Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of CYBERATTACK CAPABILITIES

William A. Owens, Kenneth W. Dam, and Herbert S. Lin, *Editors*

Committee on Offensive Information Warfare

Computer Science and Telecommunications Board

Division on Engineering and Physical Sciences

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

THE NATIONAL ACADEMIES PRESS
Washington, D.C.
www.nap.edu

civilians in a nation of choice, might also be compromised in order to support a cyberattack. These computers can be configured as "weapons for cyberattack" at will by the real attacker at essentially zero cost, even though they increase his attack capabilities by orders of magnitude, and because such scenarios were never envisioned by the traditional acquisition process, it is only a matter of policy that might inhibit the United States from doing so.

Acquisition policy should also address the issue of the proper balance of resource allocation. The absolute budget sums involved in acquiring cyberattack capabilities are relatively small, as noted in Chapter 2. But serious defensive efforts are very expensive, not least for reasons of scale—the sheer volume of computer systems and networks that must be protected. Thus, acquisition policy necessarily affects the balance between conventional military assets and cyber military assets and procedures on the defensive side. Given the dependence of today's military forces on information technologies, some analysts have argued that present-day acquisition policies do not pay sufficient attention to cybersecurity and defensive operations.

The above discussion of acquisition policy relates primarily to the defense community. But the intelligence community must also acquire various capabilities to support its intelligence collection and covert action missions. Of particular significance for acquisition policy is that a tool to collect intelligence information from an adversary computer system or network can—at little additional cost—be modified to include certain attack capabilities, as described in Section 2.6. Indeed, the cost of doing so is likely to be so low that in the most usual cases, acquisition managers would probably equip a collection tool with such capabilities (or provide it with the ability to be modified on-the-fly in actual use to have such capabilities) as a matter of routine practice.

6.1.3 Employment Policy

Employment policy specifies how weapons can be used, what goals would be served by such use, and who may give the orders to use them. Such policy has a major influence on how forces train (e.g., by driving the development and use of appropriate training scenarios).

One key question of employment policy relates to the necessary command and control arrangements. For example, although U.S. doctrine once did not differentiate between nuclear and non-nuclear weapons,[10]

[10] In 1954, President Eisenhower was asked at a press conference (March 16, 1954) whether small atomic weapons would be used if war broke out in the Far East. He said, "Yes, of course they would be used. In any combat where these things can be used on strictly mili-

this is most surely not the case today. Nuclear weapons are universally regarded as worthy of special attention, policies, and procedures, and their use is tightly controlled and highly centralized—more so than any other weapon in the U.S. arsenal. Whether similar arrangements will be made for cyberweapons in the future remains to be seen, although the discussion in Chapter 3 suggests that the command and control arrangements of today are not as centralized.

A second key question of employment policy is the targets of such weapons. Some targets are off-limits by virtue of the LOAC and other relevant international law. But the propriety of attacking other kinds of targets is often determined by doctrine and views of the adversary.

For example, in the nuclear strategy of the Cold War, considerable debate arose about the propriety of targeting adversary nuclear forces. Advocates of prompt hard-target kill capabilities (that would use a ballistic missile against a hardened adversary missile silo) argued that the adversary (generally the leaders of the Soviet Union) placed great value on their instruments of national power, such as their nuclear forces, and that placing such instruments at risk would help to deter actions that worked against the interests of the United States. Opponents of such targeting argued that threatening to destroy such targets only increased the likelihood that the adversary would launch its missiles on warning of attack, thus making accidental launch more likely.

Given that there are no cyber equivalents of hardened missile silos that constitute an adversary's retaliatory forces, no credible threat of annihilation, and no equivalent of launch on warning for cyber forces, nuclear strategy does not provide guidance for cyber targeting. What targets might or might not be appropriate for cyberattack and under what circumstances would this be so? From what can be determined from public statements, the DOD believes that cyberattack has military utility, and thus the use of cyberattack is subject to constraints imposed by the law of armed conflict.

