A HOOVER INSTITUTION ESSAY

The Domestic Legal Framework for US Military Cyber Operations

ROBERT CHESNEY

Aegis Series Paper No. 2003

Conventional wisdom holds that Congress has abandoned its duty regarding the government's war powers. It is not hard to understand why. Between the agelessness and flexibility of the 2001 and 2002 Authorizations for Use of Military Force[1] (AUMFs) and periodic unilateral uses of military force in Libya, Syria, and Iraq, the executive branch appears to act largely at its own discretion when it comes to conventional military operations. But matters are different in the cyber domain. 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. This framework reflects recurring and constructive congressional engagement. The resulting structure is far less familiar to most observers than its cousins—those architectures associated with conventional military operations and intelligence activities—but is no less important. This is particularly true in light of the Pentagon's commitment to the "defend forward" operational model.

Context: Defending Forward

Amid the fallout from the coronavirus pandemic, a group of senators from both major political parties dispatched a remarkable letter in April 2020 to General Paul Nakasone, commander of US Cyber Command (USCYBERCOM). The senators expressed "profound concerns" about "sophisticated hacking operations" targeting pandemic-related health services and research programs. In particular, they cited activity attributed to Russia, China, Iran, and North Korea. The letter concluded by asking Nakasone to "evaluate further necessary action to *defend forward* in order to detect and deter" such activity.[2]

What did they mean by "defend forward"? For anyone who had been following the evolution of the policy and legal frameworks associated with USCYBERCOM in recent years, the phrase was a familiar and significant one.

In the spring of 2018, Nakasone released a "command vision" document calling for USCYBERCOM to sustain an operational tempo of continuous—or persistent—engagement with adversaries in the cyber domain. Of course, those adversaries were already persistently engaging the United States through intrusions into US networks. The real novelty in Nakasone's vision was his insistence that USCYBERCOM need not remain in a defensive crouch, defending largely or even solely from within its own networks. Instead, it could and should focus on "defending forward as close as possible to the origin of adversary activity

[in order to extend] our reach to expose adversaries' weaknesses, learn their intentions and capabilities, and counter attacks close to their origins." By defending forward, persistent engagement could be made to impose "tactical friction and strategic costs on our adversaries," rather than vice versa.[3] The 2018 Defense Department Cyber Strategy, released later that year, affirmed the concept, "direct[ing] the Department to defend forward."[4]

Introduction of the defend forward strategy sparked a great deal of debate.[5] For some, the phrase appeared euphemistic, masking what might better be described as offensive operations. A Chinese scholar (and former People's Liberation Army colonel) insisted that the new posture would be destabilizing.[6] But for others, defending forward was a welcome development that was, if anything, long overdue given the growing array of hostile cyber activities directed against US interests.[7]

In the two years since the release of General Nakasone's command vision, we have had several glimpses of defend forward in action. Some examples—such as USCYBERCOM's forward deployment to help countries like Macedonia, Ukraine, and Montenegro defend their networks—have been innocuous (though still important) in that they did not necessarily involve operational activity in "red space"—that is, in an adversary's systems.[8] But the broader potential of the concept also has been on display. At the time of the 2018 midterm elections, for example, USCYBERCOM disrupted the networks of the "Internet Research Agency," the infamous Russian troll farm known for its efforts to spread propaganda in the United States during the 2016 election, and directly messaged individual Russian hackers in order to make clear that the United States was aware of their roles and identities.[9]

Against this backdrop, it is not hard to understand the real meaning of the senators' request that Nakasone explore opportunities to "defend forward" in the face of Russian, Chinese, Iranian, and North Korean hacking directed at pandemic-related medical and research entities in the United States. Simply put, the senators wanted USCYBERCOM operating inside the networks of those adversaries, at the very least to identify such activities but if necessary to go further and shut them down at their source.[10]

Whether or not USCYBERCOM conducts such high-stakes operations, the prospect draws attention to a critical question that lurks in the background of out-of-network operations in general but especially those targeting the systems of foreign governments: What is the domestic legal framework that governs them?

The question matters in circumstances beyond the prospect of responding to pandemic-related espionage, of course. There is a presidential election on the horizon, and given the events of 2016 and 2018, we can expect ample need for disruption in adversary networks in order to prevent interference of various kinds—and, therefore, a corresponding need

to establish and maintain access in advance. We also should not lose sight of the fact that USCYBERCOM's capacity for out-of-network operations is not limited to the defend-forward scenario. As illustrated by the summer 2019 crisis in which USCYBERCOM carried out disruption operations against Iranian assets after Iran shot down a US Navy surveillance drone (providing what proved to be a de-escalatory response at a time when the White House reportedly was considering missile strikes), there are times when such operations are intended to achieve effects unrelated to detecting, deterring, or disrupting an adversary's out-of-network operations.[11]

In short, the desire to conduct such operations will arise in a wide array of settings, and in many of them the stakes will be quite high. This places considerable pressure on the domestic legal framework that governs such operations.

In the pages that follow, I describe that framework in detail, emphasizing how Congress and the executive branch have collaborated in recent years to create a system that facilitates—but also monitors—precisely the sort of operations described above. I do so by breaking the framework down into four constituent elements:

- **Authorization** rules (which allocate decision-making authority between Congress and the executive branch);
- **Process** rules (which impact the decision-making process within the executive branch);
- **Transparency** rules (which compel the executive branch to share information with Congress); and
- **Substantive** rules (which prohibit certain actions).

