ARMS CONTROL ASSOCIATION
The authoritative source on arms control

Published on *Arms Control Association* (http://www.armscontrol.org)

Arms Control Today > November 2009 > Weighing the Case For a Convention to Limit Cyberwarfare > Weighing the Case For a Convention to Limit Cyberwarfare

Weighing the Case For a Convention to Limit Cyberwarfare

By David Elliott

- Table 1: Multilateral U.S. Arms Control Agreements That Prohibit First Hostile Use

Cyberattack is emerging as a new type of nonlethal weapon that can cause substantial harm to society, especially when used in its most advanced version by countries at war. It may be time to consider an international convention to limit the initiation of such use, particularly against targets that are part of critical national infrastructure and are basically civilian.

Cyberattack refers to offensive actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information or programs resident in or transiting these systems. Its purpose is to mislead or disable an important network-dependent activity. A passive form of attack is cyberexploitation, which gathers intelligence information. A flip side of cyberattack is cybersecurity, which undertakes, through procedural and technical means, to defend against cyberintrusions. The concern addressed in this article relates primarily to the offensive and destructive version of cyberattack by one state against another state's critical infrastructure. There have been proposals to reduce the threat of cyberwarfare through an arms control agreement; some of the key issues underlying the pursuit of such an agreement are examined in this article.

The threat of serious cyberattack by state or nonstate actors has been on the U.S. security agenda for many years. There have been notable cyberattacks in recent years on the United States and other countries,[1] and President Barack Obama's recent "clean slate" review of cybersecurity notes other serious international attacks.[2] All of these attacks have occurred against an essentially constant background of lower-level probes that are not publicized. A common attack mode is the distributed denial of service (DDOS) blitz, in which tens of thousands of unwittingly cooperating computers are combined into a network (botnet) to flood a target's Web site and thereby disable it. The identity of the organizer and initiator of such an attack can be very difficult to determine, including, importantly, whether it is another government. The public reporting of events almost always speaks only of assumed or likely sources.

Attacks much more harmful than DDOS, with cascading effects, are technically feasible and are assumed to be under development, certainly at the state level. A characterization of the threat potential appears in a recent National Academy of Sciences (NAS) study of cyberattack as a weapon of war.[3] The threat, according to the study, is expected to grow in scope and sophistication.

As the United States continues to look for ways to protect its civil cyberdomain, it also has been actively pursuing, through its national security agencies, efforts not only to protect its own cyber-based military systems but also effectively to attack the cybersystems that are integral to a potential enemy's military capacity. The focus of the latter is on military and military-relevant targets but also may include components of an enemy's national infrastructure as a target of strategic information operations.[4] The U.S. offensive programs are very sensitive and thus never openly referenced in any of the last three presidents' public reviews of cybersecurity. Yet, they will be a background factor, possibly an important one, as the United States seeks international cooperation in protecting its critical infrastructure against cyberattack. In discussions preceding Obama's July meeting in Moscow, the Russians again raised the subject of an arms control agreement to restrict cyberwarfare. The United States did not support the initiative but urged the Russians to sign the Council of Europe Convention on Cybercrime as an important step in obtaining international cooperation in controlling the general threat.[5]

More than 10 years ago, the concept of an arms control agreement was examined as part of a broader government-sponsored program at Stanford University[6] and reviewed at a conference on infrastructure protection.[7] Even though the United States might potentially be the greatest beneficiary of such an agreement, the idea was not pursued further for several reasons, detailed below. Later, a draft amendment to the laws of war was suggested to deal specifically with the effects of cyberattack,[8] but it also did not trigger government interest. The issue is likely to continue to be pursued, and a brief review of the conflicting factors facing U.S. decision-makers may be useful.

