THE NATIONAL ACADEMIES

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

This booklet is based on the report *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities.* The project that resulted in the report was supported by the MacArthur Foundation, Microsoft Corporation, and the National Research Council. It was conducted on an entirely unclassified basis, and the authoring committee did not access classified information either in gathering information for or in preparing the report.

BACKGROUND

Cyberattack refers to deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks. This report focuses on the use of cyberattack as an instrument of U.S. national policy. The U.S. armed forces are actively preparing to engage in cyberattacks, perhaps in concert with other information warfare means and/or with kinetic attacks, and may have done so in the past. Domestic law enforcement agencies also engage in cyberattack when they jam cell phone networks in order to prevent the detonation of improvised explosive devices. Such matters pose some very important issues that relate to technology, policy, law, and ethics.

Cyberattack is not the same as cyberexploitation, which is an intelligence-gathering activity rather than a destructive activity. Although cyberattack and cyberexploitation share some similarities, they differ in their objectives and in the policy and legal constructs surrounding them (Box 1). This contrast is relevant to much of the public debate using the term "cyberattack," which in common usage often lumps both attack and exploitation under the "attack" label.

Still, some technical and operational similarities have policy significance. A successful cyberattack requires a vulnerability, access to that vulnerability, and a payload to be executed (Box 2). A cyberexploitation requires the same three things—and the only difference is in the payload to be executed. That is, what distinguishes a cyberattack from a cyberexploitation is the nature of the payload. These technical similarities often mean that a targeted party may not be able to distinguish easily between a cyberexploitation and a cyberattack—a fact that may result in that party's making incorrect or misinformed decisions.

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

National Academy of Sciences • National Academy of Engineering • Institute of Medicine • National Research Council

Box 1—Cyberattack versus Cyberexploitation

	Cyberattack, attack, computer network attack	Cyberexploitation, intelligence, exploitation, computer network exploitation
Approach and intent	Degrade, disrupt, deny, destroy attacked infrastructure and systems/networks	Achieve smallest intervention consistent with desired operations
Relevant domestic law	U.S. Code Title 10 authorities and restrictions	U.S. Code Title 50 authorities and restrictions
Operational agency	U.S. Strategic Command (Joint Functional Component Command for Network Warfare)	National Security Agency
Main advocate in the U.S. government to date	U.S. Air Force	Director of National Intelligence
Interactions with tactical military operations	Based on explicit inclusion in battle plans	Based on intelligence reporting
Characterization of personnel	Warfighters	Intelligence community

Weapons for cyberattack have a number of characteristics that differentiate them from traditional kinetic weapons. Compared to kinetic weapons, many weapons for cyberattack:

- Are easy to use with high degrees of anonymity and with plausible deniability, making them well suited for covert operations and for instigating conflict between other parties.
- Are more uncertain in the outcomes they produce, making it difficult to estimate deliberate and collateral damage.
- Involve a much larger range of options and possible outcomes, and may operate on time scales ranging from tenths of a second to years, and at spatial scales anywhere from "concentrated in a facility next door" to globally dispersed.
- Are easily available to any interested party, ranging from nation-states to disaffected teenagers.

Cyberattack as a mode of conflict also raises many operational issues. For example, any large nation experiences cyberattacks all of the time, and many of these attacks are not being undertaken by an adversary nation. How will the United States know it is the subject of a cyberattack deliberately launched by an adversary government? There is also a further tension between a policy need for rapid response and the technical reality that attribution is a time-consuming task. Shortening the time for investigation may well increase the likelihood of errors being made in a response (e.g., responding against the wrong machine or launching a response that has large unintended effects).

ILLUSTRATIVE APPLICATIONS OF CYBERATTACK

Cyberattack can support military operations. For example, a cyberattack could disrupt command, control, and communications; suppress air defenses; degrade smart munitions and platforms; or undermine an adversary's defense industrial base or its warfighting capabilities. Cyberattack might be used to augment a kinetic attack or to enable such an attack to succeed, or to defend a friendly computer system or network by neutralizing the source of a cyberattack conducted against it.

