ATLANTIC COUNCIL
IDEAS. INFLUENCE. IMPACT.

ISSUEBRIEF

Jason Healey and A.J. Wilson

CYBER STATECRAFT INITIATIVE

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

Even as the Obama administration is pushing Congress to pass strong legislation to avert a "Cyber Pearl Harbor," it is insisting Congress should have little oversight in when the military engages in cyber conflicts. Cyber conflicts are too new and affect the American private sector too much to leave to the administration alone. Despite the administration's actions to the contrary, if the Department of Defense's own policies mean what they say, then Congress should have a voice in cyber operations.

The War Powers Resolution

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 overridden 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 [War Powers Resolution] plays an important role in promoting interbranch dialogue and deliberation on these critical matters," but is seeking nonetheless to limit its application to certain types of conflicts.[1]

All presidents since Nixon's successor, Gerald Ford, have submitted reports consistent with the resolution's terms, although using varying thresholds.[2]

About the Cyber Statecraft Initiative

The Atlantic Council's Cyber Statecraft Initiative focuses on the overlap of national security and cyber security to foster international cooperation and understanding of new forms of cooperation and conflict in cyberspace.

This is an edited version of a paper which first appeared a special edition of the *Georgetown Journal of International Affairs* in 2012.

This issue brief was made possible by generous support from The Morganti Group Inc.

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

> [A]ny 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.

Situations falling within items (2) or (3) trigger only this reporting requirement. However, in the circumstances contemplated by item (1), the president must, in addition to

1 Harold Hongju Koh, 'Testimony on Libya and War Powers Before the Senate Foreign Relations Committee,' June 28, 2011 ('Koh testimony'), p. 4. **http://www.foreign.senate.gov/imo/media/doc/Koh_Testimony.pdf**

2 Richard F. Grimmett, 'The War Powers Resolution: After Thirty-Six Years,' Congressional Research Service, April 22nd, 2010. **http://www.fas.org/sgp/crs/natsec/R41199.pdf**. Richard F. Grimmett, 'War Powers Resolution: Presidential Compliance,' Congressional Research Service, February 1st, 2012. **http://www.fas.org/sgp/crs/natsec/RL33532.pdf**.

Jason Healey is the director of the Cyber Statecraft Initiative at the Atlantic Council. **A.J. Wilson** is a visiting fellow at the Atlantic Council. Thanks to **Jason Thelen** of the Atlantic Council for his contributions.

satisfying the reporting obligation (and absent congressional approval of his actions), terminate the use of United States armed forces within sixty days. A further thirty days are available if the president certifies that only with such an extension can the forces committed be safely withdrawn. In other words, the president, as commander-in-chief, may commit forces for a maximum of ninety days after reporting without the approval of Congress.

The text of the War Powers Resolution has four operative terms—none of which is defined—each critical to understanding the requirement set by Congress: "Armed Forces," "Hostilities," "Territory," and "Introduction."

The text of the War Powers Resolution has four operative terms—none of which is defined—each critical to understanding the requirement set by Congress: "Armed Forces," "Hostilities," "Territory," and "Introduction."

With regard to US operations over Libya, Obama administration officials 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, describing his report as "part of my efforts to keep the Congress fully informed, consistent with the War Powers Resolution."[3] 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 May 20, 2011, the sixtieth day, he sent another letter soliciting congressional support for the deployment. This second letter did not mention the WPR. [4]

With regard to US operations over Libya, Obama administration officials sought to limit the scope of the WPR by adopting a narrow approach to the definition of "hostilities."

Subsequently, a few days before the ninety 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.[5] 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.[6] 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" because there was no chance of US casualties, limited risk of escalation, no "active exchanges of fire," and only "modest" levels of violence.

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 the factors he enumerates, the overriding emphasis is on physical risk to US 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 Congress that adopted the War Powers Resolution was principally concerned with the safety of US forces."