Such a review could be fairly wide-ranging because the targets potentially vulnerable to cyberattack are extensive and varied. This article will be limited to the major question of how an agreement might restrict cyberattack by one state-party against the critical national infrastructure of another and to the pros and cons of such restrictions from a U.S. perspective. For the purposes of this article, "critical national infrastructure" is defined to encompass those large cyber-dependent networks that are important to the efficient functioning of society, including its economy and civil governance. Frequently cited examples are the electric power grid, telecommunications, the Internet, the financial system, transportation management, and many government services, including air traffic control. Many of these systems and services are dual use, and although primarily built to support the needs of the civil sector, they are used by and important to the military sector to one degree or another.

Existing Legal Limits

Several studies have examined what restrictions the present laws of war and other, less directly applicable agreements would place on cyberattack, including one directed at critical national infrastructure.[9] There is no clear answer, and specific cases would turn on the details of the attack and arguments over the proportionality of anticipated military effect and civilian harm. The self-defense article of the UN Charter would lessen the need to demonstrate military necessity or obtain Security Council approval to carry out retaliation-in-kind and active defense in response to a cyberattack, although consideration of proportionality would remain a restraining factor.[10] Attempts to use the current laws of war to build a body of precedents for restricting cyberwarfare would be protracted, hopefully by the infrequency of wars, and have an uncertain outcome. Further, this approach would not have the normative value of an explicit agreement.

The NAS study examined whether peacetime cyberattack directed at components of another state's infrastructure might be configured to fall below the threshold of an act of war (*jus ad bellum*). Such use would add to the United States' limited options for effective coercion short of military action.

U.S. Needs

A central question is whether the United States believes it can adequately protect its infrastructure against interstate cyberattack through its own actions or, instead, finds it needs international cooperation to move toward that goal. In the latter case, might that cooperation include and possibly be predicated on an international agreement to restrict interstate attacks, with prohibition of first use being a minimum commitment? At the same time, is the United States willing to limit this particular means of visiting strategic damage on an enemy during wartime or to deny itself a tool for coercing others in situations short of armed conflict? The answers to these questions will require the U.S. government to weigh the gains and losses between two contrary and incommensurable policy choices.[11] The nongovernmental sector can contribute to this analysis and debate. However, because of the sensitive and fragile character of this particular military capability and the resulting security restrictions, only the government will be in a position to judge the trade-off fully. In assessing the trade-off, there are three important underlying questions.

- Can the U.S. infrastructure be made robust enough to withstand state-level cyberattack, such that an agreement limiting offensive use would be unnecessary?

- Can the United States devise reliable cybermeans to attack an adversary's national infrastructure and predictably produce strategically important disruption?

- Is the normative value of an international agreement that is at best self-verifying[12] worth the limitation it would place on the United States, and can other states-parties be expected to conform their offensive decisions to the restrictions of such an agreement?

Protection Without an Agreement

The cybervulnerability of various elements of critical U.S. infrastructure was first examined in detail in the mid-1990s.[13] Since then, efforts to make the infrastructure more resilient have included technical and procedural advances in system security, adoption of new standards and practices, and, importantly, recognition by the involved domestic constituencies of the need for coordinated remedial action. There have been national action plans announced by three successive presidents,[14] with contributions to the plans from government agencies, companies in potentially affected sectors, professional associations, and academia.

Unfortunately, no periodic national report card characterizes the state of the threat and assesses the overall progress being made in protecting the infrastructure, but the conclusion of the latest high-level review is that U.S. vulnerability remains acute.[15] Comparing President Bill Clinton's public assessment of the problem with that of Obama nearly 10 years later, one would judge that the country is not making adequate progress. Part of that may well be due to the laissez-faire approach during much of the Bush administration, in which case the more directed efforts of the Obama administration may show better progress. Some impediments, however, are inherent to the problem. For instance, most of the critical infrastructure is privately owned, and businesses, unless required to do so, do not include or budget for measures to combat national security risks. They will shape their operations and invest in security against recognized nonstate threats to achieve dependable functioning of their enterprise but will be less willing to go beyond that. Moreover, some steps taken by private companies would require a number of legal exceptions to be made by governments. For example, businesses would need an exemption from antitrust laws to allow confidential joint planning and cooperation among competitors on cybersecurity matters. Companies also would need immunity from the Computer Fraud and Abuse Act's prohibition on damaging actions as they attempted to neutralize an attack at its origin.

