Information Warfare and War Powers: Keeping the Constitutional Balance

KENNETH B. MOSS

Imagine the following scenario. The United States learns that a particular foreign government has regularly allowed several terrorist groups that target U.S. citizens and interests to deposit money in banks within its borders. Furthermore, this government sometimes provides money to these accounts through third parties. After weighing the options, the President agrees to an attack using information technologies, such as launching a new virus, on the networks serving this country's financial institutions. A significant disruption of banking and other transactions occurs, and the country's government, convinced that the U.S. is behind this "cyber-attack," supports a terrorist attack on a U.S. installation a few weeks later. Through intelligence channels, the U.S. learns of this direct involvement and sends air strikes against select targets in the country. The White House informs the congressional leadership of the decision only a few hours before the planned air strikes.

The last part of this scenario, involving a Presidential order to use limited military force and an ensuing disagreement with Congress over prior consultation and authorization to use force, is fairly predictable. Congress has been trying to protect its war powers—the power of declaration of war or an authorization to use force—since the 1970s through the War Powers Resolution of 1973 and other measures. But the first half of the scenario, involving "information warfare," as it is now being called, places law and U.S. lawmakers on *terra incognita.* Perhaps consultation with Congress would occur with the senior Senate and

Kenneth B. Moss is Associate Dean for Academic Programs in the Industrial College of the Armed Forces, National Defense University, and a professor in its department of grand strategy. Previously, Professor Moss was a member of the staff of the House Subcommittee on Europe and the Middle East. The opinions within are his own and reflect no position of the National Defense University or the Department of Defense.

House leadership, the Senate Foreign Relations Committee or the International Relations Committee in the House, as well as the intelligence committees, but it is just as likely that no consultation would take place. The role of Congress in information warfare operations is unclear because the status of such operations remains undefined in national law, international law, or the laws of warfare. Yet, if Congress is to protect its constitutional powers in war-making and the use of military force, the time has come when it must study the subject of information warfare and amend or create legislation to address this issue.

As Congress does so, it will have to bear in mind that even the experts do not agree on a definition of information warfare. Consider as a start the definition offered by the Joint Chiefs of Staff. Information warfare is composed of "[i]nformation operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or conflict." A key term in that definition is "information operations," which are "[a]ctions taken to affect adversary information and information systems while defending one's own information and information systems."[1] On first reading, this definition seems fairly limited to measures that are taken via computers, other information technologies, and information systems and networks. This definition of information warfare could generate congressional concerns about the efficiency and protection of U.S. information networks and systems, but it would not seemingly provoke any efforts to protect congressional war powers.

If Congress is to protect its constitutional powers in the use of military force, the time has come where it must study the subject of information warfare.

However, another definition greatly expands the scope of information warfare and raises significant questions about the relationship among information warfare, the conduct of war, and the role of congressional war powers. In *What Is Information Warfare,* Martin Libicki defines it as "conflicts that involve the protection, manipulation, degradation, and denial of information."[2] Libicki then adds that it can occur in seven different forms: strikes at command and control capabilities, intelligence-based warfare related to acquiring or protecting information that can help one dominate a battlefield, electronic warfare, psychological warfare, "hacker" warfare, economic information warfare, and various scenarios in cyber warfare.[3] This definition presents an open-ended meaning that can embrace elements of traditional means of warfare as well as recent or future ones. The inclusions of such traditional measures, which are the foundations of Congress's understanding of war, make this definition something that Congress should study closely.

An opposite approach argues that war should be removed from the term

"information warfare." The focus of such operations should be on nonviolent means or stimuli. Taking the argument possibly to an extreme conclusion, advocates of this view argue that war will not occur if the *information* part is done correctly. In short, these are acts that will prevent or pre-empt the resort to violence. It is also a concept of information warfare that implies that a number of such measures can be performed by the civilian sector rather than the military, the traditional home of war-fighting capabilities.[4] Here, it would seem Congress has little reason or basis to be concerned about the use of information or information technology as an instrument of war, since the goal is to avoid a use of traditional military force.

