SHADOW WARS

Debating Cyber 'Disarmament'

Tom Gjelten

The United States and other major military powers are well prepared to fight on land, at sea, in the air, and even in space. Now, countries must consider the prospect of combat in a fifth domain: cyberspace. It's unfamiliar, and it's frightening. The attacks in 2007 and 2008 on government Web sites in Estonia and Georgia, minor though they were, focused the world's attention for the first time on the prospect that hostile militaries could inflict great damage on other countries by targeting their computers. In announcing a cybersecurity initiative nine months after the attacks in Georgia, President Obama said they offered "a glimpse of the future face of war." Researchers who have studied the new Stuxnet computer worm, capable of commanding industrial control systems, describe it as the first "cyber superweapon."

"Cyber war" was not even part of our lexicon twenty years ago, and governments are still trying to figure out what exactly it might mean. Different ideas of the cyber danger around the world illustrate that countries vary in the way they perceive their own vulnerabilities. In advanced industrial democracies, with power, telecommunications, transportation, finance, and all other systems deeply dependent on data networking, it is not hard to see how a disruption of computer infrastructure could cripple

Tom Gjelten is a correspondent for NPR.

a society. In less developed, less networked, and more insecure countries, however, the cyber battlespace may be associated more with politics than technology. The Internet's explosive spread means that people can connect and communicate far more easily, exchange ideas, provoke each other, and mobilize for action. "Traditionally reserved and unresponsive governments appear shell-shocked by this powerful technology," notes a U.S. diplomat with years of negotiating experience. "It enables coalitions of citizens to challenge them for the first time."

Mindful in their own ways of all the cyber threats, governments are seeking new international agreements. There is interest, for example, in applying the law of armed conflict, reflecting more than a hundred years of legal thinking and war experience, to cyberspace. Thanks to treaties, the U.N. charter, the Hague and Geneva Conventions, and various "customary" understandings, we can legally distinguish aggressors from victims, and we have principles that, when honored, protect civilians from undue suffering. Another idea is to bring the idea of arms control to the cyber domain, with the goal of drafting accords under which governments voluntarily agree to constraints on the development of their own cyber capabilities and promise to behave in cyberspace.

While peace accords and disarmament agreements are attractive, however, democracies have reason to proceed cautiously in this area, precisely because of differences in the way cyber "attacks" are being defined in international forums. Russia, which for more than a decade has been promoting a global cyber arms control agreement, would like to criminalize what Soviet diplomats once called "ideological aggression," and China and allied governments, especially in the Middle East and Africa, share this view. Indeed, the idea of a cyber arms accord has been interpreted in some countries as justifying expanded governmental control over the Internet. If diplomats are not careful, one by-product of a push to regulate state-on-state cyber conflict could be a new effort to subject Internet activity to political scrutiny.

Such a trend is already under way at the International Telecommunications Union (ITU), a United Nations agency that in recent years has been known best for its assignment of country codes and its jurisdiction over international telephone charges. As the global telecommunication system has evolved, the ITU mission has declined in importance. But the spread of the Internet has put the ITU in a position to play a far more ambitious—and potentially troublesome—global role as an arbiter of what

should be allowed in the cyber domain. If ITU Secretary General Hamadoun Touré gets his way, his 192 member countries will soon be drafting a global treaty to regulate state-on-state cyber behavior. In October 2009, Touré told a meeting of ITU members that "by the end of next year, we [need to] broker a global agreement in which every country commits itself not to attack another country first." On the eve of an October 2010 ITU plenipotentiary conference in Guadalajara, Mexico, Touré reiterated his goal. "My dream is to have a cyber peace treaty," he said.

The question is: Which view of "cyber peace" will prevail? Does it mean protection against the destruction of civilian infrastructure that would result from an all-out cyber war? Or might it mean increased governmental control of Internet communications, to ensure that politically problematic content is kept to a minimum or removed entirely?

Touré, an electrical engineer from Mali who was trained in the old Soviet Union, owes his ITU election in large part to Russian backing, and he has been working hard to line up support among ITU member states for the Russian cyber agenda. The ITU plenipotentiary and other international meetings have drawn into focus the question of who, exactly—in a time of shifting global alignments—will shape the Internet of the future. "This is one of the most important geopolitical battles of our time," said a Western official who follows Internet developments closely but keeps a low profile. "This is ground zero for global diplomacy, national security work, and intelligence. It's all coming together at this little point."