Given this history and this basic impediment, it seems unlikely, certainly over the medium term, that national measures alone can achieve a strengthened U.S. infrastructure that could confidently face an evolving state-level cyberthreat, particularly if the NAS study is correct that the ease of cyberattack is increasing for many kinds of infrastructure targets.

Cyberattack Capability

Do U.S. leaders have enough confidence in their capability to attack the critical infrastructure of other states, and in the effects of such attacks, that they should resist attempts to limit that capability through international agreement? Few people can even begin to estimate an answer to this question in detail, and they cannot participate in any public debate. However, there are some general characteristics of large networked, interdependent cybersystems that should be taken into account when considering the surety of the capability. These characteristics include:

- Because the outcome of a cyberattack depends on the minute details of the target's configuration at the moment of attack and cannot be reliably predicted, such attacks are not a first-line offensive tool.

- Secondary and tertiary systemic and socioeconomic effects of an attack will often be more important than the initial effect. Because projecting these effects requires difficult-to-obtain specialized knowledge of the interdependence of the systems involved, such estimates will be unreliable. This latter consideration also makes it more difficult to project and control collateral damage.

- Because the hardware and software subsystems and operating procedures of a complex network are not permanent, maintaining a reliable attack capability may necessitate periodic digital probing, with its risks of discovery, premature exposure of target vulnerabilities, and installation by adversaries of measures to defeat the capability.

The U.S. military notes that cyberattack planning may require longer lead times, greater intelligence gathering, and more target preparation than are needed for conventional attacks.[16] It also realizes that launching an infrastructure cyberattack would require concurrent high-level political authorization.[17] Hence, its use cannot be reliably integrated into coordinated-attack planning for operations. The NAS points out that, if the government authorizes an attack, it will either have to warn the operators of U.S. infrastructure, thereby eliminating the option of plausible deniability, or accept the impact of a retaliatory attack without U.S. infrastructure defenses being alerted.[18]

The NAS study notes the argument that it is too early to consider limiting cyberattack against infrastructure as a military option because the technique is in its developmental stages. The study observes, however, that this stage is also the time of policy flexibility before a significant internal constituency has formed, in the United States and in other countries, to resist limitations on national capabilities for cyberattack.[19]

Because these considerations collectively are inconclusive, the basic question remains open within the public debate.

A Cyberattack Convention

To be acceptable to the United States, a cyberattack convention likely would have to take into account the following considerations:

- Military applications of cyberwarfare are useful and may become quite important. The United States would be unlikely to consider any limitations that would restrict the development, adoption, or use of this capability in general. Further, the development of measures to defend U.S. infrastructure will require threat characterization, to which an offensive program may be a major contributor. Such a program also would be the best source of knowledge for "red-team" testing.[20]

- The United States should insist on the option for retaliation in kind, for its potential effect and its deterrence value. The United States should also insist on the right to thwart an anticipated cyberattack by cybercountermeasures, as part of an active defense of national infrastructure.

- Barring a major breakthrough, compliance with any restrictions on use will be very difficult to verify in any reasonable time, owing to the considerable technical difficulty of forensic analysis and of tracing an attack's origin. Furthermore, treating all levels of attack as possible violations would overwhelm any U.S. verification regime, given the certainty of continuing lower-level cyberattacks from a variety of sources.

Considering these factors, the most practical convention would be multilateral and directed at first use and intent. It would set thresholds on the scale, duration, and severity of attacks and stipulate that exceeding any of the thresholds constituted a violation of the convention; reinforce the requirement for proportionality in anticipated effect on civil society; and preclude assistance to others in conducting prohibited attacks. No cooperative verification measures should be attempted, other than agreement by all parties to cooperate in the investigation of a claim of violation. Such cooperation is vital because some of the pertinent information will reside in third countries.