Authorization Rules

Military cyber operations, like military operations in general, raise complex separation of powers questions. In what circumstances has Congress authorized such actions by statute, thus rendering constitutional issues moot? To what extent can the executive branch act in the absence of statutory authorization, relying instead on authority from Article II of the Constitution? And what about Congress's major effort to curb executive branch military unilateralism, the War Powers Resolution?

Existing Statutory Authority

At the time of this writing in the summer of 2020, three statutes provide some degree of authorization for military cyber operations. Two are generally applicable military authorizations, while the third is specifically focused on USCYBERCOM.

Let's start with the two generally applicable military authorizations. First and most famously, the 2001 AUMF[12] remains on the books. It authorizes the president to use "all necessary and appropriate force" against groups and individuals whom the chief executive determines to have come within the AUMF's scope. Second, the 2002 AUMF,[13] relating to Iraq, also remains active. Together, they eventually became the basis for the full spectrum of military operations directed against the Islamic State in Syria and Iraq. These operations came to include an array of cyber activities conducted by Joint Task Force-Ares.[14] In contexts properly associated with either or both of these AUMFs, therefore, the simplest answer to the war powers question is that Congress has authorized the use of military force generally, and this encompasses operations that happen to be carried out in the cyber domain.

However broad the two AUMFs may be, though, they are not limitless. And so it matters whether there is any separate statute authorizing military cyber operations in other settings.

The answer is yes: Section 1642 of the John McCain National Defense Authorization Act (NDAA) for fiscal year 2019[15] eliminates any doubt about the authority of the executive branch to conduct cyber activities in response to certain provocations. Specifically, Section 1642 authorizes USCYBERCOM to "take appropriate and proportional action in foreign cyberspace" in order "to disrupt, defeat, and deter" ongoing adversarial activity in the cyber domain, though only where the National Command Authority—the president and secretary of defense or their deputized alternates—determines that two conditions have been met:

> (1) there is "an active, systematic, and ongoing campaign of attacks against the Government or people of the United States in cyberspace, including attempt[s] to influence American elections and democratic political processes" and
>
> (2) the entity deemed responsible for the campaign is Russia, China, North Korea, or Iran.

The importance of Section 1642 for the defend-forward concept should be apparent. Section 1642's triggering conditions read like a road map to the most strategically significant areas in which the defend-forward concept might be employed: those involving systematic adversarial activity conducted by any of the four countries usually considered primary threats to the United States in the cyber domain. This is not an accident. The act's legislative history makes clear that Congress intended for it to prune away any lingering concerns about whether USCYBERCOM has the authority to conduct cyber operations in these circumstances.

Note, however, that the relative specificity of Section 1642 raises a further question: Do its narrowing conditions imply that all *other* USCYBERCOM operations of the defend-forward or offensive varieties are illegal, absent fresh legislation or a colorable AUMF argument? No. The best understanding of Section 1642 is that it functions as a belt-and-suspenders

provision, mooting separation-of-powers objections that might otherwise arise. It does not, however, concede that those objections would have been well-taken without Section 1642. (Certainly nothing in the text or legislative history suggests such an understanding by Congress or the president.) From that point of view, the question that arises for any operation that falls outside the scope of the AUMFs and Section 1642 is the same question that existed prior to Section 1642's passage: Does a given operation even require congressional authorization in the first place, or does Article II of the Constitution confer adequate authority for the executive branch to conduct the operation?

Authority to Conduct Cyber Operations Without Statutory Authorization

The Office of Legal Counsel (OLC) has in recent decades, under administrations of both major political parties, employed a consistent framework to determine when a military operation requires separation-of-powers analysis. That framework is described in both an Obama-era analysis of the legality of using force against the Qaddafi regime in Libya in 2011 and again in a Trump-era analysis involving force against the Assad regime in Syria in 2018. In each one, the OLC takes the position that the separation-of-powers issue arises only when the military activity in question reaches the level of "war." In this instance, *war* is a constitutional term of art turning on a variety of factors, including whether service members' lives are at risk on a sustained basis.[16] As the Syria opinion puts it: "Consistent with that early recognition, we have repeatedly distinguished between limited hostilities and prolonged and substantial military engagements, typically involving exposure of U.S. military personnel to significant risk over a substantial period."[17] Under that analysis, the OLC concluded that a substantial (though localized) kinetic strike on a Syrian military airfield did not rise to the level of war, nor did the much more substantial and sustained campaign of airstrikes that ultimately played a key role in toppling the Qaddafi regime.

So long as *that* is the framework for determining when congressional authorization might be required, military operations conducted in the cyber domain, standing alone, will not likely qualify as war, barring the most extreme fact patterns. (For example, it is conceivable that an operation that would deprive a large population of electricity for a long period would entail enough anticipated harm to compel a different conclusion despite the absence of boots on the ground, though even that is unclear under the OLC's exceedingly narrow approach.) Put simply, most if not all cyber operations, when analyzed standing alone, will fall short of this standard and thus not require a constitutional war powers analysis.

What about the War Powers Resolution?

What of the War Powers Resolution of 1973?[18] The WPR is best understood as an attempt by Congress both to reinforce a particular vision of the Constitution's distribution of war powers and to generate a set of new transparency rules increasing congressional awareness of the executive branch's more significant decisions relating to the use of the military. I will review those rules in the appropriately labeled section below. For now, I will focus on how

the attempt to reinforce Congress's conception of the distribution of war powers relates to USCYBERCOM's out-of-network operations.

The WPR addresses the distribution of war powers in two ways. First, it provides a statement of Congress's views on the doctrinal boundaries between the respective roles of Congress and the president in this area. Second, it attempts to put teeth into this vision by establishing a deadline for the withdrawal of US armed forces from certain situations absent sufficient congressional authorization.

