Congress's Role in Cyber Warfare

Stephen Dycus*

In his celebrated concurring opinion in *The Steel Seizure Case*,[1] Justice Jackson cautioned that "only Congress itself can prevent power from slipping through its fingers."[2] Jackson's warning seems especially pertinent today, as we prepare urgently for cyber warfare – facing potentially enormous threats from yet unknown enemies, and finding ourselves dependent on staggeringly complex, unproven technology.[3] The executive branch, which has special expertise and agility in national security matters generally, as well as substantial constitutional authority, has taken the initiative in these preparations.[4] Yet if Congress is to be faithful to the Framers' vision of its role in the nation's defense, it must tighten its grip and play a significant part in the development of policies for war on a digital battlefield.[5] It also must enact rules to help ensure that these policies are carried out.

Congress must work hand in hand with the Executive, however, to confront these evolving threats. The importance of collaborative planning can be seen in a recent exchange of correspondence in which leaders of the Senate Select Committee on Intelligence wrote to the Director of National Intelligence to ask about "the adequacy of the Director of National Intelligence and Intelligence Community authorities over cybersecurity."[6]

---

* Professor, Vermont Law School. The author is grateful to Kimberly Chehardy, Ellen Kreitmeier, Caitlin Morgenstern, and Lindsay Osborne, all Vermont Law School students, for their assistance with research, and to William C. Banks, M.E. "Spike" Bowman, Susan S. Gibson, Peter Raven-Hansen, Paul Rosenzweig, John Cary Sims, and Mark D. Young for helpful comments.

1. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952).

2. *Id.* at 654 (Jackson, J., concurring).

3. *See generally* NATIONAL RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2009); CENTER FOR STRATEGIC AND INT'L STUDIES, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY (2008), *available at* http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

4. In January 2008, for example, the Bush administration promulgated Homeland Security Presidential Directive 23 and National Security Presidential Directive 54, establishing the Comprehensive National Cybersecurity Initiative. However, few details are publicly known about the still-classified Initiative. *See* John Rollins & Anna C. Henning, *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations* (Cong. Res. Serv. R40427), Mar. 10, 2009, at 1-2, 5-7. A declassified summary was recently released by the White House. *See* Comprehensive National Cybersecurity Initiative (March 2010), *available at* http://www.whitehouse.gov/ cybersecurity/comprehensive-national-cybersecurity-initiative.

5. This article is concerned with conflicts fought entirely or mostly with electronic weapons, or in which such weapons have major impacts.

6. Letter from Dennis C. Blair, Director of National Intelligence, to Senators Feinstein and Bond, May 18, 2009, *available at* http://www.fas.org/irp/dni/blair-cyber.pdf. The term "cybersecurity" here almost certainly refers to both offensive and defensive uses of cyber weapons.

The Director answered:

> This is a very important issue . . . . A judgment regarding the adequacy of DNI authorities and any changes, additions, or clarifications will necessarily depend on the Administration's strategic plan on cyber, and where the center of gravity will be within the Executive branch. . . . We have more work to do in the Executive Branch before I can give you a good answer.[7]

The strategic, technological, and political problems described here present challenges of unprecedented complexity. The risks of error both in the formulation of a cyber warfare policy and in its execution are substantial. And despite the importance of developing a coherent, coordinated response to this threat, it seems unlikely that we will find a way to overcome entirely the endless turf battles among federal agencies and congressional committees.[8]

Still, the need is so pressing and the stakes are so high that we cannot afford not to try. The very future of the Republic may depend on our ability not only to protect ourselves from enemies armed with cyber weapons, but also to use such weapons wisely ourselves. This article examines some of the relevant legal issues and suggests some possible solutions.

I. CONGRESS'S ROLE IN DECIDING WHEN AND HOW TO GO TO WAR

There is broad agreement that congressional authorization is needed to start a war.[9] On the other hand, the President may act without Congress's approval to repel an attack on the United States.[10] Between these two extremes, the scope of the President's unilateral authority to use military

---

7. *Id.*

8. In the words of one recent study,

> the basic deficiency of the current national security system is that parochial departmental and agency interests, reinforced by Congress, paralyze interagency cooperation even as the variety, speed, and complexity of emerging security issues prevent the White House from effectively controlling the system.

PROJECT ON NATIONAL SECURITY REFORM, FORGING A NEW SHIELD (2008), at vi.

9. *See, e.g.*, LOUIS FISHER, PRESIDENTIAL WAR POWER 14 (2d ed. 2004) ("Scholars on the war power generally agree that the framers broke with available monarchical models and vested in Congress the exclusive power to initiate hostilities against foreign nations."); LOUIS HENKIN, FOREIGN AFFAIRS AND THE UNITED STATES CONSTITUTION 76 (2d ed. 1996) ("the constitutional power to decide whether to go to war lies with Congress").