At the same time and apart from the need to comply with the LOAC, good reasons may exist for eschewing certain kinds of cyberattack against certain kinds of target for reasons other than those related to operational efficacy. For example, cyberwarfare provides tools that can be focused directly on messaging and influencing the leadership of an adversary

tary targets and for strictly military purposes, I see no reason why they shouldn't be used just exactly as you would use a bullet or anything else." (See Eisenhower National Historic Site, National Park Service, at http://www.nps.gov/archive/eise/quotes2.htm.) Indeed, in 1953, the U.S. National Security Council noted that "in the event of hostilities, the United States will consider nuclear weapons to be as available for use as other munitions." (U.S. National Security Council (NSC), "Basic National Security Policy," NSC Memorandum 162/2, October 30, 1953, available at http://www.fas.org/irp/offdocs/nsc-hst/nsc-162-2.pdf.)

state. Message-based influence might help to persuade the leadership to make decisions helpful to U.S. national interests, such as terminating hostilities or refraining from using weapons of mass destruction. But at the same time, it may be undesirable to conduct destructive or disruptive attacks on the command and control systems that connect the adversary's national command authority to forces in the field.

Disconnecting an adversary's forces from their leadership may result in serious dysfunction, uncoordinated action, and psychological impact on the adversary such as fear and poor morale. Such positive effects must be balanced against possible negative effects, such as the inability of the adversary's leadership to direct its forces to surrender or to stand down. In addition, if forces in the field lose confidence in the authoritativeness of commands from their national command authority, they may resort to following standing orders issued before the conflict began—and such orders may well instruct these forces to act in more destructive ways than they otherwise would. These considerations are particularly important if the adversary has nuclear weapons and if the cyberattack cannot differentiate between command and control systems for the adversary's conventional and nuclear forces.

Other possible targets to be avoided may include those that could have significantly damaging effects on large numbers of non-combatants. Entirely apart from the moral and ethical issues raised by such attacks, conducting such attacks against a nation with a declared policy of responding to such attacks with nuclear weapons arguably increases the likelihood that such weapons would be used. Targets in this category might include national financial systems and electric power grids.

Cyberattacks may be a preferred method for targeting infrastructure under some circumstances. The United States may wish to conduct operations related to war recovery and stabilization in the aftermath of a conflict, and thus wish to preserve infrastructure as an important element in war recovery—the U.S. intent in Operation Iraqi Freedom (the Second Gulf War) in 2003 was to occupy Baghdad for some period of time thereafter and to enable Iraq to function as a sovereign nation. In its targeting of Iraqi infrastructure, the United States had to consider the possibility that destroying parts of it (e.g., the electric power grid) might impede war recovery efforts after the conflict. If cyberattacks made it possible to attack infrastructure in such a way that it was rendered non-functional for the duration of a conflict but could be easily restored to normal operation after the conflict was terminated, attack planners would have considerable incentives to prefer such attacks over more destructive ones.

A second issue relates to options for strategic use. As with nuclear weapons, the availability of preplanned options for cyberattack varying in scale, scope, and timing would increase flexibility and the ability to respond promptly to various strategic contingencies. A number of important questions arise in this context—the large amount of intelligence information likely to be needed for such options, the timeliness of information collected to support preplanned options, and indeed the actual value of prompt cyber response under various circumstances.

A third important issue is ensuring that cyberattack activities are sufficiently visible to higher authorities, including the political leadership. It is an unfortunate reality that during times of crisis, military actions that would normally be regarded as routine or "small" can lead to misperceptions of strategic significance. For example, routine air reconnaissance undertaken during times of crisis can be interpreted as a prelude to attack. In a cyberattack context, analogs could include the routine gathering of intelligence that is needed to support a cyberattack (e.g., port scans of Zendian systems) or the self-defense neutralization of an active cyberattack threat from a Zendian patriotic hacker under standing rules of engagement. The possibility is very real that Zendian authorities might perceive such activities as aggressive actions associated with a planned and deliberate cyberattack by the United States.