Let's turn first to the WPR's claims about the Constitution. As a mere statute, of course, the WPR cannot actually alter the Constitution's allocation of military authority between Congress and the president. But since the details of the Constitution's allocation are themselves contested (as noted earlier), this part of the WPR might bear weight in interpretive calculations with some audiences, and thus it warrants brief consideration here.

The WPR opens with an assertion of Congress's view of when the president has the authority "to introduce United States Armed Forces into hostilities, or into situations where imminent involvement in hostilities is clearly indicated by the circumstances." Specifically, it claims that there are three such circumstances: "(1) a declaration of war, (2) specific statutory authorization, or (3) a national emergency created by attack upon the United States, its territories or possessions, or its armed forces."[19] First, note that this list seems incomplete insofar as it omits, for example, the use of the armed forces to protect citizens abroad. That said, the provision hinges entirely on the meaning of *hostilities*. This is a statutory term of art, and if it is interpreted to be coextensive with the OLC's understanding of the constitutional term of art *war,* then much if not all of the potential tension between this language and the OLC's constitutional analysis described above simply drops out.

Perhaps not surprisingly, the executive branch has interpreted *hostilities* that way. The best illustration, including a summation of past executive interpretations, may be the testimony in 2011 before the Senate Foreign Relations Committee of Harold Koh, at the time the State Department legal adviser. He explained the Obama administration's interpretation of *hostilities* for the purpose of analyzing the WPR's implications in the United States' continuing role in the Libya conflict.[20] Citing the course of practice since 1973 along with a consistent interpretive practice by the executive branch, Koh identified a set of factors that compelled the conclusion that America's actions did not constitute the introduction of our armed forces into hostilities—notwithstanding the existence of armed conflict and direct participation by the United States in the form of airstrikes. Specifically: the mission had a very limited purpose; the risk of US casualties was almost nonexistent since our role did not include boots on the ground; the risk of unintended escalation also was almost nonexistent for the same reason; and the military means employed were quite limited (and certainly far short of a "full military engagement"). Koh cautioned, however, that the answer might be different were any of these factors not present.

As with the interpretation of *war* for purposes of constitutional analysis, the executive branch's restrictive interpretation of *hostilities* is contested. But insofar as the executive interpretation continues to prevail in practice, as it did in Libya, it is clear that military activities in the cyber domain, analyzed as a stand-alone proposition, would not constitute the introduction of US forces into hostilities. The executive branch's decision to prioritize in the analysis the physical exposure of US service members foreordains this outcome.

In light of this analysis, the second feature of the WPR's attempt to regulate the distribution of war powers—that is, its attempt to establish an automatic deadline for the withdrawal of US forces in the form of a sixty-day "clock"—has little practical relevance for military operations in the cyber domain, at least when one analyzes such operations on a stand-alone basis. If cyber operations do not constitute the introduction of armed forces into "hostilities" (or into situations where hostilities are imminent) in the first place, the sixty-day clock never starts running.

A note of caution before moving on from these authorization rules: It should be obvious that the executive branch's restrictive approach to both "war" and "hostilities" depends upon an increasingly dated understanding of the manner and means through which the United States projects military power. Disruptive technological changes with respect to the array of capabilities for delivering kinetic attacks without placing service members in range of hostile fire, not to mention the emergence of the cyber domain in its entirety, are producing an ever-larger set of circumstances in which the United States can exercise coercion without putting troops in harm's way. To be sure, this dynamic should not change the "war" and "hostilities" analyses if in both cases the ultimate determining factor is indeed whether service members' lives are in immediate danger. But if instead considerations of escalation risk drive these analyses, their logical foundations are eroding. All of which is another reason to continue to pay attention to the potential applicability of the AUMFs and Section 1642 of the NDAA when analyzing particular operational proposals, since those authorities obviate the "war" and "hostilities" questions where they apply.

Process Rules

Proceeding on the assumption that the executive branch as a whole has the authority to conduct a particular military operation in the cyber domain (whether based on Section 1642, one of the AUMFs, or Article II), the next question is whether the domestic legal architecture requires compliance with certain decision-making procedures. More specifically, does the law require the approval of a particular person before the operation can take place?

The idea that certain operations cannot occur without the approval of particular persons is hardly foreign to military operations. From the commander in chief on down, it is common to use this approach in order to ensure that matters of particular sensitivity are decided only at higher levels in the chain. It is a matter of policy preference, expressed in the form of rules of engagement, execute orders, orders from the combatant commander, and so forth.

What we are not accustomed to seeing in the military context is *legislation* that effectively does the same thing, mandating that certain military decisions be made only with the approval of, say, the commander in chief.

Contrast that with the legal framework governing covert action—which, as we shall see, has special relevance for the cyber domain. Famously, Congress in 1974 broke new ground (in the so-called Hughes-Ryan Amendment[21]) by leveraging the power of the purse to insist upon a documentable presidential role in authorizing covert action. Specifically, Congress forbade the expenditure of funds by or on behalf of the CIA for overseas operations intended for purposes other than intelligence collection, absent what would come to be known as a presidential "finding." This was a quaintly coy way of describing covert action (i.e., operations intended to cause overseas effects where the sponsoring role of the US government is not meant to be apparent or acknowledged) and mandating that the president take personal, written responsibility for approving such operations.[22]

Why did Congress do this? The *effect* was to eliminate presidential "deniability"—that is, the situation in which a president might plausibly claim to have not known of a program. But the *reason* for doing it? The normative justification for mandating a presidential finding—the public policy gain from doing so—is that the certainty of presidential accountability naturally tends to harness the self-interest of an administration, increasing incentives for it to screen out bad or unduly risky ideas ex ante. Indeed, over time this has resulted in the executive branch's adoption of vetting procedures through which proposed covert action programs are filtered within the larger National Security Council system.[23] Those procedures, notably, have a substantial interagency element to them, giving rise to the possibility that agencies with different equities, such as the State Department, will have a chance to weigh in on the wisdom and desirability of a proposed operation. The end result is a system that is less quick and efficient than what existed before and one that might even defeat some good-but-risky ideas. Yet on the whole it strikes a reasonable balance in a situation that can entail unusually serious risks in the event of a miscalculation, risks ranging from diplomatic friction to war.