10. In *The Prize Cases*, 67 U.S. (2 Black) 635, 668 (1863), the Supreme Court noted that "[i]f a war be made by invasion of a foreign nation, the President is not only authorized but bound to resist force by force." Absent such an invasion, however, the precise contours of the President's repel-attack power are not so clear. *See, e.g.*, HENKIN, *supra* note 9, at 48 n.40 ("It has been suggested that the President can go to war also in the case of an attack on an ally, but that would not appear to be within [the repel attack] exception to Congressional power as originally conceived.").

force is less well understood.[11] Once hostilities are under way, there is a consensus that the President has the tactical powers of a Commander in Chief, although it may not always be clear which of the President's actions are tactical and which are strategic.[12]

Before an attack can be launched, of course, Congress must have supplied the President with personnel and weapons.[13] Moreover, Congress may regulate the President's actions as Commander in Chief, except when the nation comes under sudden attack or the President exercises her tactical powers (and perhaps even then). In the Supreme Court's 1800 decision in *Bas v. Tingy*, Justice Paterson, one of the Framers, echoed the other Justices in declaring that "[a]s far as congress authorized and tolerated the war on our part, so far may we proceed in hostile operations."[14] Four years later, in *Little v. Barreme*, the Court reiterated that the President must not exceed limits set forth in Congress's authorization of hostilities.[15] Since then, no court has ruled otherwise.[16]

In the intervening two centuries, Congress has adopted a number of measures to control the initiation or conduct of warfare. At the end of the Vietnam War, for example, Congress passed the War Powers Resolution (WPR),[17] which requires the President to report to Congress within 48 hours

---

11. *See, e.g.*, HENKIN, *supra* note 9, at 48 ("Most controversial have been Presidential assertions of the right to use the armed forces for purposes short of war."). A small but vocal minority insist that the President's authority to initiate the use of force, large or small, is limited only by his discretion, as evidenced in part by numerous exercises of that discretion. *See, e.g.*, John C. Yoo, Deputy Assistant Attorney General, Office of Legal Counsel, *The President's Constitutional Authority To Conduct Military Operations Against Terrorists and Nations Supporting Them*, Sept. 25, 2001, *available at* http://www.usdoj.gov/olc/warpowers925.htm.

12. In 1850, the Supreme Court declared in a dictum that "the commander-in-chief . . . is authorized to direct the movements of the naval and military forces placed by law at his command, and to employ them in the manner he may deem most effectual to harass and conquer and subdue the enemy." Fleming v. Page, 50 U.S. (9 How.) 603, 615 (1850). But such apparently tactical actions may have strategic consequences. *See, e.g.*, William H. Rehnquist, *The Constitutional Issues – Administration Position*, 45 N.Y.U. L. REV. 628, 638-639 (1970) (defending President Nixon's controversial claim of tactical authority during the Vietnam War to invade Cambodia).

13. *See* Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 644 (1952) (Jackson, J., concurring) ("only Congress can provide [the President] with an army or navy to command").

14. 4 U.S. (4 Dall.) 37, 45 (1800) (Paterson, J., concurring).

15. 6 U.S. (2 Cranch) 170 (1804). *See also* Talbot v. Seeman, 5 U.S. (1 Cranch) 1 (1801).

16. Congress's power to regulate the Commander in Chief has often been disputed by the Executive, however. *See, e.g.*, Yoo, *supra* note 11 ("Neither [the War Powers Resolution nor the September 14, 2001 Authorization for Use of Military Force] can place any limits on the President's determinations as to any terrorist threat, the amount of military force to be used in response, or the method, timing, and nature of the response. These decisions, under our Constitution, are for the President alone to make.").

17. 50 U.S.C. §§1541-1548 (2006).

the introduction of U.S. armed forces into hostilities or imminent hostilities, and to withdraw those forces within 60 days if Congress does not expressly approve of their continued deployment.[18] Lambasted by some as an unconstitutional encroachment on presidential powers, the WPR has been followed (or at least lip service has been paid to it) by each President since the Nixon administration,[19] and Congress has repeatedly referred to the WPR approvingly in subsequent legislation.[20]

If Congress now fails to enact guidelines for cyber warfare, it might be perceived as inviting "measures on independent presidential responsibility."[21] Chief Justice Marshall suggested in *Little v. Barreme* that if Congress had remained silent, the President might have been free to conduct the Quasi-War with France as he saw fit.[22] But the national interest in electronic warfare, just as in that early maritime conflict, is so great that the planning and conduct of such a war should not be left entirely to the Executive. And because a cyber war might be fought under circumstances that make it impossible for Congress to play a meaningful contemporaneous role, Congress ought to get out in front of events now in order to be able to participate in the formulation of national policy.

II. CONGRESS'S ROLE IN INTELLIGENCE AND COVERT ACTIONS

The National Security Act of 1947[23] showed Congress's determination to exert some control over this nation's intelligence apparatus. That determination was strengthened after the disclosure of widespread intelligence abuses by the CIA and other agencies.[24]

In 1991, in response to the Iran-Contra Affair, Congress adopted a measure directing the President to keep the congressional intelligence committees "fully and currently informed of the intelligence activities of the United States, including any significant anticipated intelligence

18. *Id.* §§1543(a)(1), 1544(b).

19. *See generally* THE CONSTITUTION PROJECT, DECIDING TO USE FORCE ABROAD: WAR POWERS IN A SYSTEM OF CHECKS AND BALANCES (Peter Raven-Hansen rptr., 2005).

20. *See, e.g.*, Authorization for Use of Military Force Against Iraq Resolution, Pub. L. No. 107-243, §3(c), 116 Stat. 1498, 1501 (2002). This history refutes any argument that Congress has acquiesced in, or tacitly approved, the President's unlimited, unilateral uses of military force.

21. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 637 (1952) (Jackson, J., concurring).

22. 6 U.S. (2 Cranch) 170, 177 (1804).

