (2018). This provision was updated and expanded in the 2017 and 2019 NDAAs to add and amend the required elements of these reports.

47 Chesney, *supra* note 42, at 1.

48 One might, however, compare the long-term, constant features of cyber conflict to ongoing counterterrorism operations, especially since 2001.

49 Paul M. Nakasone & Michael Sulmeyer, *How to Compete in Cyberspace: Cyber Command's New Approach*, Foreign Aff. (Aug. 25, 2020), https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.

50 Emily O. Goldman, *From Reaction to Action: Adopting a Competitive Posture in Cyber Diplomacy*, 3 Tex. Nat'l Sec. Rev. (2020), https://tnsr.org/2020/09/from-reaction-to-action-adopting-a-competitive-posture-in-cyber-diplomacy.

51 *See* Jacquelyn Schneider, *Are Cyber-Operations a U.S. Retaliatory Option for the Saudi Oil Field Strikes? Would Such Action Deter Iran?*, Wash. Post (Oct. 1, 2019), https://www.washingtonpost.com/politics/2019/10/01/are-cyber-operations-us-retaliatory-option-september-oilfield-strikes-would-this-deter-iran.

26 25 24 23 22 21 20 7 6 5 4 3 2 1

The preferred citation for this publication is Matthew C. Waxman, *Cyberattacks and the Constitution*, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2007 (November 10, 2020), available at https://www.lawfareblog.com/cyber-attacks-and-the-constitution.

About the Author

MATTHEW C. WAXMAN

Matthew C. Waxman is the Liviu Librescu Professor of Law at Columbia Law School, where he chairs the National Security Law Program. He is also adjunct senior fellow at the Council on Foreign Relations and a faculty affiliate of Columbia University's Data Science Institute Cybersecurity Center. He has served in senior roles at the US State Department, Defense Department, and National Security Council.

Working Group on National Security, Technology, and Law

The Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cybersecurity, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The group's output will also be published on the *Lawfare* blog, which covers the merits of the underlying legal and policy debates of actions taken or contemplated to protect the nation and the nation's laws and legal institutions.

Jack Goldsmith is the chair of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at http://www.hoover.org/research-teams/national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
The Johnson Center
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION