Cyber Conflict and the War Powers Resolution
Congressional Oversight of Hostilities in the Fifth Domain

Jason Healey and A.J. Wilson

Since 1973, Congress has claimed the right to terminate military engagements under the War Powers Resolution (WPR). Beginning with Richard Nixon, whose veto had to be overturned to pass the WPR, presidents have typically regarded its provisions as unconstitutional limits on the authority of the Commander-in-Chief. The Obama administration has taken a slightly different tack, however, accepting “that Congress has powers to regulate and terminate uses of force, and that the [WPR] plays an important role in promoting interbranch dialogue and deliberation on these critical matters,” but seeking nonetheless to limit the application of the WPR to certain types of conflict.

In a recent report, the Pentagon has made clear its view that, on its own, a cyber conflict would not require congressional approval under the WPR. However, since future cyber conflicts could involve physical injury and death, this is neither the only possible view nor the most obvious one. The alternative position—that the waging of cyber war ought to receive as much legislative scrutiny as kinetic conflicts—depends in large part on the recognition that, since cyber is indeed the fifth domain of conflict, logical presence in cyberspace counts for as much as physical presence.

Jason Healey is the Director of the Cyber Statecraft Initiative of the Atlantic Council, focusing on international cooperation, competition and conflict in cyberspace. Since the 1990s, he worked on cyber issues as a policy director at the White House, vice president at Goldman Sachs and a U.S. Air Force intelligence officer.

A.J. Wilson is a Visiting Fellow with the Atlantic Council’s International Security program. He is a former Political Advisor in the British Parliament, and previously practiced law with the firm of Dorsey & Whitney LLP.
in the kinetic domains. This paper argues that the WPR does, in fact, apply to cyber operations, even on the basis of the Department of Defense’s own policy statements on the matter. And so, in our view, WPR should be adopted because the waging of significant cyber warfare should not be left to the Executive alone.

We will first analyze the critical provisions of the WPR and identify the key terms. We will then focus on the current administration’s view of the Resolution, as developed in the context of the Libyan conflict, and show that it is remarkably narrow in light of the WPR’s history and intent. Then we will examine how the Pentagon has applied a similar approach in the realm of cyber conflict, and contrast that approach with other recent policy statements from the Department of Defense. Finally, we will introduce the concept of ‘logical presence’ and argue on that basis that the WPR ought to apply to cyber conflicts in the same way that it applies to physical ones.

**The Waging of significant cyber warfare should not be left to the Executive alone.**

examine how the Pentagon has applied a similar approach in the realm of cyber conflict, and contrast that approach with other recent policy statements from the Department of Defense. Finally, we will introduce the concept of ‘logical presence’ and argue on that basis that the WPR ought to apply to cyber conflicts in the same way that it applies to physical ones.

**The War Powers Resolution.**

Under the WPR, the president is obliged to report to Congress within forty-eight hours of:

- Any case in which United States Armed Forces are introduced—(1) into hostilities or situations where imminent involvement in hostilities is clearly indicated by the circumstances; (2) into the territory, airspace or waters of a foreign nation...; or (3) in numbers which substantially enlarge United States Armed Forces equipped for combat already located in a foreign nation.5

Situations falling within items (2) or (3) only trigger the reporting requirement. However, in the circumstances contemplated by item (1), the president must, in addition to satisfying the reporting obligation (and absent congressional approval of his actions), terminate the use of U.S. armed forces within sixty days.6 A further thirty days are available if the president certifies that only with such an extension can the forces committed be safely withdrawn.7 In other words, the president, as Commander-in-Chief, may commit forces for a maximum of ninety-two days without the approval of Congress.