Arms Control Models

Table 1 lists the five major multilateral arms control agreements in which the United States participates that prohibit first use. In each case, the strategic gain was judged worth the loss of a relinquished capability, the latency risk (an important factor explained below) was deemed manageable, the potential security and political import of a breach (abrogation, violation, or withdrawal) was acceptable, and uncertainty about other parties' compliance was offset to an acceptable degree by self-verification measures.

Latency risk is a function of time. Given the estimated capabilities of a party, what is the time scale for that state to create, re-establish, or conduct the particular prohibited capacity or activity? High risk means short time. For example, the time from intention to action for a party to use incendiary weapons against prohibited targets (Protocol III of the Convention on Certain Conventional Weapons [CCW]) is immediate. Based on available know-how, records, stored equipment, and the permitted prophylaxis or defense reserves, the time for Russia to reconstitute a significant biological weapon capability might be a year or two. The time scale to violate the Environmental Modification (ENMOD) Convention might be decades because the underlying capability does not exist. If there is undetected preparation, all times would be less than estimated. There are two sources of latency, from dedicated or related military programs and from unconnected but applicable civilian enterprises. Civilian latency is only a factor in a few agreements, but when present, it can be important, as in the case of the Chemical Weapons Convention, where the verification procedures involve the monitoring of certain private companies.

Table 1 also estimates the importance of a breach from a U.S. security perspective. In addition, there is the political import of a breach, and that would be uniformly high, as it should be to reinforce the normative value of arms control agreements.

Assuming a breach would necessitate some form of quid pro quo response, a state can offset high latency risk by devoting resources to maintaining a reasonable latent capacity itself. The decision to conduct such a response would depend on the importance of the particular breach at the time it occurs.[21]

The latency risk accompanying a convention to limit cyberattack directed at critical national infrastructure would be high. Special preparatory actions would be required for a specific attack, but the overall capability would exist in the agency responsible for information operations. There would be some capability at the technology level within the civil sector, but it would require a longer development time and hence have a smaller latency risk. The security and political importance of a breach would be high.

The agreements in table 1 are the most relevant models for a cyberattack convention because they all contain no-first-use commitments. In addition, four of the five agreements define the prohibited weapon, and the ENMOD Convention describes the proscribed techniques and effects by example. Other than the inferred laws of war protection of noncombatants, none except for the CCW, in two protocols, defines a protected class of target. Only the ENMOD Convention sets standards in terms of scale, duration, or severity of unacceptable damage and constrains parties from assisting others in conducting the prohibited actions. The latency risk varies among the five, as does the import of breach, although none have high import.

By adding a definition of a protected class of target, namely, specified components of critical national infrastructure, the ENMOD Convention may be the closest model for a limited cyberattack convention. The two differ in one important way: the latency risk and the security import of a breach are judged to be low for environmental attack, whereas both are high for cyberattack. Nevertheless, the ENMOD Convention model may be a useful starting point for negotiation of a limited cyberattack convention.

Conclusion

The United States must take steps to protect its critical national infrastructure against serious cyberattack. One step might be to negotiate a multilateral convention to limit such attacks by states, which are the most likely source of an attack at the level of greatest concern. Although verification of compliance would be difficult, the convention in and of itself might be worthwhile for its norm-setting value, to be a restraining factor in the offensive decisions of other states, and as a necessary step in obtaining fuller international cooperation in controlling the general cyberthreat.

On the other hand, the U.S. military believes that cyberattack in its own hands may be an important addition to its war-making capacity. It may be unwilling to limit that capacity, particularly as the understanding of cyberwarfare potential is still being formed.

Balancing these conflicting objectives will require a full debate and executive decision. This process will have to be carried out by a special high-level government group because of the sensitive and fragile nature of certain aspects of the information involved.