Regardless of the difficulty in defining it, information warfare is increasingly being examined by policy-makers because it offers a number of advantages not provided by traditional warfare. Information operations are arguably lower risk because they may accomplish their objective without resort to armed force. Furthermore, they may cost less: consider the cost of an information operation versus the deployment of almost any military unit. Finally, in a climate where both the nation's political and military leadership wish to avoid casualties, the prospect of being able to act forcefully while avoiding any socially and politically unacceptable loss of life holds a powerful attraction. In Operation Allied Force in 1999, the use of information technologies in precision-guided munitions as well as in other combat and command-and-control systems contributed significantly to the lack of fatalities for the U.S. and its NATO allies. The low casualty rate in Afghanistan seems to reinforce the appeal of this capability. On the other hand, some information warfare operations are not linked at all with the use of weaponry, and, in fact, may be a desirable alternative to it. As information warfare capabilities improve, the nation's political and military leaders will want to rely more on a choice that may offer worthwhile results at lower budgetary and human costs.

As information warfare capabilities improve, the nation's political and military leaders will want to rely more on a choice that may offer worthwhile results at lower budgetary and human costs.

The technologies and means of information warfare offer the President major advantages in the conduct of war that come at the expense of Congress. There are a number of reasons for this. Because troops and weaponry may not be involved, it is unclear whether operations in information warfare would be regarded as a use of force or a hostile act. If not judged as a use of force, what would be the constitutional basis for congressional action? Historically, Congress has been reluctant to assert its war powers against the actions of a President, even when traditional military means are used. Will the use of information technologies in weaponry and

the accompanying promise (and hope) of fewer casualties invite Congress to give the President more leeway over the authorization of military force? Taking this idea one step further, could the use of information technology rather than traditional weaponry and troops be regarded as an acceptable course that requires no congressional oversight and action? A decision to use military force and to risk lives is a difficult one—a choice leaders rightly prefer not to make not to make if they can avoid it. Legislators do not want to stare into the abyss of military action where outcomes and political consequences can be uncertain. If a new type of warfare at a lower threshold is available to the President and Congress, the need for congressional review and action may not seem as compelling. Yet, if that is the conclusion that emerges, any imbalance that already favors the President in using military force will become greater.

NEW FORMS OF LIMITED FORCE AND THE CONSTITUTION

To define its responsibilities in an information warfare environment, Congress must wrestle with a number of questions. Foremost is the question of whether information warfare and cyber attacks fall within the definition of military force used by Congress. Consider the foundation of congressional powers in this area: the power to declare war. Aside from the fact that a declaration of war is a rare event in U.S. history, another fundamental question is the definition of war itself. Throughout history there has been a common understanding that war involves the use of armed force.

Thus, one can see why a debate continues among specialists in law and information warfare over the question of whether or not such operations are an act of war. Sensing the confusion within the U.S. defense community, the Office of General Counsel in the Department of Defense presented an analysis of this question in June 1999.[5] The counsel argues that an act of war is a concept rarely heard in modern diplomatic discourse. It goes on to state:

> "An act of war is a violation of another nation's rights under international law that is so egregious that the victim would be justified in declaring war. Declarations of war have fallen into disuse, and the act of war concept plays no role in the modern international legal system."[6]

There are those who would strongly disagree with this position, but the argument reflects the calculated efforts of the U.S. for over half a century to avoid a declaration of war.[7]

Much of the current discussion about what constitutes war rests on the UN Charter and other UN declarations. For example, in 1974 the UN General Assembly passed the Definition of Aggression Resolution, which, although not regarded by the U.S. as the absolute and final word, posited that the resolution

provided "useful guidance." The important thread throughout the definition was the use of actual, or "kinetic," force, as one group of writers described it.[8] Thus, the emphasis in the resolution falls on land, air, or sea actions, such as invasions, forceful annexation, bombardment, the use of weapons by one state against another, blockade, or sending armed bands, mercenaries, irregulars or other groups against another state. There is little here to suggest that information warfare could ever fall under the definition of war as understood by the writers of the Constitution or by subsequent generations of U.S. presidents and legislators.