Russia launched its cyber arms control initiative at the U.N. General Assembly in 1998 with a resolution calling on U.N. states to develop "international principles" that would help combat what it called "information terrorism." The Russian resolution noted that new information technologies offered opportunities for "the further development of civilization" but could also be used "for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the security of States."

The Russians introduced similarly worded resolutions annually thereafter. The word "cyber" never appeared in any of the resolutions, even after it became a widely used term. The Russian concern was "information security," a concept under which words might be seen as weapons.

The idea that information transmitted via the Internet could threaten the "stability" of states appealed in particular to authoritarian regimes, and in the coming years the co-sponsors for the Russian resolution included such countries as Belarus, Burma, China, Cuba, Turkmenistan, Vietnam, and Zimbabwe.

In an effort to win the broadest possible support at the U.N., the Russians agreed every year to amendments that softened their resolutions, but Russian officials made their views clear in supplementary reports and government statements. Three experts from the Russian Ministry of Defense, writing in 2007 for the United Nations' disarmament journal, argued that an "information campaign" directed by one country against another could under some circumstances be classified as "aggression" and therefore was illegal under the U.N. charter. "Almost any information operation with a psychological basis," they said, "implemented in peacetime with respect to another state, would qualify as intervention in its domestic affairs. Even good intentions, *such as the advancement of democracy*, cannot justify such operations" (emphasis added).

In venues where the Russians felt more confident, they were even bolder. In August 2009, the six member states of the Shanghai Cooperation Organization (SCO)—Russia, Kazakhstan, Kyrgyzstan, Tajikistan, Uzbekistan, and China—approved a Russian-drafted agreement that cited the Russian U.N. resolution and elaborated on it. The SCO accord defined "information war" in part as a "confrontation between two or more states in the information space aimed at...undermining political, economic, and social systems [or] mass psychologic [*sic*] brainwashing to destabilize society and state." Among the "security threats" described in the agreement was the dissemination of information harmful to the "spiritual, moral, and cultural spheres of other States." The wording seemed to justify censorship of dissident writings on the Internet and bar countries from supporting such Internet activity in another state. The signatory countries resolved to work for "collective measures" that incorporated those ideas. U.S. officials interpreted the agreement as expressing the Russian and Chinese vision of what a U.N. cyber arms control agreement should entail, and they suspected the accord was concluded with the idea that it might serve someday as a source of customary international law, which arises through accepted precedents and practices rather than through formal conventions.

Western governments realized there was undemocratic thinking behind the Russian "information security" proposal, but the resolution also spoke to more traditional concerns about cyber conflict, and until 2005 it was approved by consensus. Important issues, however, remained unresolved. The idea of cyber arms limitation was complicated by the fact that cyber "weapons" are often software programs that, unlike missiles or tanks, cannot be seen or counted. A separate question was whether the existing law of armed conflict dealt adequately with cyber war scenarios or needed to be modified.

Current international law stipulates, first, the circumstances under which one state is justified in going to war against another and, second, how militaries should conduct themselves once they are at war, in order to minimize human suffering. Under the U.N. charter, a state has the right to use force against another state if necessary to defend itself against an "armed attack," or if it is authorized by the Security Council. Otherwise, states are prohibited from using or threatening to use force "against the territorial integrity or political independence of any state." The conduct of militaries already at war is governed by the Hague and Geneva Conventions (to the extent countries have endorsed them) and by customary international law.

But what constitutes an "armed attack" in cyberspace? There are no soldiers crossing borders or shots fired. International law pertaining to the actual conduct of military operations is also unclear. Among the key principles under the Geneva Conventions is that the damage inflicted in a military attack should be "proportional" to the objective and that civilian targets should be avoided. But the application of those principles to cyber war is problematic. A targeting officer can use algorithms to predict the damage that will be caused by a bomb, based on its size, the angle of its approach, and the strength of the target, but an attack on a computer network can have unpredictable second- and third-order effects. The geographic spread of infections from the Stuxnet computer worm suggests that even a cyber weapon with extraordinary targeting capability cannot be easily controlled once it is let loose.