If Congress had defined the scope of the covert action framework in institutional terms, applying it solely to deniable operations conducted by the Central Intelligence Agency, then we would now move on to ask whether Congress has adopted (or should adopt) something comparable for military operations in the cyber domain. But Congress did not so limit the covert-action framework. Rather, it created a two-step definition of covert action that left ample room for debate over its scope. At step one, the definition is inclusive of all parts of the US government: "covert action" as a default matter applies to *any* part of the US government that implements an operation intended to have an overseas effect with the sponsoring role of the United States neither apparent nor acknowledged. But at step two, the statute excludes various situations, including "activities the primary purpose of which is to acquire intelligence" as well as "traditional . . . military activities" (often referred to as "TMA").[24]

Note the relevance of the intelligence-collection exemption for military activities in the cyber domain. There are many circumstances in which penetration of (and persistence within) someone else's network can fairly be described as activities whose "primary purpose" is intelligence collection, even though it is foreseeable that the very same access at some point might be used to generate an effect. If and when a decision is made to seek such an effect, of course, some other exception—most likely TMA—must apply or else the covert-action default rules will snap into place. But prior to that point, and for so long as it can be said fairly that the operation is primarily about acquiring information, the intelligence exception resolves the issue and obviates the need to wrestle with the question of just what counts as TMA in the cyber domain. Then again, as I will explain in more detail, characterizing an operation in this way rather than TMA potentially implicates the transparency rules that require keeping the two congressional Intelligence Committees fully apprised of significant intelligence activities. This fact alone might provide a significant incentive (from the military's perspective) for applying the TMA label instead.

All that being the case, what actually counts as TMA in the cyber domain? Had Congress simply used the shorter phrase "military activities" in crafting this exception, it would not be a difficult question. But that is not what Congress did. The *T* in *TMA* stands for *traditional*, and this term has invited debate over the scope of the exception. That debate in turn has cast a shadow over the decision-making process for some military activities in the cyber domain.[25]

The TMA-scope issue is not just a cyber-domain matter. It first became a significant issue in the post-9/11 period thanks to noncyber, special-operations activities taking place away from combat zones. It has since become an issue with respect to military operations in the cyber domain as well.

In the two settings, the stakes are the same: If an operation is "in scope" for the TMA exception, it can be approved without a written presidential "finding" (and without the need for reporting to the House and Senate Intelligence Committees, in accordance with the transparency rules discussed in the next section). But if it does *not* qualify for the TMA exception, the opposite is true.

Complicating matters further, if the TMA exception does not apply to a proposed operation, an issue also might arise under Executive Order 12333's default rule providing that the CIA shall have responsibility for conducting "covert action" outside of contexts covered by a declaration of war or at least a notification under the War Powers Resolution.[26] The president, of course, can choose to direct the military to conduct the covert activity instead but in that case would need to make a specific determination on that point—thus ensuring elevation of the issue to the White House level in any event.

In recent years, such issues have proved to be a significant source of friction in the approval of military operations in the cyber domain. Such operations by their nature require

concealment, at least at the stage of establishing and maintaining access to a system (though concealment may or may not remain necessary at the point of seeking an operational effect via that access), and at times they involve maintaining a presence on systems or networks in contexts in which it would be preferable not to acknowledge American responsibility in the event the presence is detected.

The fact that confusion would arise about TMA's applicability in this circumstance is not surprising. First, there has long been disagreement between those who focus on the word *traditional* in *TMA* (and thus attempt to resolve the scope question by pondering whether cyber operations are sufficiently analogous to military operations, with their longer historical pedigree) and those who, instead, focus on the specific definitional compromise that Congress and the administration of President George H. W. Bush worked out on this point at the time of the relevant statutory enactment (in which case TMA applies to any operation that is [a] both commanded and implemented entirely by service members and [b] conducted in a context in which hostilities are ongoing or in which operational planning for hostilities has been approved by the National Command Authority). Second, even if everyone accepted and tried to apply the latter approach, hard questions might (and presumably did) arise with respect to whether a particular proposed operation relates sufficiently to a situation for which operational planning has been approved. Particularly in the context of gray zone engagements in the cyber domain, it is not hard to imagine circumstances for which that connection might be tricky to establish.

The first public sign of congressional concern about this issue emerged in 2011. The National Defense Authorization Act for fiscal year 2012, enacted in December 2011, was supported by a conference committee report that offered the following observation:

> The conferees recognize that because of the evolving nature of cyber warfare, there is a lack of historical precedent for what constitutes traditional military activities in relation to cyber operations and that it is necessary to affirm that such operations may be conducted pursuant to the same policy, principles, and legal regimes that pertain to kinetic capabilities. The conferees also recognize that in certain instances, the most effective way to deal with threats and protect U.S. and coalition forces is to undertake offensive military cyber activities, including where the role of the United States Government is not apparent or to be acknowledged.[27]

Those words seemed cryptic to those who were unaware of the ongoing disputes over the scope and relevance of the TMA exception. But understood in that context, the passage was reasonably clear: the conferees wanted to establish that the TMA exception does indeed apply to deniable military cyber operations. Unfortunately, the corresponding language in the statute itself fell short of the mark. Rather than state the TMA point with clarity, Section 954 of the NDAA fiscal year 2012 states that military "offensive operations in

cyberspace" are "subject to . . . the policy principles and *legal regimes* that the Department follows for kinetic capabilities, including the law of armed conflict."[28] Read in context with the legislative history, the reference to "legal regimes" could be understood as a veiled attempt to settle the TMA question in favor of its applicability. But without that context, this is anything but obvious. The issue accordingly persisted.