Cyberattack can also support covert action, which is generally designed to influence governments, events, organizations, or persons in support of foreign policy in a manner that is not necessarily attributable to the U.S. government. The range of possible cyberattack options is very large; for example, a cyberattack-based covert action might be used to influence an election, instigate conflict between political factions, harass disfavored leaders or entities, or divert money.

Box 2—Technical Aspects of Cyberattack

A cyberattack requires **access** that allows the **exploitation of a vulnerability** to deliver a **payload**.

Access

- A remote-access cyberattack is an attack that is launched at some distance from the adversary computer or network of interest. The canonical example of a remote access attack is that of an adversary computer attacked through the access path provided by the Internet, but other examples might include accessing an adversary computer through an attached dial-up modem or wireless network.
- A close-access cyberattack is an attack on an adversary computer or network that takes place through the local installation of hardware or software functionality by nonadversary parties (e.g., covert agents, vendors) in close proximity to the computer or network of interest. Close access is a possibility anywhere in the supply chain of a system that will be deployed.

Exploitable Vulnerabilities

- *Software.* Application or system software may have accidentally or deliberately introduced flaws whose use can subvert the intended purpose for which the software is designed.
- *Hardware.* Vulnerabilities can also be found in any hardware element with computing or communications capabilities, including microprocessors, microcontrollers, circuit boards, power supplies, peripherals such as printers or scanners, storage devices, and communications equipment such as network cards. Tampering with such components may secretly alter the intended functionality of the component, or provide opportunities to introduce hostile software.
- *Seams between hardware and software.* An example of such a seam might be the reprogrammable read-only memory of a computer (firmware) that can be improperly and clandestinely reprogrammed.
- *Communications channels.* The communications channels between a system or network and the "outside" world can be used by an attacker in many ways. An attacker can pretend to be an "authorized" user of the channel, jam it and thus deny its use to the adversary, or eavesdrop on it to obtain information intended by the adversary to be confidential.
- *Configuration.* Most systems provide a variety of configuration options that users can set, based on their own security versus convenience tradeoffs. Because convenience is often valued more than security, many systems are—in practice—configured insecurely.
- *Users and operators.* Authorized users and operators of a system or network can be tricked or blackmailed into doing the bidding of an attacker.
- *Service providers.* Many computer installations rely on outside parties to provide computer-related services, such as maintenance or Internet service. An attacker may be able to persuade a service provider to take some special action on its behalf, such as installing attack software on a target computer.

Payload

"Payload" is the term used to describe the things that can be done once a vulnerability has been exploited. For example, once a software agent (such as a virus) has entered a given computer, it can be programmed to do many things—reproducing and retransmitting itself, destroying files on the system, or altering files. A payload may have multiple capabilities when inserted into an adversary system, and a payload may be remotely updatable if a communications channel to the attacker is available.

THE LEGAL FRAMEWORK GOVERNING CYBERATTACK

The committee's view of the basic framework for the legal analysis of cyberattack is based on the principle that notions related to "use of force" and "armed attack" (terms of special relevance to the Charter of the United Nations) should be judged primarily by the effects of an action rather than its modality. That is, the fact that an attack is carried out through the use of cyber weapons rather than kinetic weapons is far less significant than the effects that result from such use, where "effects" are understood to include both direct and indirect effects.

Furthermore, the committee believes that the principles of the law of armed conflict and the UN Charter—including both law governing the legality of going to war (*jus ad bellum*) and law governing behavior during war (*jus in bello*)—do apply to cyberattack.

- Prior to the outbreak of acknowledged armed conflict, if the effects (including both direct and indirect effects) produced by a cyberattack would, if produced by other means, constitute an armed attack in the sense of Article 51 of the UN Charter, the cyberattack would likely be treated as an armed attack. Similarly, if a cyberattack has the same effects and is otherwise similar to governmentally initiated coercive or harmful actions that are traditionally and generally not treated as the "use of force" (e.g., economic sanctions, espionage, or covert actions such as planting information or influencing elections), such a cyberattack would likely not be regarded as an action justifying a use of force in response.
- During acknowledged armed conflict (notably when kinetic and other means are also being used against the same target nation), cyberattack is governed by all the standard law of armed conflict (LOAC) criteria of *jus in bello*—military necessity, proportionality, distinction, and so on. If the effects of a kinetic attack are such that the attack would be ruled out on such grounds, a cyberattack that would cause similar effects would also be ruled out.

