Multilateral Agreements to Constrain Cyberconflict

- Arms Control Today

James A. Lewis

Cyberspace, the globally connected collection of networked computers and devices, is a new arena for conflict. Largely because of weak governance and technological shortcomings, cyberspace provides an ideal platform for malicious activity. The emergence of this new arena for conflict raises an important question: What kind of agreement could reduce the risk of conflict or, if conflict occurs, limit the scope of damage?

All advanced militaries have cyberattack capabilities, and many others are developing them. Cyberattack capabilities are not that different from other military technologies. Like aircraft or missiles, cyberattacks are rapid, cross borders easily, and can serve both tactical and strategic purposes. Cyberattacks are cheap and can strike an opponent's homeland from a distance. Cyberwarfare will involve the disruption of opponent network services and data, to increase uncertainty among opposing commanders;[1] it could also involve strikes intended to damage critical infrastructure, assets that are essential for economic and military functions, such as electrical power or telecommunications. Nevertheless, cyberattack will not be decisive. Cyberattack by itself will not win a conflict, particularly against a large and powerful opponent, but it will provide military advantage and will be part of future military conflict.

Cyberwar, however, is only one element of cyberconflict and not the most important. Cyberconflict today almost exclusively involves espionage and crime. Conflict in cyberspace is best seen as a continuum of belligerent activity, ranging from exploits undertaken for criminal purposes or espionage to military action aimed at producing disruption or destruction. Improving security in cyberspace requires disaggregating the various risks and challenges.

An overarching cybersecurity agreement or treaty that attempted to address the full range of conflict, including crime, trade issues (such as intellectual property protection), espionage, and military action, would be impractical. These issues are better handled separately and in separate venues. Focused agreements on specific issues are more achievable. For international security, an agreement that reduced the possibility of misinterpretation, escalation, or unintended consequences in cyberconflict is a legitimate subject for negotiation and could improve international security.

Yet, it is not clear what the best approach to multilateral agreement for cyberconflict would be. There are three major difficulties. First, the importance of information superiority in warfare and the ability to gain real military advantage from the use of informational assets makes digital infrastructures too valuable a target to be declared off-limits or for cyberattacks to be relinquished. In addition, because the techniques of attack and espionage are similar, asking for a commitment not to develop or use cybertools for penetration of opponent networks is really asking for a commitment not to spy. A "no-first-use" commitment might require countries also to renounce cyberespionage—something they are unlikely to do—and could even be destabilizing if a victim were to misinterpret a cyberespionage exploit as a "first-use" attack.

Second, verification will be extremely difficult. The close linkage to espionage makes countries reluctant to discuss or even admit they possess cyberattack capabilities. The necessary technologies are either commercial or easily derived from widely available commercial products—a laptop computer, an Internet connection, and a few computer programs. It is impossible to control the "precursors" for assembling "weapons." These precursors are cheap, small, portable, easy to

conceal, and, for sophisticated programmers in or out of government, easy to construct. Special-purpose tools for exploitation and cyberattack are widely available on thriving cybercrime black markets.

Finally, attribution—tracing an attack to its source—can be difficult. This difficulty is often overstated, as it is possible in many cyberincidents to use forensic techniques or active intelligence measures to determine who is responsible. Nevertheless, the attribution problem increases the temptation to use covert attack techniques based on widely available technologies. A successfully covert attack will have much less political risk. In addition, mercenaries, usually cybercriminals recruited by a state, can launch sophisticated attacks, providing an additional degree of deniability.[2] It is easy to overstate the difficulties created by weak attribution, but they do limit the scope of possible agreement.

These problems mean that approaches that seek to limit cyberattack through multilateral agreement on technological constraints face intrinsic and insurmountable difficulties. Cyberattack is a behavior rather than a technology. Cyberconflict is shaped by covertness, ease of acquisition, and uncertainty. Any cyberwarfare agreement that drew heavily on precedents derived from strategic arms agreements, which were often based on precise technological definitions and limits on development, production, or stockpiling, such as the Strategic Arms Reduction Treaty or the Conventional Armed Forces in Europe Treaty, will be impracticable. A legally binding convention that depends on renouncing first use, that attempts to restrict technology, or that requires verification of compliance is an unworkable approach for reducing risk to international security from cyberattack.