The language of Section 954 also gave rise to two other issues. First, even if Section 954 had been clear enough to settle the TMA issue related to military "offensive operations in cyberspace," a question of scope would nevertheless arise with respect to which cyber operations count as offensive. The current-day language associated with "defending forward" underscores the point: not all out-of-network activities are necessarily offensive in nature. Second, Section 954 had the potential to give rise to further uncertainty because it also contains language confirming the general authority of the Defense Department to conduct such operations "upon direction by the *President*." That formulation might have been read to require presidential authorization on an operation-by-operation basis, in which case Section 954 would have been somewhat akin to the covert-action process rules associated with presidential "findings" (but without the statutory requirement that the authorization be in writing and without the transparency-rule requirement of sharing the finding with Congress). The language was ambiguous on this point, however, and could just as well be read to mean that presidential authorization was required as a more general matter.

At any rate, Congress remained concerned about the TMA/covert-action issue, and in 2018 it returned to the subject with a far more specific and effective statutory intervention.

The conference report for the NDAA for fiscal year 2019 makes clear that Congress once again felt that TMA-scope issues were generating unjustified friction for military cyber operations. The conferees lamented that:

> The Department of Defense faces difficulties within the interagency in obtaining mission approval. One of the challenges routinely confronted by the Department is the perceived ambiguity as to whether clandestine military activities and operations, even those short of cyber attacks, qualify as traditional military activities as distinct from covert actions requiring a Presidential Finding. As a result, with respect to actions that produce effects on information systems outside of areas of active hostilities, the Department of Defense has been limited to proposing actions that could be conducted overtly on attributable infrastructure without deniability—an operational space that is far too narrow to defend national interests. The conferees see no logical, legal, or practical reason for allowing extensive clandestine traditional military activities in all other operational domains (air, sea, ground, and space) but not in cyberspace. It is unfortunate that the executive branch has squandered years in interagency deliberations that failed to recognize this basic fact and that this legislative action has proven necessary.[29]

Inspired by hope that the problem could be solved conclusively, Section 1632 of the NDAA for fiscal year 2019 first specifies that any activity constituting a "clandestine military activity or operation in cyberspace" necessarily qualifies as TMA.[30] This clarification alone was not enough to settle the question, however. Choosing to use the word *clandestine* as a way to describe the type of operations at issue added an unnecessary layer of difficulty. The word *clandestine*, after all, does not normally connote deniability, but simply secrecy. The two concepts are distinct. *Secrecy* means that an operation is meant to be undetected. *Deniability* implies that the US government's sponsoring role is not meant to be apparent or acknowledged. Without further clarification, therefore, the label "clandestine military activity" would not necessarily encompass the very set of actions (i.e., deniable cyber operations) that gave rise to the TMA/covert-action dispute in the first place.

Some further definitional language, accordingly, was needed in order for the "clandestine" test to have the intended effect despite the term's usual meaning. And Section 1632 duly provided it. The phrase "clandestine military activity or operation in cyberspace" was specially defined there as referring to military operations in cyberspace that not only are clandestine in the traditional sense—that is, intended to go undetected—but also in the distinct sense of deniability. More specifically, the statute provided that the phrase must be understood to cover activities "marked by, held in, or conducted with secrecy, where the intent is that the activity or operation will not be apparent *or acknowledged publicly*."[31]

Having thus swept all instances of deniable military cyber operations into the TMA exception (without respect to whether the operation would better be understood as offensive or defensive in nature), Congress might have stopped. But having just ensured that no presidential findings would be required (and, by extension, that no reporting to the Intelligence Committees would be necessary), Congress then imposed a substitute rule of process.

Specifically, the same section (1632) also imposed a requirement that *either* the president or the secretary of defense authorize the operation in question.[32] To be sure, this is not as demanding as a stipulation that the president alone make the necessary determination, nor does it require that the authorization be reduced to writing. And given that the authorization can be made at the secretary of defense level, it follows that this provision does not necessarily harness the self-interest of the White House in a way that might ineluctably lead to increased vetting, including voices from outside the military. Nonetheless, it is not meaningless to insist upon such high-level authorizations.

A final note: Section 1632 contains one final condition, and it is one that proves to be a bit of a mystery. In the relevant part, Section 1632 provides that the operation in question be carried out:

> (i) as part of a military operation plan approved by the President or the Secretary in anticipation of hostilities *or as directed by the President or the Secretary*;

> (ii) to deter, safeguard, or defend against attacks or malicious cyber activities against the United States or Department of Defense information, networks, systems, installations, facilities, or other assets; or
>
> (iii) in support of information related capabilities.[33]

At first blush, the existence of that final three-pronged condition—the trio of scenarios in which a secret and deniable military cyber operation might qualify for automatic inclusion in the TMA category—implied that the same old debate could continue to rage as to *other* scenarios. And perhaps the range of "other" scenarios might be broad. But on closer inspection, it seems quite the contrary. Focus on the first of the three eligible scenarios, with an emphasis on the language italicized above. The phrasing "or" sets it off from the first part of the sentence, making it an additional, fourth, eligible scenario. And it is a broad one indeed, covering any situation in which the president or secretary of defense has directed that an operation take place. Given that Section 1632 already requires the approval of either of those two individuals, it appears that this three- or four-pronged element might be doing no actual work.