At the same time, the legal analysis in any given situation involving cyberattack may be more uncertain because of its novelty relative to the use of kinetic weapons, and new analytical work may be needed to understand how LOAC principles and those of the UN Charter do or should apply to cyberweapons. That is, some types of cyberattack are difficult to analyze within this traditional structure.

THE DYNAMICS OF CYBERCONFLICT

The escalatory dynamics of armed conflict are thought to be understood as the result of many years of thinking about the subject, but the dynamics of cyberwar are poorly understood. This report speculates on some of the factors that might influence the evolution of a cyberconflict.

For major nation-states with significant kinetic and cyber capabilities at their disposal, among the important issues regarding the dynamics of cyberconflict are the following:

- *Crisis stability.* Traditionally, crisis stability refers to that condition in which neither side has incentives to attack first. What, if any, are the requirements on forces for cyberattack that meet this condition?
- *Preventing a cyberconflict from escalating to physical space.*
- *Knowing when a cyberconflict has been terminated.* Against a background of ongoing cyberattacks, how will nations previously engaged in cyberattacks against each other know that such nationally initiated attacks have ceased?

Matters can be further complicated by the presence of non-state actors, such as cyberterrorists, patriotic hackers, and criminal groups. Perhaps the most important complication relates to identification of the appropriate party against whom action might be taken and the related availability of cybertargets whose destruction might cause pain or meaningful damage to the terrorist or criminal group.

FINDINGS

Overarching Findings

The policy and organizational issues raised by U.S. acquistion and use of cyberattack capabilities are significant across a broad range of conflict scenarios, from small skirmishes with minor actors on the international stage to all-out conflicts with adversaries capable of employing weapons of mass destruction. Outcomes of cyberattacks can vary across an enormous range and they can affect military, intelligence, diplomatic, economic, and law enforcement equities.

The availability of cyberattack technologies for national purposes greatly expands the range of options available to U.S. policy makers as well as to policy makers of other nations. Some cyberattack technologies can be operated reversibly or irreversibly; others can be used in a lethal/destructive or a non-lethal/non-destructive manner. Many cyberattack technologies are inherently clandestine and often relatively inexpensive. Cyberattack can be used for both offensive and defensive purposes, and can have both tactical and strategic implications as well. And the underlying technology is available everywhere in the world.

Nevertheless, **today's policy and legal framework for guiding and regulating the U.S. use of cyberattack is ill-formed, undeveloped, and highly uncertain.** Most of the public policy attention paid to cyberconflict focuses on the defense of friendly computer systems and networks against cyberattack. But the United States has no comprehensive publicly stated strategic national policy outside the criminal framework concerning how it will regard cyberattacks conducted on the United States or how it may use cyberattack in support of U.S. interests. One reason for the ill-formed state of policy in this domain is the fact that **secrecy has impeded widespread understanding and debate about the nature and implications of U.S. cyberattack** for military, intelligence, and law enforcement purposes. Secrecy has also meant a dearth of public scrutiny and congressional oversight and thus an increase in the likelihood that policy will be formulated with narrow parochial or short-term interests foremost in mind. Non-governmental research and investigation regarding cyberattack have been inhibited as well.

A technical point with deep and far-ranging implications for all aspects of policy related to cyberattack is that **the consequences of a cyberattack may be both direct and indirect.** Although cyberattacks are focused on computer systems or networks, it is often the case that these systems and networks control or influence other entities (people, kinetic weapons, machinery, and so on)—and **in some cases of interest, the indirect consequences of a cyberattack can far outweigh the direct consequences** and be far more significant than the direct consequences of destroying or damaging or disrupting the computer system or network initially targeted.