One model of a convention that could serve as a starting point would commit the parties to no-first-use of cyberattack directed at elements of another party's critical infrastructure if the disruption from that attack was intended[22] to be widespread, long-lasting, or severe. One reason for these thresholds is to differentiate continuing, manageable lower-level attacks from those that constitute a serious violation by a state-party. All the terms in this commitment could be defined in an Understanding Annex, as in the ENMOD Convention, and would be the subject of negotiation. The convention would also preclude assistance to others in conducting prohibited attacks.

Because the cyberthreat is evolving rapidly and is difficult to define, any proposed solution is very unlikely to address the problem effectively for the long term or perhaps even the medium term. On the other hand, it may be important to constrain this form of warfare in the relatively early stages of its development. The type of limited convention described in this article strikes an appropriate balance by establishing some important initial parameters that could serve as the basis for more comprehensive agreements in the future.

Table 1: Multilateral U.S. Arms Control Agreements That Prohibit First Hostile Use

Agreement	Subject	Cooperative Verification	Latency Risk		Security Import of Breach
			Mil.	Civ.	
Geneva	Prohibits first use of poisonous	None specified	H	None	L/M

Geneva Protocol	Prohibits first use of poisonous gases and biological weapons	None specified	H	None	L/M
Biological Weapons Convention	Bans use, development, acquisition, or possession of biological weapons and agents, except for prophylaxis or defense	None specified	M	M	M
Environmental Modification Convention	Prohibits use of classes of environmental modification techniques to damage other parties	Cooperation in investigation of claims of breach	L	L	L
Chemical Weapons Convention	Bans use, development, acquisition, or possession of chemical weapons and agents, except for defense	Monitoring of destruction of existing agent and facilities and of commercial production of precursor chemicals; challenge inspections	M	M	M
Convention on Certain Conventional Weapons	Restricts use of fragment weapons, landmines, incendiary weapons, laser blinding, and remnants of war, with certain reservations by the United States	None specified	H	None	L
Key: H-high, M-medium, L-low, Mil.-military, Civ.-civilian. Assignments of values are the author's. See Arms Control Models (below) for further explanation.					

Click here to comment on this article.

David Elliott is an affiliate of the Center for International Security and Cooperation at Stanford University and a participant in its program on information security and policy research. He was a senior staff member and director for science and technology on the National Security Council during the Nixon and Ford administrations and was involved in the negotiation or ratification of several arms control agreements.

ENDNOTES

1. Mark Landler and John Markoff, "Digital Fears Emerge After Data Siege in Estonia," *The New York Times*, May 29, 2007, www.nytimes.com/2007/05/29/technology/29estonia.html; John Markoff, "Cyber Attack Preceded Invasion," *Chicago Tribune*, August 13, 2008, http://archives.chicagotribune.com/2008/aug/13/business/chi-cyber-war_13aug13; Siobhan Gorman and

Evan Ramstad, “Cyber Blitz Hits U.S., Korea,” *The Wall Street Journal*, July 9, 2009, http://online.wsj.com/article/SB124701806176209691.html.

2. The White House, “Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure,” n.d., www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (hereinafter White House cyberspace policy review); Office of the Press Secretary, The White House, “Remarks by the President on Securing Our Nation’s Cyber Infrastructure,” May 29, 2009, www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/ (hereinafter Obama cyber infrastructure remarks).

3. William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds., “Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities,” National Research Council, 2009 (hereinafter NAS study).

4. Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press, 2001); Chairman of the Joint Chiefs of Staff, “The National Military Strategy for Cyberspace Operations,” December 2006 (declassified), www.dod.mil/pubs/foi/ojcs/07-F-2105doc1.pdf.

5. John Markoff and Andrew E. Kramer, “U.S. and Russia Differ on a Treaty for Cyberspace,” *The New York Times*, June 28, 2009, www.nytimes.com/2009/06/28/world/28cyber.html.