**Examination of the War Powers Resolution.** To analyze how the WPR may affect current or future cyber conflicts, it is first necessary to examine the law and how the present administration applies it. From Nixon to George W. Bush, presidents have regarded the WPR as an affront to their constitutional prerogatives. Yet all presidents since Nixon’s successor, Gerald Ford, have submitted reports in accordance with the resolution’s terms, although using varying thresholds.8

The text of the War Powers Resolution has four operative terms which are
critical to understanding the requirement set by Congress: "Armed Forces," "Hostilities," "Territory," and "Introduction." None of these are expressly defined. This is highly significant for present purposes: whether cyber conflict falls within the WPR depends largely on the width of the interpretations placed on these key terms. At a higher level of analysis, the narrower the interpretation of these terms, the more power to commit forces is left in the hands of the Executive alone, and the smaller the space for legislative oversight.

Analysis of the Term "Hostilities." The Obama administration, in justifying its expansive vision of Executive power, has generally sought to put forward what, in our view, are troublingly narrow definitions. With regard to U.S. operations over Libya, Obama administration officials have sought to limit the scope of the WPR by adopting a narrow approach to the definition of "hostilities." Initially, the president reported the Libyan engagement to Congress within the forty-eight hour window provided by the WPR, describing his report as "part of my efforts to keep the Congress fully informed, consistent with the War Powers Resolution.” As noted, sixty days after the submission of his initial report the president is required either to pull the forces out or to certify that a thirty-day extension is necessary in order to withdraw them safely. When that deadline arrived with respect to Libya, Obama did neither of these things. Instead, on 20 May 2011, the sixty-ninth day, he sent another letter soliciting congressional support for the deployment. This second letter did not mention the WPR.

Subsequently, a few days before the ninety-two day outer limit of the WPR, the president provided to Congress a "supplemental consolidated report... consistent with the War Powers Resolution," which reported on a number of ongoing deployments around the world, including the one in Libya. At the same time, the Pentagon and State Department sent congressional leaders a report with a legal analysis section justifying the non-application of the WPR, but also calling again for a congressional resolution supporting the war. Later, State Department legal adviser Harold Koh expanded upon this analysis in testimony before the Senate Foreign Relations Committee, arguing that operations in Libya should not be considered relevant "hostilities" for four reasons (our emphasis):

First, the mission is limited... U.S. forces are playing a constrained and supporting role in a NATO-led multinational civilian protection operation, which is implementing a UN Security Council resolution tailored to that limited purpose... Second, the exposure of our armed forces is limited... our operations have not involved U.S. casualties or a threat of significant U.S. casualties... active exchanges of fire [or] significant armed confrontations or sustained confrontations of any kind... Third, the risk of escalation is limited... [there is no] significant chance of escalation into a broader conflict characterized by a large U.S. ground presence, major casualties, sustained active combat, or expanding geographical scope...
Fourth and finally, the military means we are using are limited... The violence that U.S. armed forces have directly or indirectly inflicted or facilitated... has been modest in terms of its frequency, intensity, and severity.\textsuperscript{14}

It is apparent that in defining “hostilities” the administration’s focus is on kinetic operations passing a certain threshold of intensity: while there is no detailed indication in Koh’s testimony of what weight is to be accorded to each of these the factors he enumerates, the overriding emphasis is on physical risk to U.S. personnel. As Koh himself said, “we in no way advocate a legal theory that is indifferent to the loss of non-American lives. But... the provided there is no danger of U.S. casualties.

This is not a new view; indeed, Koh relied heavily on a memorandum from his predecessor in the Ford Administration, which defined "hostilities" as "a situation in which units of the U.S. armed forces are actively engaged in exchanges of fire with opposing units of hostile forces."\textsuperscript{17} This formulation would presumably exclude drone attacks, air strikes against primitively defended positions and, most importantly for present purposes, remote cyber operations.\textsuperscript{18}

Indeed, a large part of the administration’s case for the absence of "hostilities" in Libya, and therefore the non-application of the WPR, rested Congress that adopted the War Powers Resolution was principally concerned with the safety of U.S. forces.”\textsuperscript{15}