Legal/Ethical Findings

The conceptual framework that underpins the UN Charter on the use of force and armed attack and today's law of armed conflict provides a reasonable starting point for an international legal regime to govern cyberattack. However, those legal constructs fail to account for non-state actors and for the technical characteristics of some cyberattacks. Domestic law is also inadequate in certain ways, one consequence of which is that **in today's security environment, private parties have few useful alternatives for responding to a severe cyberattack that arrives over a network such as the Internet**. **Cyberattack also poses challenges to existing ethical and human rights regimes** in an era in which the information-technology-enabled features of modern society may be essential to life as the citizens of that society know it.

Policy Findings

Enduring unilateral dominance in cyberspace is neither realistic nor achievable by the United States. Cyberconflict is quite unlike the land, air, and maritime domains in which U.S. armed forces operate, largely because effective weapons of cyberattack are too inexpensive and easily available to be denied to any nation (or terrorist or other non-state actor for that matter), and much of the expertise needed to wield them is widespread.

In addition, **the United States has much to lose from unrestrained cyberattack capabilities that are proliferated worldwide** because it is highly dependent on the capabilities afforded by ubiquitous information technology in every sector, both military and civilian. Moreover, comparing the as-yet-unproven utility of U.S. cyberattack against its adversaries to the demonstrated growing dependence on information technology, it is reasonably clear that as a general rule, it is far more important for the United States to be able to use information technology freely in pursuit of its national interests than for it to be able to deny adversaries the use of their own systems and networks. However, this point does not rule out the possibility that cyberattacks by the United States will be an appropriate and useful action under some circumstances.

Deterrence of adversaries is the cornerstone of U.S. military strategy. However, **deterrence of cyberattacks by the threat of in-kind response has limited applicability.** Today's information technology makes it very easy for adversaries to conduct anonymous cyberattacks—and even in the event that new information technologies are developed with stronger authentication capabilities, a properly authenticated computer can still be improperly compromised by a third party. Thus, the perpetrator of a cyberattack may well be able to escape punishment or retaliation for his actions. Even if the attacker is known, an in-kind response to a cyberattack is unlikely to succeed because the attacker is likely to be able to take steps to thwart such a response.

Options for responding to cyberattacks on the United States span a broad range, and include a mix of dynamic changes in defensive postures, law enforcement actions, diplomacy, cyberattacks, and kinetic attacks. The United States is in no way obligated to employ an in-kind response to a cyberattack, even if an in-kind response may superficially seem the most obvious or natural course.

Technical/Operational Findings

Although cyberattack technologies are a relatively new addition to the technologies of warfare, **the ease of cyberattack on many kinds of information technology infrastructure targets is increasing rather than decreasing.** This is true for information technology targets in the United States, and is likely to be true for many other parties as well. This is not to say that cyberattack on certain specific targets will not be very difficult—but on average, the gap between the attacker's capability to attack many vulnerable targets and the defender's inability to defend all of them is growing rather than diminishing.

Although the actual cyberattack capabilities of the United States are highly classified, they are at least as powerful as those demonstrated by the most sophisticated cyberattacks perpetrated by cybercriminals and are likely more powerful. Although they are highly classified, knowledge of the lower bound of these capabilities is set by the most sophisticated cyberattacks known to have been perpetrated by cybercriminals, and such attacks have been sophisticated indeed. Although the fundamental base technologies available to the United States are likely to be more or less the same as those available to other parties, the enormous resources available to the U.S. government compared to those of ordinary cybercriminals would suggest that U.S. cyberattack capabilities are more sophisticated than those of even the most talented cybercriminals.

As is true for air, sea, land, and space operations, the defensive or offensive intent motivating cyber operations in any given instance may be difficult to infer. Cyberattacks, for example, can be undertaken for purposes of both offense and defense. However, the intent underlying a cyberattack may be very difficult to discern because of the constant background of cyberattack activity experienced by all computers connected to the Internet and because of a dearth of historical experience with nations or terrorists using cyberattack against the United States.