Keeping the political leadership informed of such activities is a problem even when considering traditional military operations. But because the resources and assets needed to conduct cyberattacks are small by comparison and the potential impact still large, it may be more difficult for higher authorities to stay informed about activities related to cyberattack.

Finally, the United States has a long-standing policy not to use cyberattack or cyberexploitation to obtain economic advantage for private companies (as noted in Section 4.1.2). However, the economic domain is one in which the operational policies of adversaries are markedly different from those of the United States. That is, adversaries of the United Staes are widely believed to conduct cyber-espionage for economic advantage—stealing trade secrets and other information that might help them to gain competitive advantage in the world marketplace and/or over U.S. firms. As noted in Section 2.6.2, the intelligence services of at least one major nation-state were explicitly tasked with gathering intelligence for its potential economic benefits. This asymmetry between U.S. and foreign policies regarding cyberexploitation is notable.

The committee also observes that national policy makers frequently refer to a major and significant cyberthreat against the United States emanating from many actors, including major nation-states. The result in recent years has been an upsurge of concern about the disadvantaged position of the United States in the domain of cyberconflict, and is most recently reflected in the still largely classified Comprehensive National Cybersecurity Initiative resulting from the National Security Presidential Directive 54/Homeland Security Presidential Directive 23 of January 2008.[11]

On the other hand, the committee's work has underscored many of the uncertainties that underlie any serious attempt by the United States to use cyberattack as an instrument of national policy. Moreover, military planners often engage in worst-case planning, which assumes that more things will go right for an adversary than for oneself. Thus, attack planners emphasize the uncertainties of an attack and assume that the defense will be maximally prepared and lucky. Defensive planners emphasize the uncertainties of defense and assume that the attacker will be maximally prepared and lucky.

In short, the committee sees a marked asymmetry in the U.S. perception of cyberattack—"they" (the adversary) are using cyberattack means effectively against us (the United States), but it would be difficult (though not impossible) for us to use such means effectively against them.

The question thus arises, What might be responsible for this perception? One factor is the conflation of cyberattack and cyberexploitation in the public discourse (see Box 1.4 in Chapter 1). As noted by General Kevin Chilton, commander of the U.S. Strategic Command, many of the incidents that are billed as cyberattacks are, more accurately, just old-fashioned espionage—people looking for information who don't necessarily represent military threats.[12] Thus, if the public discourse uses the term "cyberattack" (what this discussion calls cyberattack-AUIPD, for "cyberattack as used in public discourse," to distinguish usages) to include cyberexploitation, then the balance is between adversary cyberattacks-AUIPD (which would include what this report terms "cyberattack" [note absence of a tag] and which are largely espionage conducted for economic benefit) and U.S. "cyberattacks-AUIPD" (which by policy do not involve either cyberattack or cyberexploitation conducted for economic benefit), and in such a balance, adversary cyberattacks-AUIPD will obviously seem to be much more effective than those of the United States.

A third important factor contributing to this perception is the fact

[11] Public reports indicate that this initiative has 12 components intended to reduce to 100 or fewer the number of connections from federal agencies to external computer networks, and to make other improvements in intrusion detection, intrusion prevention, research and development, situational awareness, cyber counterintelligence, classified network security, cyber education and training, implementation of information security technologies, deterrence strategies, global supply chain security, and public/private collaboration. The cost of this initiative has been estimated at $40 billion. See, for example, Jill R. Aitoro, "National Cyber Security Initiative Will Have a Dozen Parts," *Nextgov*, August 1, 2008, available at http://www.nextgov.com/nextgov/ng_20080801_9053.php.