3 Letter from the President regarding the commencement of operations in Libya, March 21st, 2011. **http://www.whitehouse.gov/the-press-office/2011/03/21/letter-president-regarding-commencement-operations-libya**

4 'President Obama's Letter About Efforts in Libya,' reprinted in the New York Times, May 20th, 2011. **http://www.nytimes.com/2011/05/21/world/africa/21libya-text.html**

5 Letter from the President on the War Powers Resolution, June 15th, 2011. **http://www.whitehouse.gov/the-press-office/2011/06/15/letter-president-war-powers-resolution**. Note that the WPR requires six-monthly reports on ongoing deployments, whether or not involving hostilities: 50 USC ch. 33 sec. 1543.

6 'United States Activities in Libya,' June 15th, 2011. **http://www.foreignpolicy.com/files/fp_uploaded_documents/110615_United_States_Activities_in_Libya_--_6_15_11.pdf.**

The consequences for opposing forces, and for the foreign relations of the United States, matter less—or not at all. Libyan units were decimated by NATO airstrikes; indeed, it was a US strike that initially hit Muammar Gaddafi's convoy in October 2011, leading directly to his capture and extra-legal execution.

The consequences for opposing forces, and for the foreign relations of the United States, matter less—or not at all. Libyan units were decimated by NATO airstrikes; indeed, it was a US strike that initially hit Muammar Gaddafi's convoy in October 2011, leading directly to his capture and extra-legal execution. Significantly, though, the strike came not from an F-16 but from a pilotless Predator drone flown from a base in Nevada.[8] The significance of this for present purposes is that, apparently, even an operation targeting a foreign head of state does not count as "hostilities," provided there is no involvement of US troops.

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 US armed forces are actively engaged in exchanges of fire with opposing units of hostile forces." This formulation would presumably exclude drone attacks and, most importantly for present purposes, remote cyber operations.[7]

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 unchecked executive power. 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.

Likewise, the Pentagon has made clear its position that other forms of remote warfare, cyber operations, are also not covered by the WPR.

War Powers and Offensive Cyber Operations

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:[8]

> 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.

With the focus on "personnel," this passage makes clear that the WPR will typically not apply to exclusively cyber conflicts. With cyber warriors executing such operations 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, there is no relevant "introduction" of armed forces. Without such an "introduction," even the reporting requirements are not triggered.

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 US service personnel out of harm's way unless authorized by Congress. If 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.

Arguing the point, an administration lawyer might ask, rhetorically, what exactly do cyber operations "introduce"? On a literal, physical level, electrical currents are redirected; but nothing is physically added to—nor, for that matter, taken away from—the hostile system. To detect any "introduction"

7 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. Nevertheless, as Koh's reference to a Ford-era opinion makes clear, presidential statements about WPR applicability set precedents.

8 United States Department of Defense, 'Cyberspace Policy Report,' November 2011, p. 9. ('Sec. 934 report') **http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf**

at all, we must descend into metaphor; and even there, all that is really introduced is lines of code, packets of data: in other words, information. At most, this information constitutes the cyber equivalent of a weapon. "Armed forces," by contrast, consist traditionally of weapons plus the flesh and blood personnel 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.

Rebutting the Administration's Argument

Yet this narrow interpretation of "hostilities," that requires reporting only if action would put American troops at risk, falls short. While the explanation of every administration has been to submit WPR reports only for actions that put American lives in danger, this definition seems divorced from the text of the WPR that makes no mention of this requirement. 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. The WPR's text declares its purpose to "insure that the collective judgment of both the Congress and the President will apply" to the decision to introduce US armed forces.

Military force is the most drastic—not to mention the most costly—manifestation of national power on the international stage which must not be used recklessly or go un-checked by other branches of government. Recognizing this, the Framers of the Constitution made the president commander-in-chief—but gave Congress the power to declare war. In an age in which formal declarations of war are as out of fashion as the imperial-collared diplomats who once delivered them, the WPR's language is deliberately drafted broadly in order to give voice to this careful parceling of power instead of unilateral action. When evaluated in the context of the WPR's policy and purpose, it is accordingly appropriate to take a broader view of when "United States armed forces" are "introduced into hostilities." If there were such a re-look on this issue, hostilities in cyberspace should be treated no differently from the domains or air, land, or sea.