23. Pub. L. No. 80-253, 61 Stat. 495 (codified as amended in scattered sections of 10 & 50 U.S.C.).

24. Those abuses are described vividly in the fourteen reports of the Church Committee, SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES (1975-1976), *available at* http://www.aarclibrary.org/publib/contents/church/contents_church_reports.htm. Congress responded by enacting the Foreign Intelligence Surveillance Act, 50 U.S.C. §§1801-1871 (2006), *as amended by* Pub. L. No. 110-261, 122 Stat. 2436 (2008), and other measures.

activity."[25] The term "intelligence activity" expressly includes "covert actions,"[26] which additionally require a written finding by the President that they are "necessary to support identifiable foreign policy objectives of the United States and [are] important to the national security of the United States."[27] Intelligence activities are also understood to include "all activities that elements of the Intelligence Community are authorized to conduct pursuant to [Executive Order No. 12,333]," the executive charter for such activities.[28] The "intelligence community" includes the Office of the Director of National Intelligence, CIA, NSA, other Defense Department intelligence components, and other federal intelligence elements,[29] which are authorized to engage in, *inter alia*, intelligence collection and analysis and "activities to protect against international terrorism . . . and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents."[30] This broad mandate certainly encompasses many U.S. efforts to defend against cyber attack and to employ cyber weapons offensively. By this definition, most preparations for and conduct of cyber warfare should be reported to the intelligence committees as "intelligence activities." It is significant that the reporting requirement in the 1991 law is not limited to agencies within the intelligence community.

Yet this legislation provides no guarantee that Congress will receive the information it needs to play a meaningful role in the development or execution of cyber warfare policy. It is not known, for example, precisely what it means for the intelligence committees to be "fully and currently" informed, what kinds of intelligence activities are regarded as "significant" enough to report, or who decides.[31] Other sections of the 1991 law call on

---

25. 50 U.S.C. §413(a)(1) (2006). This provision is part of a suite of reforms, Intelligence Authorization Act, Fiscal Year 1991, Pub. L. No. 102-88, §§602-603, 105 Stat. 429, 441-445 (1991) (codified as amended at 50 U.S.C. §§413-413b, 414 (2006)).

26. *Id.* §413(f). "Intelligence activities" are not further defined by statute.

27. *Id.* §413b(a). The history and practical application of the intelligence oversight laws are reviewed in A. John Radsan, *An Overt Turn on Covert Action*, 53 ST. LOUIS UNIV. L.J. 485 (2009).

28. Executive Order No. 12,333 (as amended), *United States Intelligence Activities*, §3.5(g), 73 Fed. Reg. 45,325 (July 30, 2008).

29. *Id.* §3.5(h).

30. *Id.* §1.4(b).

31. Senator Christopher Bond, Vice Chairman of the Senate Intelligence Committee, was quoted recently as saying, "The CIA doesn't have the time, we don't have the time, to be briefed on everything the agency's doing around the world. Every time they sneeze, we don't hear about it, unless it's a significant impact, or there's a major impact on our activity." Ronald Kessler, *Sen. Bond: Democrats Conducting "Jihad" To Protect Pelosi*, NEWSMAX.COM, July 13, 2009.

Section 321(d)(3)(C) of the pending Intelligence Authorization Act for Fiscal Year 2010, H.R. 2701, 111th Cong. (2009), would define "significant undertaking" in the context of covert actions as one that:

(A) involves the potential for loss of life;

all agencies involved in intelligence activities, not just the President, to keep the intelligence committees informed about those activities, but only "[t]o the extent consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters."[32] The "due regard for" language might be invoked to keep Congress in the dark.

Under the 1991 law, "covert actions," those with respect to which "it is intended that the role of the United States Government will not be apparent or acknowledged publicly,"[33] need only be reported to a small group of legislators known as the "Gang of Eight,"[34] and then only in a "timely fashion," a term not defined by statute.[35] Characterization of U.S. planning and execution of electronic warfare as "covert" could enable reporting to the smaller group, making it more difficult for Congress to play a significant role.[36] Moreover, any reporting might be delayed indefinitely.[37]

(B) requires an expansion of existing authorities, including authorities relating to research, development, or operations;

(C) results in the expenditure of significant funds or other resources;

(D) requires notification under [50 U.S.C. §414];

(E) gives rise to a significant risk of disclosing intelligence sources or methods; or

(F) could cause serious damage to the diplomatic relations of the United States if such activity were disclosed without authorization.

The same criteria might be adopted to describe cyber activities that would require consultation and reporting to Congress.

32. 50 U.S.C. §§413a(a), 413b(b)(1).

33. 50 U.S.C. §413b(e).

34. Reporting may be so restricted "[i]f the President determines that it is essential to limit access to the finding to meet extraordinary circumstances affecting vital interests of the United States." 50 U.S.C. §413b(c)(2). The "Gang of Eight" refers to leaders of the House and Senate and of their intelligence committees. *See generally* Alfred Cumming, *Sensitive Covert Action Notifications: Oversight Options for Congress* (Cong. Res. Serv. R40691), Jan. 29, 2010.

35. 50 U.S.C. §413b(c)(3).

36. Even if reports reveal activities that appear to be unwise, unauthorized, illegal, or perhaps extremely dangerous, legislators might feel constrained by Congress's own internal secrecy rules from sharing that information with congressional colleagues and formulating a response. *See* Frederick M. Kaiser, *Protection of Classified Information by Congress: Practices and Proposals* (Cong. Res. Serv. RS20748), Jan. 27, 2010. Or they might feel limited by conditions attached to their briefings. When members of the Bush administration told selected members of Congress about its abusive interrogation of terrorist suspects, for example, Senators and Representatives reportedly were forbidden to consult even with their staff members. Administration officials then argued, without even a hint of irony, that the legislators' subsequent silence was evidence of their tacit approval of those activities. *See* Paul Kane, *Accusations Flying in Interrogation Battle; Pelosi Says CIA Misled Congress on Methods*, WASH. POST, May 15, 2009, at A1.