Transparency Rules

This brings us to a topic already mentioned a few times above: transparency rules.

Transparency rules oblige executive branch actors to provide certain information to Congress (or to subparts of Congress), if not also to the public. In theory, they serve the important purpose of making it more reasonable for Congress to conduct oversight of secret, highly sensitive activities and thus to be in a reasonable position to legislate or take other actions as needed. They also have the salutary effect of ensuring that the executive branch actors understand that someone from outside their immediate sphere will to some extent be aware of what they do (thus incentivizing greater care). Indeed, in extreme cases, transparency rules might allow these actors to intervene and stop undesirable activity. And while it may be that transparency rules at times also constitute a vector through which others are able to stop truly desirable activities without good enough reasons, that trade-off provides an essential element of legitimacy in a situation in which we want to have both rule of law in a democratic society and also the secrecy needed for national-security activities to be carried out effectively.

As noted above, we long ago struck such a balance in regard to covert action. In particular, for decades we have required that presidential findings for covert action be shared with the Intelligence Committees and so too with important updates to existing findings. We have parallel transparency rules for important intelligence-collection activities, moreover, and in the course of actual practice a great deal more oversight takes place through interactions at the staff level.

With the TMA issue seemingly settled in favor of *not* treating military cyber operations as covert action, the covert-action and intelligence-collection transparency rules fall by the wayside. Congress has not left matters there, however. Instead, it has gradually constructed a series of alternative transparency rules, geared toward the military and running to the Senate and House Armed Services Committees.

As was the case with the TMA debate, attention to this issue originated not with cyber-domain activities but, rather, with special operations activities conducted in physical space. In particular, it originated with a desire to craft replacement transparency rules concerning the killing or capturing of individuals that might take place outside of certain recognized areas of hostilities. In a series of NDAA provisions enacted over a period of years, Congress designated such scenarios "sensitive military operations" and mandated periodic reporting about them to both Armed Services Committees.[34]

We now have something analogous for the cyber-domain activities described above in the preceding section. In 2017, Congress borrowed from the "sensitive military operation" transparency rule to create a nearly identical rule for "sensitive military *cyber* operations."[35] Specifically: the secretary of defense must submit a written notification to the Armed Services Committees within forty-eight hours of any military cyber operation intended to have effect in a foreign location other than ones in which US forces "are involved in hostilities."[36]

This requirement is the most tailored of the military cyber transparency rules, perhaps, but it is not the only one.

First, back in 2013, Congress instituted an obligation for the secretary of defense to provide "quarterly briefings on all offensive and significant military operations in cyberspace carried out by the Department of Defense during the immediately preceding quarter."[37] The briefings must be broken down with reference to each geographic and functional command's separate experience during the reporting period and must include an "overview of authorities and legal issues applicable to the operations, including any relevant legal limitations."[38] They also must address "any hostile cyber activity directed at the command"[39] in question and "any interagency activities and initiatives relating to" the command's cyber operations.[40]

Second, in 2017, Congress imposed a separate transparency rule requiring the secretary of defense to notify the Armed Services Committees on a quarterly basis regarding the application of the Pentagon's "weapons review" process to cyber capabilities—that is, the process of ex ante review of the legality of novel weapons as required by Department of Defense Directive 5000.01. Congress also required forty-eight hours' notification upon use of any capability that has been the subject of such review.[41]

Third, in late 2019 Congress enacted a different sort of transparency rule. As noted above, one of the most important authorization rules in that legal architecture is Section 1642 of the NDAA enacted in late 2018. The provision eliminates any doubt that USCYBERCOM can conduct out-of-network operations in response to systematic hostile cyber activity conducted by Russia, China, Iran, or North Korea. Critically, that provision contains an embedded process rule in that it expressly lodges the authority to act under that provision at the level of the National Command Authority. Then, in the NDAA for fiscal year 2020, Congress enacted a related transparency rule. Henceforth, the secretary of defense must give notice within fifteen days if the president delegates to the secretary any authority related to military operations in cyberspace that would otherwise be lodged at the National Command Authority level. That includes a description of the authority so delegated. Further, the same provision requires the secretary to notify the Armed Services Committees of any "concepts of operation" that the secretary may then approve under that delegated authority, again within fifteen days. Notably, this operational notification must include an array of particulars, including any actual activities that are conducted or planned to be conducted, the objectives to be achieved, the countries where the activities may occur, and details regarding any associated orders the secretary may have issued.[42]

Further research (in particular, extensive interviews with persons involved in operationalizing these transparency rules over time) is needed to assess how well the rules are functioning, both in absolute terms and in comparison to the analogous rules for oversight of covert action and collection. For now, it is enough to observe that Congress rapidly built a parallel transparency-rule architecture at much the same time it was endeavoring to shield military cyber operations from the covert action and intelligence legal frameworks, thus addressing in advance what otherwise might have been a significant objection to the latter project.

A final note regarding the WPR: In addition to the distribution-of-powers rules discussed above, the resolution is known for its transparency rules. Specifically, it requires consultation and notification to Congress regarding the introduction of US armed forces into hostilities or situations in which hostilities are imminent. And though some administrations have questioned the constitutionality of that statutory obligation, all have chosen to comply, or at least act "consistent with," that obligation. But much like the narrow reading of "hostilities" emphasized above, the use of cyber capabilities standing alone—especially without boots on the ground—would not trigger this obligation.