The consequences for opposing forces, and for the foreign relations of the United States, matter less, if not at all. Libyan units were decimated by NATO airstrikes; indeed, it was a U.S. strike that initially hit Muammar Gaddafi’s convoy in October 2011, leading directly to his capture and execution. Significantly, though, the strike came not from an F-16 but from a pilotless Predator drone flown from a base in Nevada.\textsuperscript{16} The apparent significance of this for present purposes is that even an operation targeting a foreign head of state does not count as "hostilities,” on its ability to keep pilots out of harm’s way by carrying out low-level, tactical strikes such as the raid on Gaddafi’s convoy using unmanned aerial vehicles instead of traditional manned aircraft.\textsuperscript{19} As remote war-fighting technology becomes ever more capable, reliable, and ubiquitous, the administration’s restrictive definition of “hostilities” could open up a huge area of untrammeled executive power.\textsuperscript{20} For example, neither the current administration nor its immediate predecessor has reported under the WPR any of the hundreds of remote drone strikes carried out in Pakistan, Yemen, or Somalia over the past decade. Speculation about their reasons for failing to do so
is beyond the scope of this paper. But the Pentagon has recently made clear its position that another form of remote warfare, cyber operations, are also not covered by the WPR.

**Analysis of the Term “Introduction.”** A recent Department of Defense pronouncement reveals how Obama’s minimalist approach to the WPR has been carried into the cyber realm. In a report submitted to Congress in November 2011, pursuant to a mandate in section 934 of the National Defense Authorization Act for fiscal year 2011, the Pentagon, quoting the WPR’s operative language, stated that:

> Cyber operations might not include the introduction of armed forces personnel into the area of hostilities. Cyber operations may, however, be a component of larger operations that could trigger notification and reporting in accordance with the War Powers Resolution. The Department will continue to assess each of its actions in cyberspace to determine when the requirements of the War Powers Resolution may apply to those actions.

This declaration receives no further explanation in the Section 934 report. But the general assumption is clear: the WPR will typically not apply to exclusively cyber conflicts, because the personnel carrying out such operations will usually work from centers inside the United States, such as the CYBERCOM facility at Fort Meade, Maryland, at a significant distance from the systems they are attacking and well out of harm’s way. Thus, the report argues, there is no relevant “introduction” of armed forces. Without such an “introduction,” even the reporting requirements are not triggered.

As we have seen, in addition to its “hostilities” provisions, which set the sixty-day clock running, the WPR also requires notification (though without starting the clock for withdrawal) when armed forces are “introduced” into foreign “territory, airspace, or waters” in circumstances short of hostilities. This provision is ignored in the Section 934 report. The Pentagon seems to have interpreted the congressional request to address “use of force in cyberspace” as mandating an exclusive focus on introduction into hostilities. But, as we argue below, the “introduction” provisions are as important as the “hostilities” provisions when it comes to understanding the WPR’s application in cyberspace.

**War Powers and Offensive Cyber Operations.**

*The Administration’s Argument.* One advantage (to the Pentagon) of the Section 934 report’s focus on “introduction” rather than “hostilities” is that it potentially creates a fallback argument for the DoD’s lawyers: even if there is “introduction” in a cyber operation—requiring a report to Congress—there may nevertheless be no “hostilities” to trigger the sixty-day pullout provision because, consistent with Koh’s Libya testimony, Americans are not put at risk. Such an argument would be a tough sell, however, given that the same report expressly refers to “hostile acts in cyberspace.” Indeed, as we shall see, current U.S. military doctrine appears to accept the notion that hostilities can and do take place in the cyber realm.
The view that there can be no introduction of forces into cyberspace follows naturally from the administration’s argument that the purpose of the WPR is simply to keep U.S. service personnel out of harm’s way unless Congress authorizes it. If unequal campaigns of manned airstrikes and devastating unmanned missions do not fall under the scope of the resolution, it is reasonable to argue that a conflict conducted in cyberspace does not either. Never mind that the cyber weapons an operator deploys might be causing physical destruction—even death—on the other side of the planet; according to the administration, the WPR focuses on the “introduction” of forces, not the consequences of such introduction for the adversaries of the United States or, who wield them. And that brings us back to our cyber-soldier who, without leaving leafy Maryland, can choreograph electrons in Chongqing. Finally, even if armed forces are being introduced, there are no relevant “hostilities” for the same reason: no boots on the ground, no active exchanges of fire, and no body bags.