37. President Reagan defended his failure to report on the secret sale of arms to Iran and transfer of the proceeds to the Nicaraguan Contra rebels by insisting that he could defer reporting "until such time as I believe it can safely be done with no risk to others." *See* Ruth Marcus, *Intelligence Law: What Notice Does It Require?*, WASH. POST, Dec. 21, 1986, at A21.

Another potential obstacle to congressional involvement is the reportedly common but statutorily unauthorized practice of informal reporting to an even smaller "Gang of Four" – the leaders of the intelligence committees – generally for sensitive non-covert intelligence activities.[38]

The Defense Department is heavily engaged in preparations for cyber warfare, having recently announced the establishment of a new U.S. Cyber Command.[39] But congressional oversight of the work of this command could be hampered by the military's reported practice of labeling its clandestine activities – those that are intended to be secret, but that can be publicly acknowledged if discovered or inadvertently revealed – as "operational preparation of the environment," rather than intelligence activities, even though they may pose the same diplomatic and national security risks.[40] As thus characterized, these activities might not be reported to the intelligence committees.[41] Any oversight that occurred would be conducted instead by the House and Senate Armed Services Committees.[42] Such a division of responsibilities might create dangerous confusion.

Congressional involvement also might be frustrated by the statutory exclusion of "traditional . . . military activities or routine support to such activities" from the definition of "covert action."[43] If secret military preparations for cyber war are regarded as "traditional military activities," under the rationale outlined above they might escape both the presidential

38. *See* Alfred Cumming, *"Gang of Four" Congressional Intelligence Notifications* (Cong. Res. Serv. R40698), Jan. 29, 2010. The pending FY 2010 Intelligence Authorization bill would require reporting of covert actions to the full intelligence committees unless the committees agreed otherwise. H.R. 2701, 111th Cong. §321(d)(2) (2009).

39. *See* Donna Miles, *Gates Establishes New Cyber Subcommand*, AM. FORCES PRESS SERV., June 24, 2009, *available at* http://www.defenselink.mil/news/newsarticle.aspx?id=54890. A significant military role in domestic aspects of cyber security might be viewed by some as posing an unacceptable threat to civil liberties. Defense officials have stressed, however, that the new command "would focus solely on military networks." Siobhan Gorman & Yochi Dreazen, *Military Command Is Created for Cyber Security*, WALL ST. J., June 24, 2009. *See generally* Stephen Dycus, *The Role of Military Intelligence in Homeland Security*, 64 LA. L. REV. 779 (2004).

40. *See* Alfred Cumming, *Covert Action: Legislative Background and Possible Policy Questions* (Cong. Res. Serv. RL33715), July 6, 2009, at 8.

41. According to one knowledgeable source, all such activities probably are reported as "intelligence activities" under §413, although the military regards these reports as voluntary.

42. In a report accompanying the FY 2010 Intelligence Authorization bill, the House Intelligence Committee complained that "[c]landestine military intelligence-gathering operations . . . often escape the scrutiny of the intelligence committees, and the congressional defense committees cannot be expected to exercise oversight outside of their jurisdiction." H.R. Rep. No. 111-186 (2009).

43. 50 U.S.C. §413b(e)(2).

findings requirement for covert actions and any reporting to the intelligence committees.[44]

III. A LEGISLATIVE HAND ON THE CYBER WAR MOUSE

Cyber warfare, as that term is used here, refers to conflicts that utilize cyber or electronic weapons either offensively or defensively, or both. Cyber weapons are currently employed offensively in kinetic warfare, for example, to suppress an enemy's air defenses or disrupt its communications, or defensively to track enemy troop movements. These weapons might also be used offensively to disable an enemy's cyber weaponry or defensively in response to an enemy attack, to prevent further aggression.

The term "cybersecurity" might be understood to refer to defense against cyber attacks. "Cyber attack" suggests offensive use, but the label is inexact and might be misleading. A preemptive strike to ward off an imminent enemy attack is considered defensive. Digital espionage might be part of the preparation for an attack, or it might be perceived that way by the target, which might then be provoked to defend itself by responding with a preemptive attack, either cyber or kinetic.

The important point here is that any use of cyber weapons, offensive or defensive, could have enormous consequences for the security and other interests of the United States. The effect of such use, actual or potential, matters more than the labels. And if the effect – on human life or property, for example, or diplomatic relations or compliance with the law of armed conflict – is substantial, Congress has a role to play in adopting policy for that use.

Congress has not thus far adopted measures suited to the regulation of cyber warfare. The War Powers Resolution, for example, is concerned with sending U.S. troops into harm's way, rather than with clicking a computer mouse to launch a cyber attack, although the strategic consequences might be similar. And the WPR's relatively relaxed timetable for executive notice and legislative response is unrealistic for war on a digital battlefield. Similarly, if cyber warfare is regarded as an intelligence activity, the intelligence oversight measures just described cannot, for reasons already indicated, ensure that Congress will be able to play a meaningful role. In the words of the National Research Council study cited above, "Today's policy and legal framework for guiding and regulating the use of cyberattack is ill-formed, undeveloped, and highly uncertain."[45]

Our experience with nuclear weapons may point to needed reforms. Since the beginning of the Cold War, the United States has had a fairly clear nuclear policy (albeit one that deliberately includes an element of

---

44. *See* Cumming, *supra* note 40.

45. NATIONAL RESEARCH COUNCIL, *supra* note 3, at 27. *See also* Letter from Dennis C. Blair, *supra* note 6.

ambiguity) – one known generally to Congress, the American public, and potential enemies.[46] Congress has approved or disapproved the purchase of the weapons and delivery systems. It has been briefed on the policy, and it has debated that policy vigorously.[47] While Congress has not articulated U.S. nuclear policy in any coherent form, it has collaborated closely with the executive branch in the development and execution of that policy.