To cloud the issue further, an ongoing debate continues over whether or not the technologies used in information warfare, such as computers, are really weapons. An Air Force instruction document in 1994 suggested that "computer systems would probably not be considered weapons." "Weapons are devices designed to kill, injure, or disable people, or to damage or destroy property. Weapons do not include...electronic warfare devices." This definition places full emphasis on the consequences. A weapon has to destroy something; if it does not, it is not a weapon.

If a new type of warfare at a lower threshold is available to the President and Congress, an imbalance that already favors the President in using military force may become greater.

A different approach to defining a weapon places emphasis on its intended use. This definition suggests that the computer relaying the information to the actual destructive device could be regarded as a weapon on its own. This very question is one of the major disagreements about the Outer Space Treaty. Some argue satellites are not weapons, since they merely relay information. Obviously, a personal computer on its own is hardly a traditional or kinetic weapon (unless perhaps heaved by a frustrated employee at a supervisor), but when linked to an actual weapon on the ground, sea, or in the air is it not essentially the same?[9] It does provide the information, such as guidance, that enables the device to destroy the target.

The above question pertains to information technology linked through a system or network to a real weapon. A harder question to answer is posed, however, when a computer, not linked to any weapon, is used to provide commands or to install a virus that causes disorder or even destruction elsewhere. Stand-alone computers would have played an important part in the introductory scenario—the attacks on the foreign country's banking network. It may seem a stretch of the imagination to equate a collection of digital signals to bombs and bullets, but cyber-attacks can produce very destructive consequences such as downed power grids that shut off power in hospitals or the disruption of flood control systems at dams. Such impacts are not significantly different from the results of a bomb dropped on a power station or on a dam. Consequently, as the Department of Defense's own legal

counsel points out, one may have to answer the question about a computer as weaponry not in terms of the technology but in terms of the consequences. If the results are comparable to what might be produced by traditional weapons in an act of aggression, a government may well be justified in responding not with another cyber operation but with direct military force.[10]

In such circumstances, Congress is poorly equipped to act and to review, much less challenge, the actions of a President who has ordered an information operation against another state. Current laws simply provide no effective means for doing so.

Consider the War Powers Resolution of 1973, in which Congress tried to strengthen its powers to control Presidential actions in instances where military force was being used without a declaration of war. The key words are at the beginning of Section 4(a): "In the absence of a declaration of war, in any case in which United States Armed Forces are introduced..." and with the pivotal words being "United States Armed Forces." Section 4(a) (1) concerns introducing forces "into hostilities or into situations where imminent involvement in hostilities is clearly indicated by the circumstances."[11] This is the most vague of the three provisions in the law requiring a presidential report to Congress. One may argue that the use of U.S. military resources (such as employing troops at computers) to commence an information warfare operation against a foreign actor might be a form of introducing armed forces into hostilities or situations where they are imminent. However, that is a very sweeping interpretation that seemingly exceeds the intent of the law. The provision clearly implies movement of personnel.

If Congress was preparing to use the War Powers Resolution in this context, it should revisit the entire statute and determine after close scrutiny what types of information operations may amount to measures that could bring the United States into hostilities. Presidents have consistently challenged the constitutionality of the War Powers Resolution, and it is certain any President would do so if Congress tried to expand its definition to information warfare scenarios. A President would likely argue that these are pre-hostile measures and that Congress's authority in war powers does not commence until the decision to move U.S. forces occurs. However, it is the prospect of consequences comparable to an actual use of force offered by some information warfare scenarios that justifies congressional study of this question.

The President cannot be given an instrument of warfare over which Congress has no power.

It is also possible that some information operations could fall under the jurisdiction of the intelligence committees. The Intelligence Oversight Act of 1991 requires the President to keep the two committees "fully and currently informed of the intelligence activities of the United States, including any significant anticipated

intelligence activity [covert action] as required by this title." This act defines covert action as "an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly." Certainly, the need to conceal the origins of the action requires any information warfare measures to be covert. However, the provision specifically excludes from the definition "traditional diplomatic or military activities or routine support to such activities."[12] Information warfare activities are not traditional, but they are becoming another option in the military's arsenal alongside the personnel and weapons that a President can use. To the extent that the intelligence committees can provide oversight of information warfare, they are not in the best position to protect Congress's role in war powers. That falls primarily in the jurisdiction of the Senate Foreign Relations Committee, the House International Relations Committee, and the two armed services committees.