The administration might further argue that the WPR was passed in the wake of an open-ended war in Vietnam whose principal tragedy was its mass, fruitless casualties. The intention, surely, was simply to protect future generations of American boys from this fate. If future operations do not put them in harm’s way in the first place, the WPR’s objective has already been achieved.

Rebutting the Administration’s argument. Yet, these explanations fall short. First, they are divorced from the history of the WPR. Previous administrations submitted WPR reports on remote strikes that did not put Americans in danger. Notably, Reagan reported the bombing of Tripoli in 1986, and Clinton reported his cruise missile attacks on Afghanistan and Sudan in response to the 1998 bombings of U.S. embassies in Africa as well as the high-level bombing of Yugoslavia during the Kosovo conflict in 1999. At least one contemporary scholar concluded that a major reason the WPR was able to...
pass in 1973—and not in 1970, 1971, or 1972, when Congress had debated similar drafts—was the widespread public revulsion towards the bombing of North Vietnam and Cambodia during late December 1972 and early 1973: remote, high-level operations which can scarcely be said to have put U.S. personnel at risk.28

Secondly, and more fundamentally, while preventing unnecessary American deaths is an essential part of the justification for having curbs on the Executive’s power to initiate hostilities, it is by no means the whole story. Military force is also the most drastic—not to mention the most costly—manifestation of national power on the international stage. It should not be used, and nor should its use be prolonged, recklessly. Recognizing this, the framers of the Constitution made the president Commander-in-Chief—but gave Congress the power to declare war.29

The WPR’s language is deliberately drafted broadly in order to give voice to this careful parceling of power in an age in which formal declarations of war are as out of fashion as the imperial-collared diplomats who once delivered them.

Moreover, nowhere other than in the single passage of the Section 934 report discussed above has the DoD asserted that forces cannot be introduced into hostilities in cyberspace. Other DoD writings clearly imply the opposite, and even the Section 934 report itself discusses “hostile acts in cyberspace.” What are “hostilities,” after all, if not a succession of hostile acts? Elsewhere, the DoD has made clear its intention to “treat cyberspace as an operational domain ... to ensure the ability to operate effectively in cyberspace,”30 while the U.S. Air Force’s mission is to “fly, fight, and win in air, space, and cyberspace.”31 It would make little sense to prepare to operate or fight, let alone win, in a domain into which one’s forces cannot be introduced for the purpose of engaging in “hostilities.” More pithily, we might simply say that the Pentagon’s cyber strategy refers to cyber operations both as “intrusions” and “breaches” for good reason.32

It is therefore appropriate to take a broader view of when it is that “United States armed forces” are “introduced into hostilities.” That view should pay attention to the consequences for U.S. foreign relations as well as the risks to American personnel. From this point of view, it would be surprising—to say the least—if a campaign designed, as cyber warfare can be, to degrade another sovereign nation’s economy or ability to defend itself required no congressional imprimatur. Why should such a campaign be treated differently simply because it is conducted not from the air, but from (or, for that matter, in or through) cyberspace?

Physical & Logical Presence.

What, then, might it mean for “armed forces” to be “introduced” into foreign “territory, airspace, or waters” in the cyber realm, or into “hostilities” taking place in cyberspace? In other words, what is the difference between physical and logical introduction? With a little thought, we can begin to sketch out an answer.