Under the Bush administration, little progress was made in the cyber war discussions at the U.N. and elsewhere. Many conservatives had a longstanding aversion to arms control in general, having concluded from experiences with the Soviets during the Cold War that the U.S. military

would generally adhere to treaty and legal commitments while its adversaries would not. Among those who question the value of discussing cyber war from a legal or arms control perspective is Stewart Baker, a former general counsel at the National Security Agency and an assistant secretary for policy at the Department of Homeland Security under President George W. Bush. "It is a near certainty that the United States will scrupulously obey whatever is written down," Baker says, "and it is almost as certain that no one else will."

The U.S. disadvantage would be compounded by the fact that, by most analyses, no other military has such an advanced offensive capability for cyber war. Under a comprehensive cyber arms limitation agreement, the United States would presumably have to accept deep constraints on its use of cyber weapons and techniques. Critics also point to the so-called "attribution problem." In conventional warfare, an aggressor can quickly be identified, and the responsibility for war crimes or treaty violations can be determined, but an attack on a computer network can be almost impossible to attribute. The use of hijacked "zombie" computers means the geographic origin of an attack may be unclear, as will be the identity of the perpetrator. "Since no one is going to get caught," says Baker, "to say [a cyber attack] is a violation of the law of war is simply to make the law of war irrelevant."

When the Russian cyber arms limitation resolution came up before the General Assembly in December 2008, it passed 178–1, with only the United States opposed. Around the world, there was deep suspicion of U.S. cyber designs. The Internet was a Pentagon invention, and some foreign government officials thought the United States was secretly using it to advance its geopolitical interests and destroy its enemies.

The U.S. Air Force inadvertently boosted these beliefs when it sought to recruit "cyber warriors" with ads trumpeting a new mission to "dominate" cyberspace. The commander of the Air Force's "Network Operations Center" was quoted in 2008 as saying his unit was "a keystroke away from executing an action that can have a dramatic effect [on adversaries]. And it doesn't necessarily have to be a physical effect... It could be information operations. Using their systems to convey a message or a thought that results in actions... that are to our best advantage." To many people

around the world, it seemed the United States really did see the Internet as a tool for global domination. James Lewis, a cybersecurity expert at the Center for Strategic and International Studies who has consulted at the United Nations Institute for Disarmament Research, recalls one foreign diplomat telling him, in all seriousness, that Twitter was "an American plot to destabilize foreign governments."

Resentment over the perceived U.S. control of the Internet surfaced at the World Summit on the Information Society, which was convened in Geneva and Tunis in 2003 and 2005. Governments from around the world joined in demanding that the United States relinquish its management of the Internet. Their target was the Internet Corporation for Assigned Names and Numbers (ICANN), a nonprofit organization chartered by the U.S. government. The group's role—maintaining the global Internet address book—was fairly technical, but it was the only body that had actual Internet governance powers. European governments, along with those from developing nations, wanted ICANN's responsibilities transferred to a new international body.

In a direct challenge to the United States, the participating states resolved that "all governments should have an equal role and responsibility for international Internet governance," and they affirmed that states had a "sovereign right" to enact their own Internet policies. The International Telecommunications Union, an organization where each member country had an equal voice, was given the responsibility of "facilitating" the governance changes. The ITU chief of strategy, Alexander Ntoko, laid out the ITU reform plan in an April 2010 interview with the Intellectual Property Watch news service. "For example, you are the minister of defense," Ntoko said. "What influence do you have in the policies that govern the Internet so they can take into account your national needs? I think it is a lot about sovereignty." So much for the original vision of the Internet as an unbordered space. The push for national sovereignty raised the prospect of different versions of the Internet, tailored and filtered in accordance with the priorities of each government. The battle to control the Internet was in full swing.

Under President Obama, the U.S. government took a new approach in the cyber discussions at the U.N. In previous years, American diplomats

focused mainly on the need for countries to improve their own cybersecurity and cooperate in the fight against cyber crime; beginning in 2009, however, the White House began to engage on the cyber war issue, recognizing that other governments wanted to find ways to limit state-on-state cyber conflict.