Cyber weapons bear a striking resemblance to nuclear weapons in some important ways. An enemy's cyber attack would, like a nuclear strike, probably come without a clear warning. There are as yet no reliable defenses against either a cyber attack or a nuclear attack. Collateral damage from a nuclear attack would almost certainly be very extensive and would linger for an extended period.[48] The direct and indirect effects of a cyber attack, while different in kind and degree, still could be widespread and indiscriminate.[49]

In other ways, cyber weapons are critically different from their nuclear counterparts. For one thing, the time frame for response to a cyber attack might be much narrower. A nuclear weapon delivered by a land-based ICBM could take 30 minutes to reach its target. An electronic attack would arrive instantaneously, and leave no time to consult with or even inform anyone outside the executive branch before launching a counterstrike, if that were U.S. policy.

What most distinguishes digital warfare, however, is the potential difficulty in identifying the source of a cyber attack. It is always possible, of course, that an enemy might covertly deliver a nuclear device to the U.S. homeland in a shipping container or a Cessna. But the apparent ease with which a cyber attack may be carried out without attribution could make it impossible to fight back at all. If an attacker made it appear that the source was an innocent neutral state or perhaps another enemy of the attacker, a misdirected U.S. response might provoke a wider conflict. The potential

---

46. *See generally* David M. Kunsman & Douglas B. Lawson, *A Primer on U.S. Strategic Nuclear Policy* (Sandia Nat'l Laboratories), Jan. 2001, *available at* http://www.nti.org/e_research/official_docs/labs/prim_us_nuc_pol.pdf; *see also infra* note 70. That policy may be changing. *See* Christopher F. Chyba & J.D. Crouch, *Understanding the U.S. Nuclear Weapons Policy Debate*, WASH. Q., July 2009, at 21; COUNCIL ON FOREIGN REL., U.S. NUCLEAR WEAPONS POLICY (2009).

47. Many examples may be found in Kunsman & Lawson, *supra* note 46.

48. According to the International Court of Justice, the "destructive power of nuclear weapons cannot be contained in either space or time." Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 243 (July 8). The explosion of a nuclear weapon would release "not only immense quantities of heat and energy, but also powerful and prolonged radiation" that would "affect health, agriculture, natural resources and demography over a very wide area. Further, the use of nuclear weapons would be a serious danger to future generations. Ionizing radiation has the potential to damage the future environment, food and marine ecosystem[s], and to cause genetic defects and illness in future generations." *Id.*

49. *See* NATIONAL RESEARCH COUNCIL, *supra* note 3, at 121-124, 224-225.

difficulty in tracking the source also makes a policy of deterrence based on a threat of retaliation far less credible.

Given these characteristics of cyber warfare, and the continuing refinement of cyber weaponry, we approach a state of extreme strategic instability, with each nation on hair-trigger alert. The execution of an ill-conceived cyber war policy calling for a prompt response – or any response – to an attack or threatened attack could have disastrous, unanticipated consequences. It also might, depending on the circumstances, violate the law of armed conflict.

Congress accordingly needs to work closely with the executive branch in the development of a policy for this new kind of conflict. Such a policy ought to reflect the distinctive technology and strategy of digital warfare, and it should be reviewed constantly as the technology evolves. Like other regulations dealing with dynamic subjects, this policy should include general approaches that reflect this nation's broad strategic concerns and fundamental values. But the policy must also be crafted with enough flexibility to allow those charged with its execution to deal with future developments that cannot now be predicted. And it should set out a procedure for such adaptive use by identifying, for example, who must be consulted under what circumstances, and who will make the final critical decisions.

It is at least theoretically possible that Congress could play an active, real-time role in the implementation of whatever cyber warfare policy is adopted. The policy might, for example, like the War Powers Resolution, require consultation "in every possible circumstance."[50] But it seems more likely that a digital war would begin and end before any notice could ever reach Capitol Hill. Congress therefore needs to lay down clear guidelines, with as much flexibility as prudence requires, for executive branch officials to follow if consultation is not reasonably possible. And Congress should require a prompt and full account of every significant use of cyber weapons.

IV. OUTSOURCING CYBER WAR?

Private companies furnish most of the computer hardware and software employed by the defense and intelligence communities. Many of the specific, tailored applications of such technology for national security purposes have also been developed by private companies under contract. All this makes perfect sense, given the high level of expertise in cyber technology outside the government. It echoes the well-established practice of buying uniforms and weapons from private suppliers.

What may be surprising is that private companies have sometimes been employed to *operate* this technology – for example, in collecting and

50. 50 U.S.C. §1542.

analyzing intelligence.[51] These companies are guided by the terms of their contracts, including any provisions for ongoing government supervision, and by company policies. But contractor employees may feel divided loyalties because their first duty is to their employers' shareholders. And because the delegation of responsibilities adds at least one link to the chain of command, the process of monitoring and disciplining such employees is necessarily more difficult than controlling government personnel.[52] Not surprisingly, the terms of most of these contracts are classified, so public accountability is almost nonexistent.