Substantive Rules

The legal frameworks that regulate national-security-related activities include not just rules of authorization, process, and transparency but also "substantive" rules, which simply prohibit certain actions or outcomes. Sometimes those rules are sourced in our domestic law, and sometimes they flow from international law. Sometimes it is both. With detainee

treatment, for example, there are important domestic-law substantive rules (such as the Torture Act and the War Crimes Act) and also important international-law rules (the Geneva Conventions, for example).

Critically, the United States simply has not adopted *cyber-specific* domestic laws of this kind. There is no statute or executive order, for example, that flat out forbids the implanting of malware in industrial control systems associated with the electrical grid in a foreign country. Nor have there been any significant proposals for statutes of that kind. Any applicable substantive rules, as a result, are those that apply more generally rather than being cyber specific. And there are no obvious examples of general domestic laws likely to significantly constrain USCYBERCOM operations of the sort described earlier, such as operations meant to disrupt Russian election interference or respond to Iranian military actions in and around the Persian Gulf.

What of international law as a source of substantive constraints? This is the topic that several others in this series will address. Here, I will simply observe that we do not as yet have any *cyber*-specific international laws constituting substantive constraints. There is, to be sure, much talk of cyber *norms*—that is, a hoped-for convergence of international opinion regarding the moral or policy propriety of this or that action. But that should not be confused with the formation of customary international law, let alone a treaty. What we *do* have, instead, are general-purpose international law concepts that can be applied to cyber-domain operations as much as any other.

Conclusion

The domestic legal framework for military cyber operations is surprisingly robust, considering its recent vintage. Far more quickly than it did for earlier institutional innovations such as the emergence of the CIA's covert action capability, Congress has responded to the maturation of USCYBERCOM by adopting relatively detailed rules of authorization, process, and transparency. The resulting framework has gone far toward eliminating otherwise-debilitating obstacles to the ability of USCYBERCOM to carry out its mission through out-of-network operations. At the same time, though, it imposes increasingly detailed oversight mechanisms that one hopes will induce desirable care and caution in making use of this greater freedom of action. Time will tell if the interaction of these rules results in a stable and effective equilibrium—perhaps sooner than we might wish, given the looming election, ongoing military tensions with Iran and North Korea, and pandemic-related espionage.

NOTES

1 Pub. L. No. 107-40, 115 Stat. 224 (2001); Pub. L. No. 107-243, 116 Stat. 1498 (2002).

2 Letter from Sen. Richard Blumenthal et al., to Christopher Krebs, Director, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, and Gen. Paul M. Nakasone, Commander, US Cyber

Command (April 20, 2020) (emphasis added), https://www.blumenthal.senate.gov/imo/media/doc/2020.04.20%20-%20CISA%20and%20CC%20-%20Coronavirus%20Cybersecurity%20-%20FINAL.pdf.

3 US Cyber Command, Achieve and Maintain Cyberspace Superiority 6 (2018).

4 US Dept. of Defense, Summary: Department of Defense Cyber Strategy 2018, at 7 (2018) (emphasis removed).

5 See, e.g., Monica Kaminska, Strauss Center, "Workshop Report: A Transatlantic Dialogue on Military Cyber Operations," August 13, 2019, https://strausscenter.org/wp-content/uploads/pdf/Amsterdam-Workshop-Report-Final-Oct-1.pdf (summarizing discussions from a two-day workshop in Amsterdam involving experts from military, civilian, and academic institutions from seven countries); Jacquelyn G. Schneider, "Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy," *Lawfare* (blog), May 10, 2019, https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy.

6 Lyu Jinghua, "A Chinese Perspective on the Pentagon's Cyber Strategy: From 'Active Cyber Defense' to 'Defending Forward,'" *Lawfare* (blog), October 19, 2018, https://www.lawfareblog.com/chinese-perspective-pentagons-cyber-strategy-active-cyber-defense-defending-forward. For my response to that scholar, see Robert M. Chesney, "An American Perspective on a Chinese Perspective on the Defense Department's Cyber Strategy and 'Defending Forward,'" *Lawfare* (blog), October 23, 2018, https://www.lawfareblog.com/american-perspective-chinese-perspective-defense-departments-cyber-strategy-and-defending-forward.

7 See H.R. Rep. 115-874, at 1049 (2018) (Conf. Rep.).

8 See, e.g., Mark Pomerleau, "Here's How Cyber Command Is Using 'Defend Forward,'" *Fifth Domain*, November 12, 2019, https://www.fifthdomain.com/smr/cybercon/2019/11/12/heres-how-cyber-command-is-using-defend-forward.

9 See Ellen Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms," *Washington Post*, February 26, 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; Julian E. Barnes, "U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections," *New York Times*, October 23, 2018, https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html.

10 This echoes the recent announcement that the Australian Signals Directorate (roughly equivalent to the American NSA) has been conducting disruption operations targeting criminal hacking crews that are exploiting the pandemic with ransomware attacks targeting Australians. See Senator the Hon. Linda Reynolds CSC, "On the Offensive Against COVID-19 Cyber Criminals," press release, April 7, 2020, https://www.minister.defence.gov.au/minister/lreynolds/media-releases/offensive-against-covid-19-cyber-criminals. Doing the same to state-sponsored attackers, of course, involves greater risks.

11 Robert M. Chesney, "The Legal Context for CYBERCOM's Reported Operations Against Iran," *Lawfare* (blog), June 24, 2019, https://www.lawfareblog.com/legal-context-cybercoms-reported-operations-against-iran.