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 debilitate its military itself required no congressional imprimatur.

Yet this seems to be exactly the position of the DoD. In its Section 934 report to Congress (discussed above) the DoD seems to assert that since US personnel cannot be introduced into hostilities in cyberspace then a purely cyber campaign would never trigger the President's requirement under the WPR to report to Congress. No soldiers would be endangered, so it is purely an Executive matter.

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,"[9] while the US Air Force's mission is to "fly, fight, and win in air, space, and cyberspace." Of course armed forces are introduced into cyberspace – why else does the Pentagon's own cyber strategy refers to cyber operations as "intrusions" and "breaches"? 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." True, American soldiers, sailors, airmen and marines would be astoundingly unlikely to be harmed in these hostile cyber actions, but have no doubt, the DoD recognizes they would be engaged in hostile acts in cyberspace.

In addition, our experience in cyber conflicts is still new and they are likely to escalate in ways unanticipated to the DoD. When these conflicts do escalate, they are far more likely to blowback not against our military forces, but against the US private sector, which owns and operates so much of cyberspace. We may already be seeing just such blowback, as the US finance sector has been the subject of a large-scale and prolonged cyber campaign, widely held to be conducted by Iran. This counterattack is assumedly in response not just to financial sanctions but also the Stuxnet virus, launched by the US and Israel to disrupt the Iranian nuclear program. Given the dominant role of the private sector in cyberspace, and the vulnerability of the US private sector, cyber hostilities should arguably receive more scrutiny by both the political branches, not less.

9 United States Department of Defense, 'Strategy for Operating in Cyberspace,' July 2011, p. 5. **http://www.defense.gov/news/d20110714cyber.pdf**

Recommendations

The administration's interpretation of "hostilities" should go beyond the risk to American lives to have more logical consistency with cyberspace as a warfighting domain, like the land, sea, air, and space.

Table 1 shows a more consistent vision of "logical" presence that may be useful in determining when US armed forces have been sufficiently "introduced into foreign territory [etc.]" or "into hostilities" to trigger the WPR's reporting and/or withdrawal requirements.

Involving the legislative branch in cyber conflict decision-making in this gradated manner—which, as the table shows, is easily transposed to the physical realm—need be neither unreasonable nor disproportionate. After all, transparency is required of those who govern open societies. Especially in this information age, we as citizens are right to expect it.

The United States needs the capacity to carry out offensive operations in cyberspace, but the Executive branch 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 War Powers Resolution 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.

FEBRUARY 2013

Table 1: "Introduction" of Armed Forces in Cyber Conflict

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

Atlantic Council Board of Directors

CHAIRMAN
*Chuck Hagel

CHAIRMAN, INTERNATIONAL ADVISORY BOARD
Brent Scowcroft

PRESIDENT AND CEO
*Frederick Kempe

VICE CHAIRS
*Robert J. Abernethy
*Richard Edelman
*C. Boyden Gray
*Richard L. Lawson
*Virginia A. Mulberger
*W. DeVier Pierson