Private contractors are already engaged in work related to cyber warfare.[53] It is not known publicly whether those contractors are making operational decisions or engaging directly in cyber warfare on behalf of the United States. But such actions would surely fall within the definition of "inherently governmental functions" – those that are "so intimately related to the public interest as to require performance by Federal Government employees," including activities that "require . . . the exercise of discretion in applying Federal Government authority."[54] A Department of Defense instruction elaborates on the meaning of the term "inherently governmental functions" in the context of war fighting:

> The U.S. government has exclusive responsibility for discretionary decisions concerning the appropriate, measured use of combat power. . . . Because combat operations authorized by the U.S. government entail the exercise of sovereign government authority, involve substantial discretion, and can significantly affect the life, liberty, or property of private persons or international relations,

---

51. *See generally* TIM SHORROCK, SPIES FOR HIRE: THE SECRET WORLD OF INTELLIGENCE OUTSOURCING (2008).

52. *See* Geoffrey S. Corn, *Unarmed but How Dangerous? Civilian Augmentees, the Law of Armed Conflict, and the Search for a More Effective Test for Permissible Civilian Battlefield Functions*, 2 J. NAT'L SECURITY L. & POL'Y 257, 260-261 (2008) (arguing that "only lawful combatants – individuals who genuinely qualify as 'members of the armed forces'" – should be allowed to perform functions that implicate law of armed conflict principles, because only such individuals can be expected to have the "level of training, discipline, selflessness, and responsibility associated with the performance of war fighting functions").

53. *See, e.g.*, Christopher Drew & John Markoff, *Contractors Vie for Plum Work, Hacking for U.S.*, N.Y. TIMES, May 31, 2009, at A1 (reporting that "[n]early all of the largest military companies . . . have major cyber contracts with the military and intelligence agencies").

54. The quoted language appears in §5(2) of the Federal Activities Inventory Reform (FAIR) Act of 1998. Pub. L. No. 105-270, 112 Stat. 2382, 2384-2385 (1998) (codified at 31 U.S.C. §501 note (2006)). A similar definition appears in OMB Circular A-76, which requires inherently governmental functions to be performed by government personnel. OMB Circular A-76 Revised, *Performance of Commercial Activities*, May 29, 2003, at Attachment A, ¶B.1.a., *available at* http://www.whitehouse.gov/omb/circulars/a076/a76_incl_tech_correction.html.

> they are IG [inherently governmental] . . . and cannot be legally contracted.[55]

Given the extraordinary risks associated with cyber weapons, Congress should not rely on executive agencies to decide which cyber warfare functions to outsource.[56] It should expressly bar delegation to private contractors of authority for operation of cyber weapons, either offensive or defensive, and it ought to expressly prohibit any expenditure of appropriated funds for that purpose.[57]

V. A FIRM CONGRESSIONAL HANDSHAKE WITH THE EXECUTIVE

Congress obviously cannot act alone to develop a cyber warfare policy for the United States. Its members and staff lack the technical expertise, agility, and organization to wield this new, evolving weaponry. On the other hand, Congress's job in our constitutional system is to set national policy for the executive branch to execute. Especially in the matter of cyber warfare, where the diplomatic and strategic stakes are potentially as high as they are in any kinetic conflict, Congress has a critical role to play. It has perspective gained from long experience in foreign affairs and a host of related issues, and it may be more responsive to the popular will. The solution to this apparent conundrum may be found in a close collaboration between the political branches in the planning and implementation of rules for cyber warfare.[58]

Congress needs to act now to create authority and set boundaries within which the President may develop more refined protocols. This legislative

---

55. Dep't of Defense Instr. (DODI) No. 1100.22, *Guidance for Determining Workforce Mix*, Encl. 2.1.3, Apr. 6, 2007, *available at* http://www.dtic.mil/whs/directives/corres/pdf/110022p.pdf.

Despite the apparent clarity of "inherently governmental functions," Congress has directed the Office of Management and Budget (OMB) to develop a "single consistent definition" of the term, in order to "ensure that [such functions] only be performed by officers or employees of the Federal Government or members of the Armed Forces," and to report its definition by October 14, 2009. Duncan Hunter National Defense Authorization Act for FY 2009, Pub. L. No. 110-417, §321, 122 Stat. 4356, 4411 (2008); *see* John R. Luckey, Valerie Bailey Grasso & Kate M. Manuel, *Inherently Governmental Functions and Department of Defense Operations: Background, Issues, and Options for Congress* (Cong. Res. Serv. R40641), Feb. 1, 2010.

56. *See* Luckey et al., *supra* note 55, at 26-32.

57. The FY 2009 Defense Authorization Act did not go nearly far enough. It merely provided, "It is the sense of Congress that . . . regulations issued by the Secretary of Defense . . . should ensure that private security contractors are not authorized to perform inherently governmental functions in an area of combat operations." Pub. L. No. 110-417, *supra* note 55, §832(4), 122 Stat. 4535.

58. A helpful description and comparison of current executive and legislative programs, as well as legislation pending in the 111th Congress, may be found in Catherine A. Theohary & John Rollins, *Cybersecurity: Current Legislation, Executive Branch Initiatives, and Options for Congress* (Cong. Res. Serv. R40836), Jan. 12, 2010.

development should be guided by advice from executive branch officials. The process must be cooperative rather than competitive. The resulting rules will necessarily be partly statutory, partly executive. The recent White House Cybersecurity Policy Review recommended that the "Administration should partner appropriately with Congress to ensure [that] adequate law, policies, and resources are available to support the U.S. cybersecurity-related missions."[59]

Set out below are some steps that Congress might take to create an appropriate partnership. Some of these steps involve changes in congressional committees and responsibilities. Others would require coordination of cybersecurity functions within the executive branch. Still others would direct the President to keep Congress fully informed about anticipated and actual uses of cyber weapons. Several would restrict potential executive branch actions that seem – as a matter of policy – particularly unwise.