The 2008 Russian "information security" resolution called for the establishment of a "group of governmental experts" that would study cyber threats and "cooperative measures to address them." The United States, Russia, China, and all other leading cyber powers were represented. At the first meeting, the Russian representative spoke passionately about the damage countries could do to each other in an all-out cyber war. In response, the U.S. delegation declared that existing international law could theoretically be applied to cyber conflict and that the United States would support the establishment of "norms of behavior" that like-minded states could agree to follow in cyberspace. One example would be a commitment from states not to allow their territories to be used as launching pads for cyber attacks. U.S. officials also took the position that civilians should not be the object of cyber attacks and that disproportionate or indiscriminate cyber attacks should be avoided. Before any cyber attack was carried out, the risk of collateral damage would have to be assessed, just as it would be in advance of a physical attack. Never had the United States taken such clear positions on the legality of cyber war.

The first public hint of the revised U.S. position came from Army General Keith Alexander, director of the National Security Agency and the Obama administration's choice to lead the military's new Cyber Command. When asked at a news conference in June 2010 about the Russian proposal, Alexander said, "I do think we have to establish the rules, and what Russia has put forward is, perhaps, the starting point for international debate."

Alexander's comment got immediate attention. Stewart Baker raised the question in his blog of whether the United States was "going wobbly" on the Russian initiative. Jack Goldsmith, the Harvard law professor who once ran the Office of Legal Counsel under President George W. Bush, thinks the United States made a concession to Russia by changing the subject from cyber crime to cyber war. "All nations are interested in preventing other countries from doing what they're good at and in being prevented themselves from doing what they're not good at," Goldsmith told me. "Russia is the source of much of the crime in the cyber world. On that theory, the Russians want a cyber war treaty but not a crime treaty,

because they think they have a disadvantage in cyber war."

Other former Bush administration officials were more positive. Retired Air Force General Michael Hayden, the former CIA director, praised the initiative, saying that while he did not support formal cyber treaty commitments ("because they're totally unverifiable"), he approved the establishment of "international norms among responsible states and sanctions for the violation of those norms." Russian diplomats, experienced in international negotiations, said they could endorse the U.S. contribution to the governmental experts group. For the Chinese representatives, however, the United States was going too far. While they liked the idea of a cyber accord designed around the idea of "information security," they balked at the application of international law to cyber conflict. The U.S. contribution on that subject was dropped from the report.

American officials were nonetheless pleased to find some common ground with the Russian members. The report did refer to the value of "international norms pertaining to State use of [information communication technologies]" and suggested that "additional norms could be developed over time." Whether the achievement was enough to forestall the other ongoing attempts to reshape the Internet in the name of international peace, however, was doubtful.

Even as the United States and other U.N. nations were discussing ways to minimize the chances of cyber war, the ITU leadership was moving ahead with plans to demand changes in the governance of the Internet. In April 2010, ITU Secretary General Hamadoun Touré proposed that his organization be given the responsibility for developing a "system wide approach" to "address the policy issues posed by the growing challenges to cyber security and cyber peace." Such a role would put the ITU at the forefront of Internet governance. In the previous months, the United States had agreed to loosen its ties to the Internet Corporation for Assigned Names and Numbers, but many of the states represented in the ITU were still pushing for a transfer of ICANN's powers to another international body, and the ITU was a strong candidate.

In September, I asked the ITU's Alexander Ntoko whether it was likely the ICANN role would be discussed at the plenipotentiary conference in Guadalajara.

"*Likely?*" he chortled, amused by what struck him as an understatement. "It will be a very hot topic!"

No ICANN official would be heard at the conference, however. Rod Beckstrom, ICANN's president and CEO, wrote Touré in July to ask whether ICANN might be given "observer status," but Touré tersely rejected the request, saying the ITU charter did not recognize ICANN as an official entity.

To the dismay of those who still believed in an Internet free of government interference, the most powerful countries in the developing world—including Brazil and India—were coalescing in support of an international accord to tighten Internet controls. Touré was portraying the move as a step toward a cyber arms limitation pact, and he was serving Russian and Chinese interests in the process. The Internet may have been an American invention, but the United States had lost the ability to determine its character.

"How could it be any other way?" says Jack Goldsmith, who wrote a book called *Who Controls the Internet?* "This is a hugely important tool, and powerful nations are going to wield it and shape it in ways that reflect their interests."

It has taken a few years for countries to adjust to this new arena of opportunity and conflict, but neither warfighting nor peacemaking will be the same again.