TREASURER
*Brian C. McK. Henderson

SECRETARY
*Walter B. Slocombe

DIRECTORS
Odeh Aburdene
Timothy D. Adams
*Michael Ansari
Richard L. Armitage
Adrienne Arsht
*David D. Aufhauser
*Ziad Baba
Elizabeth F. Bagley
Ralph Bahna
Sheila Bair
Lisa B. Barry
*Thomas L. Blair
Julia Chang Bloch
Francis Bouchard
R. Nicholas Burns
*Richard R. Burt
Michael Calvey
James E. Cartwright
Daniel W. Christman
Wesley K. Clark
John Craddock
David W. Craig
Tom Craren
*Ralph D. Crosby, Jr.
Thomas M. Culligan
Gregory R. Dahlberg
Brian D. Dailey
*Paula J. Dobriansky
Christopher J. Dodd
Markus Dohle
Lacey Neuhaus Dorn
Conrado Dornier
Patrick J. Durkin
Thomas J. Edelman
Thomas J. Egan, Jr.
Stuart E. Eizenstat
Dan-Åke Enstedt
Julie Finley
Lawrence P. Fisher, II
Alan H. Fleischmann
Michele Flournoy
*Ronald M. Freeman
*Robert S. Gelbard
Richard L. Gelfond
Edmund P. Giambastiani, Jr.
*Sherri W. Goodman
John A. Gordon
*Stephen J. Hadley
Mikael Hagström
Ian Hague
Frank Haun
Rita E. Hauser
Michael V. Hayden
Annette Heuser
Marten H.A. van Heuven
*Mary L. Howell
Robert E. Hunter
Robert L. Hutchings
Wolfgang Ischinger
Deborah James
Robert Jeffrey
*James L. Jones, Jr.
George A. Joulwan
Stephen R. Kappes
Francis J. Kelly, Jr.
Zalmay M. Khalilzad
Robert M. Kimmitt
Roger Kirk
Henry A. Kissinger
Franklin D. Kramer
Philip Lader
David Levy
Henrik Liljegren
*Jan M. Lodal
*George Lund
*John D. Macomber
Izzat Majeed
Wendy W. Makins
Mian Mansha
William E. Mayer
Eric D.K. Melby
Franklin C. Miller
*Judith A. Miller
*Alexander V. Mirtchev
Obie Moore
*George E. Moose
Georgette Mosbacher
Bruce Mosler
Hilda Ochoa-Brillembourg
Philip A. Odeen
Sean O'Keefe
Ahmet Oren
Ana Palacio
Torkel L. Patterson
*Thomas R. Pickering
*Andrew Prozes
Arnold L. Punaro
Kirk A. Radke
Joseph W. Ralston
Teresa M. Ressel
Jeffrey A. Rosen
Charles O. Rossotti
Stanley O. Roth
Michael L. Ryan
Harry Sachinis
William O. Schmieder
John P. Schmitz
Kiron K. Skinner
Anne-Marie Slaughter
Alan J. Spence
John M. Spratt, Jr.
Richard J.A. Steele
James B. Steinberg
Philip Stephenson
*Paula Stern
John Studzinski
William H. Taft, IV
John S. Tanner
Peter J. Tanous
*Ellen O. Tauscher
Clyde C. Tuggle
Paul Twomey
Henry G. Ulrich, III
Enzo Viscusi
Charles F. Wald
Jay Walker
Michael F. Walsh
Mark R. Warner
J. Robinson West
John C. Whitehead
David A. Wilson
Maciej Witucki
R. James Woolsey
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
David C. Acheson
Madeleine K. Albright
James A. Baker, III
Harold Brown
Frank C. Carlucci, III
Robert M. Gates
Michael G. Mullen
William J. Perry
Colin L. Powell
Condoleezza Rice
Edward L. Rowny
James R. Schlesinger
George P. Shultz
John W. Warner
William H. Webster

LIFETIME DIRECTORS
Carol C. Adelman
Lucy Wilson Benson
Daniel J. Callahan, III
Kenneth W. Dam
Stanley Ebner
Barbara Hackman Franklin
Chas W. Freeman
Carlton W. Fulford, Jr.
Geraldine S. Kunstadter
James P. McCarthy
Jack N. Merritt
Steven Muller
William Y. Smith
Marjorie Scardino
Helmut Sonnenfeldt
Ronald P. Verdicchio
Carl E. Vuono
Togo D. West, Jr.

**Executive Committee Members*
List as of September 17, 2012

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

1101 15th Street, NW, Washington, DC 20005 (202) 463-7226
www.acus.org