This does not mean that there can be no international agreement to constrain cyberwarfare. Although the United States remains cautious, there are indications that it and other nations are now willing to consider multilateral approaches to limiting cyberconflict. Multilateral agreements could increase stability and reduce the risks of miscalculation or escalation by focusing on several specific areas: confidence-building and transparency measures, such as increased transparency in doctrine; creation of norms for responsible state behavior in cyberspace; and expansion of common understandings on the application of international law to cyberconflict, or development of assurances on the use of cyberattacks.

Transparency

Building confidence through greater transparency in doctrine, in bilateral or multilateral exchanges, could reduce the chance of miscalculation or inadvertent escalation. The lack of transparency is politically damaging and could make it more difficult to win agreement on limiting cyberconflict. A recent global survey found that the United States was the most feared potential attacker in cyberspace; China was second.[3]

A few nations have produced public documents describing aspects of their cybersecurity strategy,[4] but their military doctrine on how they will use cybertechniques for offensive purposes remains hidden. Given the classified nature of military planning and the close ties to intelligence activities, complete disclosure in very unlikely, but this does not make it impossible to exchange views or discuss cyberwarfare. Although nations are unlikely to discuss specific techniques or technologies, an initial and general discussion of decision-making and authorization processes and principles for use could increase stability.

Greater insight into how combatants will decide when and how to use cyberattack would be stabilizing. In the Cold War, after years of discussion, the United States and the Soviet Union understood that nuclear weapons would be used only in extremis. Doctrinal debates and, ultimately, military and political exchanges on use allowed each side to better assess intentions and risk. Understandings among potential opponents on escalation of cyberconflict could allow for signaling, provide some measure of deterrence, and constrain actual conflict.

Most doctrine for the use of cyberattack remains secret, but some elements that have emerged into public view suggest that cyberattacks form an important part of planning for military conflict among leading countries.[5] There is anecdotal reporting that major powers have carried out network reconnaissance of potential critical infrastructure targets in preparation for possible attacks.[6]

These activities increase the risk of misinterpretation and unintended consequences, including the escalation and widening of conflict.

Miscalculation or misinterpretation could easily arise because the initial steps of cyberattack and espionage are identical. In both cases, the attacker conducts reconnaissance of the target network, gains access, and implants malicious software to take control. For espionage, the intent of the malicious action is to exfiltrate information. For an attack, the action would instead entail disruption or destruction instead of exfiltration. Better mutual understandings on doctrines and thresholds might reduce the chance of misinterpreting an intelligence exploit as an imminent attack.

Thresholds

The development of mutual understandings among nations on thresholds for conflict, including what actions can be considered a violation of sovereignty, on what constitutes an act of war, and what actions are seen as escalatory, could reduce the potential for cyberwar. Discussion by the international community of thresholds and how to define acceptable wartime conduct would help reduce ambiguities and possible misinterpretations.

The starting point for discussion lies with the law of war. There are two related bodies of law: jus ad bellum, which provides the framework for deciding whether a cyberexploit triggers a nation's right to self-defense, and jus in bello, laws that provide the framework for the use of cyberattack during an armed conflict. If cyberwarfare is approached as the use of a new technology to gain military advantage, the current body of international law can be applied to cyberconflict, but some issues may need expanded or new definitions or rules.

Agreement on what constitutes an act of war in cyberspace would be helpful. This could be defined as any action that produced an effect equivalent to an armed attack using kinetic weapons. One fundamental question is whether a cyberexploit must produce physical damage and casualties to be regarded as the use of force or whether intangible damage can be considered a use of force and an act of war.

Explicit agreements or understandings on what is a legitimate target in cyberspace could be stabilizing before and during conflict. Military infrastructures are clearly a legitimate target. Attacks against critical infrastructure—the electrical grid, government centers, oil and gas pipelines—are also legitimate targets even though they could cause significant harm to a civilian population. In this regard, cyberattacks resemble the use of airpower and "strategic" bombing, in that an attacker can use them to damage an opponent's will and capacity to continue to fight. Multilateral agreements for cyberattack would need to recognize that if it is legitimate to attack a target physically, it is also legitimate to attack it using cybertechniques.

Any agreement will need to distinguish between actions taken on one's own network, in territory under one's own jurisdiction, to defend against attack and actions taken against the attacker's network in the national territory of the opponent. Defensive actions taken within one's own territory pose a much lower risk of misinterpretation, retaliation, or escalation of conflict.

Actions over third-party networks pose a more difficult problem, what can be termed the "overflight" issue. Almost all cyberexploits require traversing third-country networks to reach the target. They are disguised as legitimate commercial traffic that is permitted to cross frontiers under existing commercial law and "interconnect" agreements among Tier 1 service providers—the large, interconnected, high-capacity networks that connect countries and continents.