1. Designate a single committee in each House with primary responsibility for cyber warfare in order to develop a coherent and consistent legislative approach.[60]

2. Charge the designated committees with the development of broad policy and oversight of its implementation for both offensive and defensive uses of cyber weapons, given the close, perhaps indistinguishable, connection between the two uses.

3. Make the designated committees responsible for oversight of the relevant activities of the White House and every government agency concerned with cyber warfare, including the Defense Department, and their contractors, whether overt, clandestine, or covert.

4. Designate a lead federal agency to coordinate ongoing planning among agencies.[61] The congressional committees would

---

59. CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE 10 (2009), *available at* http://www.whitehouse.gov/ assets/documents/Cyberspace_Policy_Review_final.pdf.

60. The designated committees might be new, or they might already exist. This first step may be the most challenging. As the 9/11 Commission observed, "Few things are more difficult to change in Washington than congressional committee jurisdiction and prerogatives." NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 419 (2004).

61. Implementation of the mostly secret Comprehensive National Cybersecurity Initiative, *see supra* note 4, is currently being coordinated by a task force operating under the Director of National Intelligence. CYBERSPACE POLICY REVIEW, *supra* note 59, at 9. The Obama administration's recent cybersecurity review recommended "appointing a cybersecurity policy official at the White House . . . to coordinate the Nation's cybersecurity-related policies and activities," but not to have authority either to make or to execute those policies. *Id.* at 7-8. In December 2009, President Obama appointed Howard Schmidt to serve as the White House Cybersecurity Coordinator.

then have a principal point of contact for the collaborative development of policy.

5. Designate a lead agency to execute the cybersecurity plan.[62]

6. Order the preparation of a National Cybersecurity Strategy at prescribed intervals.[63] This document should be declassified to the greatest extent possible, in order to inform every member of Congress and the public about the basic elements of U.S. cyber policy.

7. Require frequent, periodic briefings of the congressional committees, to enable serious consultation and advice in both directions as cyber policy evolves over time. These briefings should include information about rules of engagement, procedures for deciding to use cyber weapons, and any delegations of authority for such use.

8. Require consultation with the designated congressional committees in every possible instance before any significant use of cyber weapons.[64]

---

62. The recent White House review of cybersecurity policy included this observation:

> Responsibility for a federal cyber incident response is dispersed across many federal departments and agencies because of the existing legal, but artificial, distinctions between national security and other federal networks. Depending on the character of an incident – for example, a major vulnerability, a criminal attack, or a military incident – different departments or agencies may have or share the lead role for response, while others may never learn of the event. Moreover, the lead for the overall incident may not be clear. Although each player has defined areas of expertise and legal authorities, they are difficult to pull together into a single coordinated structure. Any consolidation of authorities in a unified structure may require legislation.

CYBERSPACE POLICY REVIEW, *supra* note 59, at 23.

Congressional designation of a lead agency could help eliminate turf battles that might otherwise prove dangerously distracting and wasteful. Reports persist, for example, of continuing uncertainty about whether the NSA or the Defense Department's new Cyber Command will be responsible for offensive cyber operations. *See, e.g.*, David E. Sanger & Thom Shanker, *Pentagon Plans New Arm To Wage Computer Wars*, N.Y. TIMES, May 29, 2009, at A1; James Risen & Eric Lichtblau, *Control of Cybersecurity Becomes Divisive Issue*, N.Y. TIMES,, Apr. 17, 2009, at A18. That uncertainty may be due in part to the appointment of the Director of NSA to head the Cyber Command, where, in Beltway-parlance, he apparently will be "dual hatted." *See* Siobhan Gorman, *Gates To Nominate NSA Chief To Head New Cyber Command*, WALL ST. J., Apr. 24, 2009.

63. This document should resemble and be consistent with the National Security Strategy. *See, e.g.*, The White House, NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA (2006), *available at* http://georgewbush-whitehouse.archives.gov/nsc/nss/ 2006/nss2006.pdf. Section 16 of the Cybersecurity Act of 2009, S. 773, 111th Cong. (2009), would require the preparation of a Quadrennial Cyber Review beginning in 2013.

64. A National Research Council study suggests possible advance congressional approval of some offensive uses of cyber weaponry based on, *inter alia*, the scale of a contemplated attack, the target, and other circumstances. NATIONAL RESEARCH COUNCIL, *supra* note 3, at 56. Because of the possible need for immediate action, advance approval is not recommended here. Possible criteria for determining when a contemplated use is

9. Require a written finding by the President, in advance of any significant use of cyber weapons whenever reasonably possible, or within a day or two afterward, that such use is or was necessary to the national security of the United States, that such use is or was as limited in scope as possible and consistent with the laws of armed conflict, and that Congress was consulted or could not be consulted because of the urgency of the threat.

10. Require immediate reports to the designated committees of any significant use of cyber weapons, either offensive or defensive.

11. Expressly forbid any withholding of information from the committees based on classification or for other reasons of secrecy.

12. Direct that all required reports be delivered to the designated committees as a whole, not merely to selected members.[65]

13. Expressly forbid automated *offensive* responses to actual or threatened cyber attacks on the United States under any circumstances. Given the potential for misperception or misinterpretation of an enemy attack, the difficulty of identifying the attacker and of assessing any resulting damage, and the risk of inadvertent escalation, any such response should be directed by a sentient human hand, informed by as much consultation with various government officials as the circumstances will permit.[66]

14. Create a government structure to coordinate assistance to private entities that come under cyber attack, so that such entities do not take matters into their own hands.[67]

"significant" for these purposes are suggested *supra* note 31.

65. *See supra* notes 34-38.