6. Kevin Soo Hoo, Lawrence Greenberg, and David Elliott, “Strategic Information Warfare—A New Arena for Arms Control?” October 1996, http://fsi.stanford.edu/publications/strategic_information_warfare___a_new_arena_for_arms_control/.

7. Kevin J. Soo Hoo et al., “Workshop on Protecting and Assuring Critical National Infrastructure: Setting the Research and Policy Agenda,” October 1997, http://iis-db.stanford.edu/pubs/10354/it5.pdf.

8. Davis Brown, “A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict,” *Harvard International Law Journal*, Vol. 47, No. 1 (Winter 2006): 179-221.

9. For a summary of this extensive literature and further development of the subject, see NAS study, section 7.

10. NAS study, box 7.1.

11. In an arms control agreement, a government typically decides to accept a reduction in some aspect of its military capability so that it can better protect its military personnel and assets, as a result of the other side’s comparable military reduction. Although such tradeoffs may be difficult to assess, they are generally less difficult than those, such as the type under discussion in this article, in which the reduction in military capability must be weighed against the benefits to civilian populations and infrastructure. A further complication in the case of assessing the value of a cyberattack agreement is that the level of civilian damage and the value of the forgone military capability are difficult to quantify at this stage of cyberattack development.

12. Self-verification means that individual states determine the compliance of another state without help from any international entity, such as the International Atomic Energy Agency, or trustworthy cooperation from a suspected miscreant, but may include some input from an ally on a bilateral basis.

13. The White House, “Report of the President’s Commission on Critical Infrastructure Protection,” October 1997, http://lccn.loc.gov/98113463.

14. The White House, “Defending America’s Cyberspace: National Plan for Information Systems Protection Version 1.0: An Invitation to a Dialogue,” January 2000, http://clinton5.nara.gov/media/pdf/npisp-fullreport-000112.pdf; The White House, “The National Strategy to Secure Cyberspace,” February 2003, www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf; Obama cyber infrastructure remarks.

15. White House cyberspace policy review.

16. Joint Chiefs of Staff, “Information Operations,” Joint Publication 3-13, February 13, 2006, www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf.

17. John Markoff and Thom Shanker, “Halted ‘03 Iraq Plan Illustrated U.S. Fear of Cyberwar Risk,” *The New York Times*, August 2, 2009, www.nytimes.com/2009/08/02/us/politics/02cyber.html; Joint Chiefs of Staff, “Information Warfare: A Strategy for Peace, the Decisive Edge in War,” USGPO Doc. D 5.2:IN3, 1997, http://handle.dtic.mil/100.2/ada318379.

18. NAS study, pp. 1-25 – 1-26, 2-39.

19. NAS study, p. 10-6.

20. Red-teaming is a technique used in the development of military systems in which an independent friendly force undertakes to defeat a system and thereby identifies vulnerabilities that must be fixed. In the case of the Eligible Receiver project, government experts, using public information, analyzed and probed certain civil operational systems and found that many of them, thought to be secure from cyberattack, could be penetrated. See www.globalsecurity.org/military/ops/eligible-receiver.htm; John Hamre, interview, *Frontline*, PBS, February 18, 2003.

21. A good example of sensitivity to the circumstances of a breach is Russia’s recent deployment of troops in violation of the Conventional Armed Forces in Europe Treaty. That violation elicited little international response. If it had occurred during the Cold War, it could have been a *casus belli*.

22. U.S. intelligence analysts and the U.S. military would be expected to have some insights into an adversary’s intentions from its military manuals and journals and through military exchanges, observation of its military maneuvers, national technical means, and espionage.

Arms Control Today Features

1313 L St., NW, Ste. 130
Washington, DC 20005
Tel: (202) 463-8270 | Fax: (202) 463-8273

Source URL: http://www.armscontrol.org/act/2009_11/Elliott