Certain cyberattacks undertaken by the United States are likely to have significant operational implications for the U.S. private sector because the private sector owns and operates much of the infrastructure through which a cyberattack might be transmitted and also has a significant stake in the continuing operation of that infrastructure. It is not new that military decision makers must consider the impact of their decisions on civilian parties (for example, reducing the availability of Global Positioning System satellites could have a major impact on nonmilitary transportation), but in many or most of these instances, such impacts could be spatially localized. But spatial localization of cyberconflict may well be impossible where the Internet is concerned, and the United States must be prepared to deal with the consequences should it take actions that provoke in-kind counterattack by an adversary. "Blowback" is also a concern, in the sense that actions taken to affect an adversary's systems or networks may inadvertently and negatively affect the United States.

If and when the United States decides to launch a cyberattack, significant coordination among allied nations and a wide range of public and private entities may be necessary, depending on the scope and nature of the cyberattack in question. Although cyberattacks that are narrowly focused on highly specific objectives may not have much potential for interfering with other ongoing cyber operations initiated by other parties, a sufficiently broad cyberattack might indeed interfere. In such cases, it may be necessary to coordinate among a number of parties, including various U.S. government agencies and allied nations, all of which may have various cyber operations underway that might interfere with a U.S. cyberattack on an adversary. In addition, these agencies and nations would likely benefit from the strengthening of their defensive postures that could occur with advance notice of a possible in-kind response. The same considerations apply to private sector operators of information infrastructure that would be likely targets of an adversary's in-kind response to a U.S. cyberattack and for which advance notice of cyberattack would be helpful in strengthening their defensive posture. Finally, in the midst of an overt conflict with another party, the United States will almost certainly have to suppress the actions of "patriotic hackers" who launch cyberattacks on the adversary nation on their own initiative. Such actions might interfere tactically with operations planned by the U.S. government, and strategically they might be misinterpreted by the party being attacked as intentional U.S. actions and thus complicate the conduct of diplomatic actions.

Planners for any kind of attack, kinetic or cyber, must take into account many uncertainties about the characteristics of the target and the environment around it. Nevertheless, because the information needed for a successful cyberattack (e.g., details of connections between two systems) is often more difficult to obtain through traditional methods such as remote photo reconnaissance, **the outcomes of many kinds of cyberattack are likely to be more uncertain than outcomes for other kinds of attack.** Greater intelligence efforts to resolve uncertainties are likely to be necessary to achieve levels of confidence equivalent to those that generally characterize kinetic attacks.

Early use of cyberattack may be easy to contemplate in a pre-conflict situation, and so a greater degree of operational oversight for cyberattack may be needed compared to use of other options. It is not new that "small" activities in a tense pre-conflict situation may have large consequences. But the operational footprint left by cyberattack capabilities is small, a fact that tends to render activities related to this area less visible to senior decision makers. Thus, senior leaders will need to take special care to maintain situational awareness of their own forces under these circumstances as well as awareness of adversary forces.

Lastly, **developing appropriate rules of engagement for the use of cyberweapons is very difficult,** and under some circumstances may be more difficult than developing rules for traditional weapons.

Organizational Findings

Both the decision-making apparatus for cyberattack and the oversight mechanisms for that apparatus are inadequate today. Adequate policy decision making and oversight require a sufficient base of technical knowledge relevant to the activities in question, an organizational structure that enables decision making and oversight to take place, and information about activities that are actually undertaken under the rubric of policy. But cyberattack is a relatively new addition to the menu of options that policy makers may exercise, and there are few precedents and little history to guide them today. Thus, it is perhaps not surprising that an adequate organizational structure for making decisions and exercising oversight has not emerged, and much of the information relevant to conducting oversight is unavailable.

The U.S. Congress has a substantial role to play in authorizing the use of military force, but the contours of that authority and the circumstances under which authorization is necessary are at least as uncertain for cyberattack as for the use of other weapons. The limits of that authority are the subject of much dispute between the executive and legislative branches. However, cyberweapons raise particularly difficult issues in this context (as do certain non-cyberweapons), because of the need for speed in using such weapons (e.g., because of a target's transience), the risk of unintended and unknown consequences, and the lack of visibility of their use.