Presence in cyberspace—that is to say, logical or virtual presence—is not a monolithic concept; but this is also true in the physical space. As with the physical world, where a satellite taking images
Table 1: "Introduction" of Armed Forces in Cyber Conflict

<table>
<thead>
<tr>
<th>Type of logical presence</th>
<th>WPR status</th>
<th>Approximate physical world equivalent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connecting own system to the public Internet</td>
<td>None (passive presence)</td>
<td>Setting up sensors to detect and respond to incoming attack, e.g. a PATRIOT missile battery</td>
</tr>
<tr>
<td>Mapping or scanning foreign systems</td>
<td>None (transient presence)</td>
<td>Photographing hostile installations, e.g. from the ground or from a satellite</td>
</tr>
<tr>
<td>Intrusion into foreign systems and &quot;owning&quot; them</td>
<td>&quot;Introduced&quot; into &quot;terrority of a foreign nation&quot; but not &quot;into hostilities&quot; (active presence). Congress requires notification in 48 hours.</td>
<td>Limited covert operation short of attack on host country, e.g. Iranian hostage rescue attempt; raid on Bin Laden compound.</td>
</tr>
<tr>
<td>Maliciously manipulating (i.e. breaking) foreign systems</td>
<td>&quot;Introduced into hostilities&quot; (hostile presence). Unless Congress approves, forces must be withdrawn in 60/90 days.</td>
<td>Armed attack on host country, e.g. Operation Unified Protector.</td>
</tr>
<tr>
<td>Long-term campaign of such manipulation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

of a battlefield would be regarded very differently from a team of commandos rappelling into it, not all forms of cyber-presence would count as an "introduction," or as an introduction into "hostilities."

Table 1 shows a provisional typology of forms of logical presence that may be useful in determining when U.S. armed forces have been sufficiently "introduced into foreign territory [etc.]" or "into hostilities" to trigger the WPR’s reporting and/or withdrawal requirements.

Since the DoD has been clear that cyberspace is a domain like air, land, sea, and space, consistency requires application of the WPR whenever US armed forces are "introduced" into a foreign corner of cyberspace.33

Just as in the physical world, armed forces may have to be introduced into a potential cyber battlefield prior to the onset of hostilities, to scout or prepare the ground for the main assault. Such intrusions may constitute "introduc-
tions” sufficient to trigger congressional notification. Administrations may regard this as problematic because pre-hostilities preparation must be secret and notification is seen as inviting leaks. But separation of powers is an important precept, and the WPR achieves it in a subtly proportionate way for intrusions conducted under Title 10 military authority. In the planning phase, prior to any introduction of forces, the only requirement is “consultation” with Congress, and even then only when such consultation is possible in the circumstances. Once forces are introduced, but before they engage in hostilities—as in the scouting or preparation scenarios described above—Congress must be notified. But the sixty day window for withdrawal does not begin until the onset of actual or imminent hostilities. The involvement of Congress is thus phased in a manner appropriate to the magnitude of the operations concerned.

Intrusions under Title 50 intelligence authority, where secrecy is paramount, would receive congressional oversight through the appropriate intelligence committees and not through a WPR report. As a practical matter, the intrusions may be similar (and may even be conducted by the same units and personnel), but this distinction between war fighting and intelligence-gathering is an important one for U.S. foreign policy, and indeed for the balance between secrecy and oversight.

The gradation in the WPR, and the availability of two distinct authorities, thus provides a reasonable compromise between executive freedom of action and legislative oversight. Indeed, presidents may well prefer this to the alternative: namely, the prospect of Congress using its power of the purse to regulate military activity. This “nuclear option” of restraint via the federal budget is politically far easier to use in cyber conflicts: whereas few congressmen would approve of cutting funds to soldiers in harm’s way in foreign fields, they need have no such reservations in respect of malware in foreign hard drives.

Involving the legislative branch in executive decision-making in this graduated manner—which, as the table shows, is easily transposed to the logical realm—need be neither unreasonable nor disproportionate. On the contrary, it needs to occur to some extent. After all, openness is required of those who govern open societies. Especially in this information age, we as citizens are right to expect it.