[12] Wyatt Kash, "Cyber Chief Argues for New Approaches," *Government Computer News*, August 22, 2008, available at http://gcn.com/articles/2008/08/22/cyber-chief-argues-for-new-approaches.aspx.

that as noted in earlier chapters, the United States provides only limited assistance to the private sector when it comes under cyberattack and restricts the ability of the private sector to engage in self-help activities (as discussed in Section 5.2), and it refrains from sharing intelligence information that would benefit individual private sector companies (as discussed in Section 4.1). Some other nations do not practice such restraint. The committee speculates that this asymmetry in policy may account for at least some of the perception of asymmetric advantage derived by others.

If these observations are accurate, what—if anything—can be done about it?

Regarding the conflation of cyberattack and cyberexploitation in public discourse, there is no remedy except to insist that a user of the term "cyberattack" make clear what is included under the rubric of the term he or she is using. If the many foreign cyberexploitation efforts were not described as "cyberattack," the level of tension over cyberattack would be knocked down to a considerable degree.

The case for the current U.S. policy regarding eschewing the use of U.S. intelligence agencies for the benefit of private firms is largely based on the desire of the United States to uphold a robust legal regime for the protection of intellectual property and for a level playing field to enable competitors from different countries to make their best business cases on their merits. If this policy position is to be revised, it seems that two of the most prominent possibilities are that (1) intelligence gathering for economic purposes ceases for all nations, or (2) the United States uses its intelligence-gathering capabilities (including cyberexploitation) for economic purposes. Under traditional international law, espionage—for whatever purpose—is not banned, and thus the first possibility suggests a need to revise the current international legal regime with respect to the propriety of state-sponsored economic espionage. The second possibility raises the prospect that current restraints on U.S. policy regarding intelligence collection for the benefit of private firms might be relaxed.

Both of these possibilities would be controversial, and the committee takes no stand on them, except to note some of the problems associated with each of them. The first—a change in the international legal regime to prohibit espionage—would require a consensus among the major nations of the world, and such a consensus is not likely. The second—a unilateral change in U.S. policy—does not require an international consensus, but has many other difficulties. For example, the U.S. government would have to decide which private firms should benefit from the government's activities, and even what entities should count as a "U.S. firm." U.S. government at the state and local level might well find that the prospect of U.S. intelligence agencies being used to help private firms would not sit well with foreign companies that they were trying to persuade to relocate to the United States. And it might well undercut the basis on which the United States could object to other nations conducting such activities for the benefit of their own domestic industries and lead to a "Wild West" environment in which anything goes.

After all is said and done, it may turn out that the most desirable (least undesirable) option for the United States is to learn to live with the current asymmetry. But if that is indeed the case, it should reflect a deliberate and considered assessment of the pros and cons of various options that in the committee's view has not yet been engaged.

6.1.4 Operational Oversight

Operations translate employment policy into reality. In practice, the U.S. armed forces operate on a worldwide basis and have many ongoing operations at any given time. For example, they constantly gather intelligence and reconnaissance information. Some of those operations are sensitive, in that they might be seen as provocative or otherwise inappropriate.

Thus, the U.S. government has established a variety of mechanisms intended to ensure that such operations are properly overseen. For example, the U.S. government sometimes specifies criteria in advance that define certain sensitive military missions, and then requires that all such missions be brought to the attention of senior decision makers (e.g., the National Security Council staff). In rare cases, a mission must be approved individually; more typically, generic authority is granted for a set of missions that might be carried out over a period of many months (for example). The findings and notification process for covert action is another mechanism for keeping the executive and legislative branches properly informed. From time to time these mechanisms are unsuccessful in informing senior decision makers, and it is often because the individual ordering the execution of that mission did not believe that such an order required consultation with higher authority.

In a cyberattack context, oversight issues arise at two stages—at the actual launch of a cyberattack and in activities designed for intelligence preparation of the battlefield to support a cyberattack.

6.1.4.1 Launching a Cyberattack

Another important operational issue involves delegation of authority to launch a cyberattack as part of an active defense of U.S. computer systems and networks. As noted in Chapter 3, the U.S. Strategic Command has authority to conduct such attacks for active defense under a limited set of circumstances. But it is not known how far down the chain of command such authority has been delegated.