A CHALLENGE FOR CONGRESS

It is unfair to suggest that Congress has ignored information warfare or cyber warfare. Like the executive branch, it has paid much attention to measures to protect the United States against such attacks. However, the prospect of an attack on America using information technologies invites another prospect—that of retaliation by the United States.[13] This question, and the question of whether the measures selected amount to or are equivalent to a use of force by the United States, should also concern Congress. Four years ago, Congress received just such a warning from the President's Commission on Critical Infrastructure Protection, when it urged Congress to examine this very issue in light of the War Powers Resolution.[14] Nothing has happened, however. Meanwhile, U.S. strategic thinking is evolving in a way that increasingly foresees information operations as a dimension of war fighting.

As with any major policy development, Congress needs first to educate itself about information operations and cyber warfare before it considers any legislation. Doing so through hearings and study will provide a major service not only to itself, but also to the nation at large. One of the most difficult aspects of information warfare is clearly defining it. Hearings will help the strategic community clarify its own thinking as it tries to explain concepts and applications to Congress. Information warfare is a subject discussed mainly in a small, specialized community. In spite of some coverage in the press, it still carries too many science fiction connotations to be quickly understood and comfortably discussed in the larger policy community.

More importantly, as in any debate and vote on the use of traditional military force, Congress's placement of information warfare within the context of the

Constitution guarantees that the President's policy towards it will have a stronger legal foundation and public support. This is critical not only for sustained acceptance of the policy at home but also for international recognition of the justification of the President's decisions abroad. Ultimately, information warfare, cyber-attacks, or cyber warfare must come under the same requirements for accountability in the Constitution as traditional military force. The President cannot be given an instrument of warfare over which Congress has no power. ■

NOTES

1 Following the definition further upstream, information is defined as "1) Facts, data, or instructions in any medium or form. 2) The meaning that a human assigns to data by means of the known conventions used in their representation." See *Department of Defense Dictionary of Military and Associated Terms,* Joint Publication 1-02, April 12, 2001 (Washington, D.C.: Department of Defense, 2001), 202-203.

2 Martin C. Libicki, *What Is Information Warfare?* (Washington, D.C.: National Defense University Press, August 1995).

3 See the explanation of different concepts of information warfare made by Lieutenant Colonel Charles Ayala, U.S. Air Force, in Thomas E. Copeland, ed., *The Information Revolution and National Security* (Carlisle, Pennsylvania: U.S. Army War College, Strategic Studies Institute, August 2000), 136-137.

4 Office of General Counsel, Department of Defense, "An Assessment of International Legal Issues in Information Operations," <http://www.infowar.com/info_ops_061599a_j.shtml> (June 15, 1999).

5 Ibid., 12.

6 See, for example, Brien Hallett, *The Lost Art of Declaring War* (Urbana: University of Illinois Press, 1998).

7 Office of General Counsel, Department of Defense, "An Assessment of International Legal Issues," 13-14. Also see the discussion by Lawrence T. Greenberg, Seymour E. Goodman, and Kevin J. Soo Hoo, in *Information Warfare and International Law,* especially Chapter 2, "The Conduct of Information Warfare and International Law," (Washington, D.C.: Department of Defense Command and Control Research Program, National Defense University Press, 1998), 17-55.

8 This paragraph draws on DiCenso, "Cyberlaw," 4, 9-10.

9 Office of General Counsel, Department of Defense, "An Assessment of International Legal Issues." 18-19.

10 The text is provided in Louis Fisher, *Presidential War Powers* (Lawrence: University Press of Kansas, 1995), 214-218.

11 The text of the Intelligence Oversight Act is also found in Fisher, *Presidential War Power,* 219-223.

12 A good summary of Congress's actions can be found in Stephen A. Hildreth, *Cyberwarfare,* CRS Report for Congress, Congressional Research Service, The Library of Congress, November 15, 2000.

13 See *Major Federal Legislation: A "Legal Foundations" Study,* Report to the President's Commission on Critical Infrastructure Protection, <http://www.info-sec.com/pccip/web/> (December 21, 2001).