**Conclusion.** The United States needs the capacity to carry out offensive operations in cyberspace, but the executive must accept that the same checks and balances that apply to physical hostilities apply also to cyber conflict. Future cyber attacks may have the ability to destroy or degrade an adversary’s critical infrastructure, cripple its economy, and seriously compromise its ability to defend itself. They may cause physical injury or even death. Their strategic consequences—not to mention their fiscal and economic costs—may be just as significant as a physical attack. This is, indeed, why the Pentagon has rightly decided to treat cyberspace as the fifth domain. But it must, by the same token, accept that logical forms of presence matter in cyberspace in the same way that physical forms matter in
the kinetic space, and therefore it must apply the WPR accordingly.

The Founding Fathers could not have imagined a world in which weapons made of information travel around the globe at the speed of light; but they did know how to distribute power to encourage restraint in its application. Even in cyberspace, there is a voice for both branches.

NOTES

2 United States Constitution, art. II, sec. 2.
5 War Powers Resolution, § 1543(a).
6 Ibid, § 1544(b).
7 Ibid.
9 The lack of definition in the statute is probably intentional (Koh, 4–5). “Armed forces” is defined in Title 10 of the US Code as comprising the Army, Navy, Air Force, and Marines, but that definition does not apply for Title 50 purposes, and in any event scarcely takes our understanding any further.
14 Koh, 7–10, supra note 3.
15 Ibid, 9.
17 Koh, 6, supra note 3.
18 Of course, political reality must be acknowledged. If the administration had been able to obtain congressional authorization, it surely would have welcomed it, and discarded its argument that such approval was unnecessary. A deeply divided and war-weary legislative branch made such decisive support unlikely, however. No doubt it was this political impasse more than anything else that drove the administration to field its restrictive interpretation of “hostilities.” Nevertheless, as Koh’s reference to a Ford-era opinion makes clear, presidential statements about WPR applicability set precedents.
21 One argument for failing to report the strikes—albeit, in our view, a deeply unattractive one—might be that drone strikes outside Afghanistan are carried out by the CIA, not the military, and therefore fall outside...
the scope of a resolution that deals with the deployment of "armed forces."

22 Singer
23 Cyberspace Policy Report
24 Ibid, 9.
25 This is probably the legal explanation for why the Administration felt obliged to report the Libyan operation to Congress, but denied that it required congressional approval to continue the conflict.
27 Grimmett War Powers Resolution: Presidential Compliance
29 United States Constitution. art. II, sec. 2; art. I, sec. 8.
32 Strategy for Operating in Cyberspace, 6.
33 Unless an administration chose to make the case that a cyber operation was not an intrusion but akin to flying a satellite in space over another nation, which doesn’t involve any intrusion. It would be odd indeed if the U.S. were to make this argument, given the characterization of cyber operations as "hostile acts" discussed above.
34 While the WPR is codified under Title 50 of the U.S. Code, here we are using 'Title 10' and 'Title 50' as shorthand for the president’s authority in federal law to, respectively, use military force and gather intelligence.
CALL FOR SPONSORS
CYBERDIALOGUE2013 MARCH 17-18, UNIVERSITY OF TORONTO

The Cyber Dialogue conference convenes an influential mix of global leaders from government, civil society, academia and private enterprise to participate in a series of facilitated conversations around cyberspace security and governance. An exciting program is currently being developed, featuring panel discussions and a number of social and networking events.

Sponsoring the Cyber Dialogue 2013 is an excellent way to reach a targeted audience and demonstrate your association with the best and brightest minds in the increasingly important discussion on Internet governance, security, and human rights issues. Past sponsors include Google, Microsoft, Internet Society and Afilias.

PRESENTED BY:

FOR MORE INFORMATION:
www.cyberdialogue.ca

Write for the
GJIA Blog!

The Georgetown Journal of International Affairs is seeking professors and experts in the study of international affairs to contribute regular columns or features online.

Contact gjia@georgetown.edu with your proposals. Visit http://journal.georgetown.edu for more details.