RECOMMENDATIONS

Fostering a National Debate on Cyberattack

1. The United States should establish a public national policy regarding cyberattack for all sectors of government, including but not necessarily limited to the Departments of Defense, State, Homeland Security, Treasury, and Commerce; the intelligence community; and law enforcement. The senior leadership of these agencies should be involved in formulating this national policy.
2. The U.S. government should conduct a broad, unclassified national debate and discussion about cyberattack policy, ensuring that all parties—particularly Congress, the professional military and the intelligence agencies—are involved in discussions and are familiar with the issues.
3. The U.S. government should work to find common ground with other nations regarding cyberattack. Such common ground should include better mutual understanding regarding various national views of cyberattack, as well as measures to promote transparency and confidence building.

Organizing the Decision-Making Apparatus of the U.S. Government for Cyberattack

4. The U.S. government should have a clear, transparent, and inclusive decision-making structure in place to decide how, when, and why a cyberattack will be conducted.
5. The U.S. government should provide a periodic accounting of cyberattacks undertaken by the U.S. armed forces, federal law enforcement agencies, intelligence agencies, and any other agencies with authorities to conduct such attacks in sufficient detail to provide decision makers with a more comprehensive understanding of these activities. Such a periodic accounting should be made available both to senior decision makers in the executive branch and to the appropriate congressional leaders and committees.

Supporting Cyberattack Capabilities and Policy

6. U.S. policy makers should judge the policy, legal, and ethical significance of launching a cyberattack largely on the basis of both its likely direct effects and its indirect effects.
7. U.S. policy makers should apply the moral and ethical principles underlying the law of armed conflict to cyberattack even in situations that fall short of actual armed conflict.
8. The United States should maintain and acquire effective cyberattack capabilities.
9. The U.S. government should ensure that there are sufficient levels of personnel trained in all dimensions of cyberattack, and that the senior leadership of government has more than a nodding acquaintance with such issues.
10. The U.S. government should consider the establishment of a government-based institutional structure through which selected private sector entities can seek immediate relief if they are the victims of cyberattack.

Developing New Knowledge and Insight into a New Domain of Conflict

11. The U.S. government should conduct high-level wargaming exercises to understand the dynamics and potential consequences of cyberconflict.
12. Foundations and government research funders should support academic and think-tank inquiry into cyberconflict, just as they have supported similar work on issues related to nuclear, biological, and chemical weapons.

THE NATIONAL ACADEMIES
Advisers to the Nation on Science, Engineering, and Medicine

The nation turns to the National Academies—National Academy of Sciences, National Academy of Engineering, Institute of Medicine, and National Research Council—for independent, objective advice on issues that affect people's lives worldwide.
www.national-academies.org

COMMITTEE ON OFFENSIVE INFORMATION WARFARE

WILLIAM A. OWENS, AEA Holdings, Inc., *Co-chair*
KENNETH W. DAM, University of Chicago, *Co-chair*
THOMAS A. BERSON, Anagram Laboratories
GERHARD CASPER, Stanford University
DAVID D. CLARK, Massachusetts Institute of Technology
RICHARD L. GARWIN, IBM Fellow Emeritus
JACK L. GOLDSMITH, Harvard Law School
CARL G. O'BERRY, The Boeing Company
JEROME H. SALTZER, Massachusetts Institute of Technology (retired)
MARK SEIDEN, MSB Associates
SARAH SEWALL, Harvard University
WALTER B. SLOCOMBE, Caplin and Drysdale
WILLIAM O. STUDEMAN, U.S. Navy (retired)
MICHAEL A. VATIS, Steptoe & Johnson LLP

Staff

Herbert S. Lin, Chief Scientist, CSTB and Study Director
Kristen Batch, Associate Staff Officer
Ted Schmitt, Consultant
Janice Sabuda, Senior Project Assistant through March 2008
Eric Whitaker, Senior Project Assistant

Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the organizations that provided support for the project.

Details about obtaining printed copies of the report on which this brochure is based, together with more information about the Computer Science and Telecommunications Board and its activities, can be found at http://www.cstb.org. The Computer Science and Telecommunications Board is a unit of the National Research Council that provides independent and informed assessments of computing, communications and public policy.

Copies of this booklet are available free of charge from the Computer Science and Telecommunications Board, National Research Council, 500 Fifth Street, N.W., Washington, DC 20001, www.cstb.org.

Printed in the United States of America