12 Pub. L. No. 107-40, 115 Stat. 224 (2001).

13 Pub. L. No. 107-243, 116 Stat. 1498 (2002).

14 For a collection of declassified documents concerning JTF-Ares, see "Joint Task Force ARES and Operation GLOWING SYMPHONY: Cyber Command's Internet War Against ISIL," National Security Archive, August 13, 2018, https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-13/joint-task-force-ares-operation-glowing-symphony-cyber-commands-internet-war-against-isil.

15 Pub. L. No. 115-232, 132 Stat. 1636, 2132 (2018).

16 See, e.g., Memorandum Opinion from Caroline D. Krass, Principal Deputy Assistant Attorney General, Office of Legal Counsel, to the Attorney General, "Authority to Use Military Force in Libya," April 1, 2011; Memorandum

Opinion from Steven A. Engel, Office of Legal Counsel, to the Counsel to the President, "April 2018 Airstrikes Against Syrian Chemical-Weapons Facilities," May 31, 2018.

17 Engel, "April 2018 Airstrikes" (internal citations and quotation marks omitted).

18 50 U.S.C. §§ 1541–48 (2018).

19 50 U.S.C. §§ 1541(c).

20 For the full text of his statement, and the colloquy at the hearing, see Libya and War Powers: Hearing Before the S. Comm. on Foreign Relations, 112th Cong. 89 (2011) (statement of Harold Koh, Legal Adviser, US Department of State). For a summary of his testimony, see Robert M. Chesney, "An Overview of Harold Koh's Testimony on the WPR at Today's SFRC Hearing," *Lawfare* (blog), June 28, 2011, https://www.lawfareblog.com/overview-harold-kohs-testimony-wpr-todays-sfrc-hearing.

21 Section 32 of the Foreign Assistance Act of 1974, Pub. L. No. 93-559, 88 Stat. 1804, amended the Foreign Assistance Act of 1961, Pub. L. No. 87-195, 75 Stat. 424 (codified as amended in scattered sections of 22 U.S.C.), adding a new section 662 as described in the text above.

22 The provision is now found in 50 U.S.C. § 3093.

23 See, e.g., National Security Decision Directive 159, Covert Action Policy Approval and Coordination Procedures, January 18, 1985, https://www.cia.gov/library/readingroom/docs/CIA-RDP97M00248R000500190016-9.pdf.

24 50 U.S.C. § 3093(e)(1)–(2).

25 For an in-depth exploration of this debate and its practical relevance, see Robert M. Chesney, "Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate," *Journal of National Security Law and Policy* 5, no. 2 (January 24, 2012).

26 Executive Order No. 12,333, 46 Fed. Reg. 59,941, at § 1.7(a)(4) (Dec. 4, 1981) ("No agency except the Central Intelligence Agency [or the Armed Forces of the United States in time of war declared by the Congress or during any period covered by a report from the President to the Congress consistent with the War Powers Resolution, Public Law Number 93-148] may conduct any covert action activity unless the President determines that another agency is more likely to achieve a particular objective.").

27 H.R. Rep. 112-329, at 686 (2011) (Conf. Rep.) (commenting on Section 954).

28 National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, § 954(1), 125 Stat. 1298, 1551 (2011) (emphasis added).

29 H.R. Rep. 115-874, at 1049 (2018) (Conf. Rep.) (commenting on Section 1632).

30 10 U.S.C. § 394(c) (2018).

31 10 U.S.C. § 394(f)(1)(A) (emphasis added).

32 10 U.S.C. § 394(f)(1).

33 10 U.S.C. § 394(f)(1)(B) (emphasis added).

34 For an overview, see Robert M. Chesney, "Expanding Congressional Oversight of Kill/Capture Ops Conducted by the Military: Section 1036 of the NDAA," *Lawfare* (blog), December 8, 2016, https://www.lawfareblog.com/expanding-congressional-oversight-killcapture-ops-conducted-military-section-1036-ndaa.

35 10 U.S.C. § 395 (emphasis added).

36 10 U.S.C. § 395(c)(1)(C)(i). Originally, Congress specified that such operations only triggered reporting requirements if they constituted either "offensive" operations or else operations to respond to "ongoing or imminent" threats. In late 2019, Congress abandoned that effort, albeit in an awkward way. The statute now specifies that the operation in question must be either offensive or defensive in nature. That pairing covers the

waterfront, meaning that the language no longer is doing any work. See Pub. L. No. 116-92, § 1632, 133 Stat. 1198, 1746 (2019) (codified as amended in 10 U.S.C. § 395) (replacing the "ongoing or imminent" threat language).

37 10 U.S.C. § 484(a) (2018).

38 10 U.S.C. § 484(b)(2).

39 10 U.S.C. § 484(b)(1).

40 10 U.S.C. § 484(b)(3).

41 10 U.S.C. § 396 (2018).

42 Pub. L. No. 116-92, § 1642, 133 Stat. 1198, 1751–52 (2019) (This provision now appears in the notes accompanying 10 U.S.C. § 394).

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

The preferred citation for this publication is Robert Chesney, *The Domestic Legal Framework for US Military Cyber Operations*, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2003 (July 29, 2020), available at https://www.lawfareblog.com/domestic-legal-framework-us-military-cyber-operations.

About the Author

ROBERT CHESNEY

Professor Robert Chesney holds the James A. Baker III Chair in the Rule of Law and World Affairs at the University of Texas School of Law, where he also serves as the associate dean for academic affairs. Separately, he serves the broader university as director of the Robert Strauss Center for International Security and Law. He is a cofounder of *Lawfare*, the leading online source for national security law news and analysis, and also cohosts the popular weekly show the *National Security Law Podcast*.

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