66. *See* NATIONAL RESEARCH COUNCIL, *supra* note 3, at 64, 230. I acknowledge the departure here from my own recommended use of terminology. But it would make no sense to forbid purely defensive responses, such as automatically plugging an opening in a computer firewall under attack or automatically overriding an enemy's cyber command to open the floodgates of Grand Coulee Dam. The challenge in defining what is offensive and therefore forbidden is obvious. My purpose here is simply to avoid inadvertent, highly undesirable results, such as provoking a wider conflict.

67. An offensive private response to an actual or perceived cyber threat or attack could have catastrophic consequences if, for example, that response were interpreted as an official act of the U.S. government and provoked a wider conflict. *See id.* at 36-37, 202-212. Private use of such "active threat neutralization" might violate the Computer Fraud and Abuse Act, 18 U.S.C. §1030 (2006), *as amended by* Pub. L. No. 110-326, §§203, 204(a), 205-208, 122 Stat. 3560, 3561-3563 (2008).

15. Review and appropriately amend existing legislation designed to protect privacy within the United States.[68] Needed amendments might require technical fixes, such as review of email traffic in anonymized form, or appointment of privacy officers in agencies responsible for implementation of cyber policy.[69]

16. Require the public disclosure of U.S. cyber warfare policy to the greatest extent possible, in order to inform those in government who are not directly involved in its development, to promote public debate, and to let potential enemies know that the United States has a viable policy in place.[70]

17. Prohibit the outsourcing of responsibility for operating cyber weapons systems either defensively or offensively. Because of the grave potential consequences and the attendant need for close control and accountability, such operations should be undertaken only by government officials.

---

68. Relevant existing legislation includes the Privacy Act, 5 U.S.C. §552a (2006); the Foreign Intelligence Surveillance Act, 50 U.S.C. §§1801-1871 (2006), *as amended by* Pub. L. No. 110-261, 122 Stat. 2436 (2008); and the Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986), as amended. President Obama has pledged that U.S. cyber security efforts "will not – I repeat, will not – include monitoring private sector networks or Internet traffic." The White House, *Remarks by the President on Securing Our Nation's Cyber Infrastructure*, May 29, 2009. But it is difficult to imagine a program to detect digital attacks on U.S. assets without some such monitoring. *See* Thom Shanker & David E. Sanger, *Privacy May Be Victim of Cyberdefense Plan*, N.Y. TIMES, June 13, 2009, at A1.

69. *See* CYBERSPACE POLICY REVIEW, *supra* note 59, recommending designation of a "privacy and civil liberties official to [a new National Security Council] cybersecurity directorate."

70. According to the National Research Council study cited above,

> Secrecy has impeded widespread understanding and debate about the nature and implications of U.S. cyberattack. . . . Secrecy about policy relevant to cyberattack inhibits public scrutiny and thus increases the likelihood that policy will be formulated with narrow parochial or short-term interests foremost in mind.

NATIONAL RESEARCH COUNCIL, *supra* note 3, at 28-29.

In a report on the FY 2009 National Defense Authorization Act, the Senate Armed Services Committee noted that

> [i]t is difficult to conceive how the United States could promulgate a meaningful deterrence doctrine if every aspect of our capabilities and operational concepts is classified. In the era of superpower nuclear competition, while neither side disclosed weapons designs, everyone understood the effects of nuclear weapons, how they would be delivered, and the circumstances under which they would be used. Indeed, deterrence was not possible without letting friends and adversaries alike know what capabilities we possessed and the price that adversaries would pay in a real conflict. Some analogous level of disclosure is necessary in the cyber domain.

S. Rep. No. 110-335, at 390 (2008).

These recommendations are, of course, riddled with terms that require careful definition. They also omit many critical details. Specific provisions relating to timing of notices and the requirement of consultation, for example, must be worked out between the political branches.

Congress's active role in the development and implementation of cyber warfare policy is no guarantee of national security. The policy might be flawed in various ways. There is also a risk that whatever policy is adopted will not be properly executed or that its execution will have unintended results. The policy might be misunderstood or might not provide clear or appropriate guidance in the urgent circumstances facing its interpreter. The person charged with implementing the policy might make a mistake – for example, by interpreting a potential enemy's electronic espionage as an attack. Available cyber weaponry might not work as planned. Or a purely defensive move by U.S. operators might be construed by another nation as offensive, and provoke an attack. Nor can the clearest policy, statutory or executive, guarantee compliance by an Executive determined to ignore it.[71] The rules might be construed by the President in a way that reduces the importance of Congress's role. Or they might be challenged in court.

Congress should not, however, hesitate to take the steps outlined here merely because they might produce unintended results or because they could be difficult to enforce. Exactly the same criticisms could be leveled at almost any reorganization or legislative initiative. The high stakes in this instance, and Congress's constitutional responsibility for formulation of national security policy, mean that Congress cannot sit this one out.

It might be suggested that these proposed measures would dangerously tie the President's hands, thereby limiting her freedom to respond to unpredictable future national security threats. The very point of the recommendations, however, is that Congress should place limits on the President's actions – to require her to share the responsibility for deciding to go to war. Even then, if the nation comes under sudden cyber or kinetic attack the President will remain free to respond as she sees fit.

The United States faces unprecedented challenges from enemies equipped with new weaponry possessing vast, evolving destructive potential. The two political branches must draw on their respective expertise and experiences to work together to meet these challenges, as the Framers intended.

---

71. Recently, for example, the CIA failed for seven years to inform Congress about its development of plans to dispatch paramilitary teams to kill al Qaeda leaders. *See* Mark Mazzetti & Scott Shane, *House Looks into Secrets Withheld from Congress*, N.Y. TIMES, July 18, 2009, at A10.