Few states now know what passes over their networks en route to somewhere else or what the intent of that traffic may be, due to the covert or clandestine nature of these exploits. Over time, this knowledge will increase. Countries are enhancing their capability to monitor what crosses their networks in order to intercept malicious traffic aimed at themselves or to block content they deem inappropriate. One example is a technology known as "deep packet inspection," a relatively new technology that allows traffic to be screened for malicious content. These technologies are extending national sovereignty into cyberspace. Should they become widespread, understandings on passage rights or restrictions on military traffic may become essential.

The potential for collateral damage complicates the planning of cyberattacks. Neutral third-party networks may connect to or depend on the target network in ways that are not immediately apparent or easily discovered. These third-party networks could be found on the opponent's territory or in other states, even in allied countries. The grid of networks that comprise cyberspace does not follow the logic of national boundaries but of commercial and technical efficiency. The interconnections among different countries are extensive, evolve rapidly, and in many cases are not known to attackers or even to the parties that rely on them. A cyberattack aimed at North Korea, for example, might inadvertently damage China or Japan, harming an ally or threatening to widen any conflict.

In itself, the difficulty of assessing the scope of collateral damage imposes a constraint on cyberconflict, by increasing the political risk of cyberattack intended to produce disruption or destruction. Because an attacker cannot predict with confidence that a large-scale attack will damage only the intended target or even only the intended target country, military commanders and political leaders are likely to be cautious in the use of cyberattack. The same constraint, however, does not apply to nonstate actors.[7]

Attacks on an opponent's military networks and information or the networks that support critical infrastructure can be defended as legitimate military objectives, but decisions to move from exploitation to disruption and damage create a real risk of escalation of conflict beyond cyberattack. A decision to broaden the scope of an attack from an opponent's network or computers to other networks not directly involved, or to move from purely military targets to civilian targets, such as critical infrastructure, brings significant risk of escalation. It would be useful to have agreement among states on the implications of moving from military targets to broader critical infrastructure or other civilian targets and whether this is an expansion in the intensity or scope of cyberattack.

NATO and Soviet doctrine each ultimately reserved the use of nuclear weapons for extreme situations. In contrast, because no advanced military is likely to renounce exploitation of an opponent's networks, cyberattacks (at least against military networks) will be routine in future conflict. Such circumstances raise the risk of misinterpretation or unintended consequences; it therefore would be useful to identify the types of thresholds described above.

Even in a conflict, a decision to strike civilian targets in an opponent's homeland using cyberattack is a major step that brings with it the risk of serious escalation. A decision to undertake this kind of attack, or to move from military targets to civilian targets, such as critical infrastructure, could be interpreted as a major escalation. Countries may reserve these serious cyberattacks against targets in the opponent's homeland for either retaliation for attacks against their own homeland or extreme situations, but this implicit or presumed constraint on use could be strengthened by greater transparency and discussion.

Inadvertent damage to third-party networks, including those in neutral countries and allies, also carries significant political risk and the potential for expanding any conflict.

In considering what would be legitimate targets for cyberattack, some observers have proposed the idea of designating certain networks, such as those of hospitals, as sanctuaries. It would be possible to reach agreement not to deliberately target such networks—not to scramble or erase patient data in hospitals, for example—but there can be no assurance that the disruption or damage caused by a serious cyberattack will be confined to the intended target. A decision to disrupt power supplies will affect military targets and hospitals. An attack on critical infrastructure, with its unavoidable spillover to civilian targets, does not allow for the possibility of sanctuary. To the extent belligerents have already agreed to the legal principle of "distinction," which requires that attacks be limited to legitimate military objectives and that civilian objects not be the object of attack unless "demanded by the necessities of war," additional agreements specifically for cyberconflict may be redundant.[8]

Norms

Norms shape behavior and can limit the scope of conflict. Nonproliferation provides many examples of nonbinding norms that exercise a powerful influence on state behavior, such as the Missile

Technology Control Regime's (MTCR) understandings on missile transfers. A country's calculus of the benefits of a cyberattack can be affected, to varying degrees, by the concern over the reaction of the international community. The goal in developing international norms for cyberconflict would be to stigmatize certain actions in cyberspace and to reduce uncertainty by creating a normative framework for cyberconflict. There are already implicit norms for conflict in cyberspace; international security would be improved if these were expanded and made explicit.

Norms could be based on implicit understandings on what constitutes an act of war and on a distinction between defensive actions taken on one's own networks and defensive actions that involve interfering with the alleged attacker's networks. Making these understandings explicit would help to constrain cyberconflict.

Other norms could provide multilateral understandings on acceptable behavior in cyberspace—explicit norms or obligations that established state responsibility for the private actions of its citizens. Such an obligation, for example, would remove Russia's ability to plausibly deny its involvement in attacks on Estonia on the grounds that it was "patriotic hackers" rather than the government that carried out these exploits.[9] Just as nations feel a degree of constraint from norms and agreements on nonproliferation, establishing explicit international norms for behavior in cyberspace would affect political decisions on the potential risk and cost of cyberattack. A related line of inquiry would be to establish what actions the international community should take when a sovereign state fails to exercise responsibility for actions taken on its territory.

Another norm might be agreement on preserving the stability and continued operation of the global Internet. Although the Internet itself is very robust and resilient, and administrative bodies such as ICANN work to increase this,[10] there are likely vulnerabilities that a nation could exploit in conflict. An extreme action would target the global Internet itself, perhaps by corrupting the protocols that guide its operation. Incidents in 2002 involving fairly primitive attacks showed that the Internet itself can be targeted.[11] Agreement not to interfere with the stability and continued operation of the global system would be useful in limiting damage from cyberconflict.

Obstacles to Agreement

China and Russia talk about information security, not cybersecurity, and see access to certain kinds of information over the Internet as destabilizing and hostile, another form of attack.[12] In contrast, the United States and other Western countries do not see free access to information as a hostile act but rather as something intrinsically valuable.[13] Disagreement over this issue could be the first hurdle any cyberconflict agreement would face. China and Russia see access to information as posing as much risk as attacks on critical infrastructure; they will be unwilling to accept an agreement that address Western concerns but not their own.

Some countries use cybercriminals as proxies or irregular forces for cyberconflict. Better cooperation in reducing cybercrime would constrain the use of proxy forces. The dilemma is that it can be difficult to determine if the attacker is a state or a private party. The international community could reduce this dilemma through greater multilateral cooperation in fighting cybercrime. This would reduce the risk of interpreting a criminal act as an attack and, with it, the scope for misinterpretation or deception.

There is considerable dispute over how best to achieve this cooperation. The United States and its partners prefer the Council of Europe's Convention on Cybercrime.[14] China and Russia have refused to sign and instead offer the Shanghai Cooperation Organization as a vehicle for cooperation on cybercrime.[15] Brazil, India, and South Africa say the Council of Europe convention is too cumbersome and that they did not participate in its development. The absence of an agreed vehicle for multilateral cooperation against cybercrime is a serious impediment to better cybersecurity. Establishing a norm making a state responsible for cyberactions taken from its territory, combined with increased cooperation against cybercrime, would make these irregular forces less attractive and more difficult to sustain.

The Way Ahead

For years, the United States resisted the idea of any international agreement to constrain cyberwarfare. In the case of a binding cybersecurity treaty originally proposed by Russia in 1998 in the United Nations to ban information weapons, the United States questioned its efficacy and the intentions of its sponsors.[16] The refusal also reflects the larger rejection by the Bush administration of the UN, arms control, and international engagement. This blanket rejection of international engagement did not serve U.S. interests in cyberspace. Although the United States has very advanced offensive capabilities in cyberspace, it is also the country most dependent on networks for military and economic activities. The United States would benefit more than other countries from norms and constraints. The failure to engage allows countries with different values and interests to set the agenda for cybersecurity.

Perhaps more importantly, this blanket rejection only reinforced foreign concern over U.S. intentions and capabilities in cyberspace. Other countries were alarmed by announcements from the United States on the creation of an Air Force Cyber Command and the call for “cyberwarriors.” They saw this, along with the refusal to engage in negotiations, as part of a larger U.S. strategy to dominate cyberspace (similar to the 2005 National Space Strategy, which called for control and dominance in space).[17] This apparent plan for dominance redounded against the United States in many ways, not the least of which was a determined effort by other nations (still ongoing) to wrest “control” of the Internet from the United States.

It is in the U.S. national interest to negotiate and enter into agreements to constrain other nations’ abilities to attack in cyberspace. This will require the United States to develop a serious negotiating strategy that identifies the strategic trade-offs and linkages—the limits the United States would seek and the capabilities it might be willing to give up to achieve them. Despite a 2003 national strategy and a 2009 60-day review for cybersecurity, the United States has not made this strategic calculation. Thinking about cyberconflict is at an early stage, similar to the state of U.S. thinking on nuclear weapons in the 1950s.

Venue and format will be important elements in the development of any agreement on norms, transparency, and common understandings. The options include working with a group of like-minded nations, working with a broader group of key actors in fora such as the Group of 20 (G-20), or a global effort through the UN or one of its agencies. All three approaches have merit. Like-minded nations are more likely to reach agreement on norms; the experience of the MTCR shows that starting with a limited group avoids the possibilities of opponents acting as “spoilers” and can lay the groundwork for broader cooperation in the future. A G-20 approach has the benefit of involving influential nations, such as Brazil, China, India, and Russia, beyond NATO and other U.S. allies. Although this increases the chances of initial discord, the ultimate acceptance of norms and understandings by these nations is essential for success.

Similarly, discussion in the UN involves a broader audience of nations not directly involved in cyberconflict and whose views and actions may be shaped by some larger political agenda. Nevertheless, the UN has a useful body of precedent in counterterrorism and arms control. Given the global nature of cyberspace, some global understanding of norms for behavior will ultimately be required.

In the end, engagement at all three levels—like-minded countries, key actors, global community—may be necessary. Some lessons from nonproliferation can be instructive. Internationally, the United States strengthened existing multilateral organizations against weapons of mass destruction or created new ones, such as the MTCR, to develop cooperative approaches to security. Working with like-minded partners, the United States was able to make nonproliferation a norm for international behavior and, over time, see other nations adopt this norm. Although the precedent is not perfect, and the risks and requirements are different for cyberwarfare, nonproliferation offers a useful framework for developing the elements of a cooperative approach to cyberwarfare.

James A. Lewis is a senior fellow and director of the Technology and Public Policy Program at the Center for Strategic and International Studies. He was project director for the center’s report, “Securing Cyberspace in the 44th Presidency.”

ENDNOTES

1. This is more than traditional disinformation as it could include scrambling of data and interference with sensors.

2. Covert operations are “planned and executed [so] as to conceal the identity of or permit plausible denial” by the attacking state. U.S. Department of Defense, Dictionary of Military and Associated Terms (Joint Publication JP1-02).

3. John Sexton, “U.S. Most Likely Suspect in Cyber Wars: IT Survey,” China.org.cn, January 30, 2010.

4. UNIDIR, “Existing and Potential Threats in the Sphere of Information Security,” November 2009.

5. See, for example, Qiao Liang and Wang Xiangsui, Unrestricted Warfare (Beijing: PLA Literature and Arts Publishing House, 1999).

6. A recent example is GreyLogic, “Project Grey Goose Report on Critical Infrastructure: Attacks, Actors, and Emerging Threats,” January 21, 2010.

7. Shane Harris, “Why the U.S. Won’t Pull a Brazil Yet,” The Atlantic, November 19, 2009.

8. Article 23 of the Hague Convention, for example, forbids belligerents “to destroy or seize the enemy’s property, unless such destruction or seizure be imperatively demanded by the necessities of war.”

9. Roland Oliphant, “Patriotic Hackers,” The Moscow News, August 2009.

10. The Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for managing the Internet’s addressing system. See ICANN, “Plan for Enhancing Internet Security, and Resiliency,” June 2009.

11. Edward Hurley, “Attack on DNS Servers Marks Trend of More Internet Threats,” SearchSecurity.com, October 24, 2002.

12. See, for example, Andrey Krutskikh, “On Legal and Political Foundations of Global Information Security,” International Trends, Vol. 5, No. 1 (January-April 2007); World Federation of Scientists Permanent Monitoring Panel on Information Security, “Toward a Universal Order of Cyberspace: Managing Threats From Cybercrime to Cyberwar,” WSIS-03/GENEVA/CONTR/6-E, August 2003.

13. Hillary Rodham Clinton, Remarks on Internet freedom, Washington, DC, January 21, 2010.

14. The cybercrime convention is a legally binding treaty that defines criminal acts in cyberspace. Fifteen states have ratified it; another 30 have signed, but not ratified the convention.

15. The Shanghai Cooperation Organization is a multinational arrangement for security cooperation that was created by China, Russia, and four other nations in 2001.

16. John Markoff and Andrew E. Kramer, “U.S., Russia Disagree on Need for Cyber Treaty,” The New York Times, June 28, 2009.

17. Ambassadors to the UN, interviews with author, February 2009.

Posted: June 4, 2010

Source URL: https://www.armscontrol.org/act/2010_06/Lewis