CYBER WAR v. CYBER STABILITY

By Jody R. Westby, Esq.[1]

Paper for the
42nd Session
World Federation of Scientists
International Seminars on Planetary Emergencies
August 19-22, 2009
Erice, Italy

Cyber war has become the drumbeat of the day. Nation states are developing national strategies, standing up offensive and defensive cyber war capabilities, and, actually conducting cyber reconnaissance missions and engaging in cyber attacks -- with alarming frequency. What is blatantly apparent is that far more financial resources and intellectual capital are being spent on figuring out how to conduct cyber warfare than are being spent on figuring out how to prevent it. The lack of international dialogue and activity with respect to the containment of cyber warfare is stunning. As Winston Churchill famously noted, "It is better to jaw-jaw than to war-war." *It is time for governments to begin discussions aimed at assuring an agreed upon level of geo-cyber stability through mutual cooperation and international law.*

"Geo-cyber stability" is defined by the author as the ability of *all* countries to utilize the Internet for both national security purposes and economic, political, and social benefit while refraining from activities that could cause unnecessary suffering and destruction. With 1.6 billion online users in 266 countries and territories connected to the Internet, cyber attacks have become so commonplace and the capabilities to exploit the full range of information and communication technologies (ICTs) so great, that government systems, military networks, and business operations are in a continual state of risk.

Recent Attacks That Undermined Geo-cyber Stability

Although cyber attacks have been commonplace for the past decade, the frequency and sophistication of the attacks over the past two years have caused a shift in the stability of the Internet and created uncertainty whether nations will be able to secure and control their infrastructure, systems, and information. The 2007 attacks on government and private sector networks in Estonia were the watershed event that served as a government wake-up call. The attacks quickly escalated, seriously impacting government Web sites and systems and shutting down newspaper and financial networks. The attacks demonstrated the rapid pace at which a cyber attack can become to a national security issue, involve other nation states, and raise the issue of collective defense.

[1] Jody R. Westby is CEO of Global Cyber Risk LLC, located in Washington, DC and serves as Adjunct Distinguished Fellow to Carnegie Mellon CyLab. She also chairs the American Bar Association's Privacy & Computer Crime Committee and is co-chair of the World Federation of Scientists' Permanent Monitoring Panel on Information Security.

Even though Estonia is one of the most "wired" countries in the world, the attacks were also significant because Estonia quickly had to call for help in tracking and blocking suspicious Internet addresses and traffic. Before the attacks ended, computer security experts from the U.S., Israel, the EU, and NATO were assisting Estonia – and learning its lessons. The Estonian government was forced to close large parts of the country's network to outside traffic to gain control of the situation. Estonia blamed the attacks on Russia and claimed that it had tracked some communications to an Internet address belonging to a Kremlin official. Notably, Russia refused to cooperate in the investigation of the attacks even though it strongly denied any responsibility for them.

The attacks highlighted the global nature of cybercrime and the difficulty of tracking and tracing cyber activities. Traffic involved in the attacks was traced to countries as diverse as the U.S., China, Vietnam, Egypt, and Peru. The Estonian attacks also may have represented a situation in which rogue actors, such as botherders or organized cyber criminals, were aligned with a nation state in conducting and concealing the attacks, though this has not been proven. (Botherders are persons who control thousands to millions of computers (botnet) on which they have surreptitiously planted software that can be activated to cause the infected computers to take certain actions, such as sending repeated communications to a network as part of a denial of service attack.)

A few months after the Estonia attacks, U.S. Pentagon computer networks were allegedly hacked by the Chinese military in what has been called "the most successful cyber attack on the U.S. defense department,"[2] shutting down parts of the Pentagon's systems for more than a week. Chinese hackers have also been blamed for attacks that compromised German government systems and cyber espionage incidents against the United Kingdom's (UK) government systems. The Director-General of the UK's counter-intelligence and security agency, MI5, posted a confidential letter to 300 CEOs and security officers on the Web site of the Centre for the Protection of National Infrastructure, warning them that their infrastructure was being targeted by "Chinese state organizations" and that the attacks were designed to defeat security best practices. Like the Estonian events, these attacks raised profound legal questions with respect to nation state use of cyber mercenaries to conduct intelligence or military activities.

The 2008 attacks on Georgian systems during the Russia-Georgia conflict over South Ossetia were a more obvious example of cyber warfare that demonstrated the degree to which governments are dependent upon computers and communications networks – especially during crisis management. A sequence of distributed denial of service (DDOS) attacks against Georgian government Web sites essentially shut down government communications. The Georgian government quickly obtained assistance from other countries – and companies. Estonia sent cyber security experts to Georgia and took over the hosting of the Georgian Ministry of Foreign Affairs Web site. The Polish government made space on its Web site for Georgian updates on its conflict with Russia, and U.S. companies, such as Google and Tulip Systems, helped the Georgian government move some of its Web content to the U.S. where its would be protected.

[2] Demetri Sevastopulo, "China 'hacked' into Pentagon defence system," *Financial Times,* Sept. 6, 2007 at 1.

While the Estonia attacks raised questions whether cyber attacks could trigger NATO's Article V protections of collective defense, the Georgian attacks raised issues regarding other aspects of international law. Stephen Korns and Joshua Kastenberg have analyzed the assistance provided to Georgia and pondered whether Georgia violated the United States' right of neutrality under the Hague Convention when it took the "unorthodox step of seeking cyber refuge" in the U.S. without first seeking the permission of the U.S. government. Tulip Systems's CEO, a Georgian who happened to be visiting in Georgia at the time of the attacks, called the Georgian government and volunteered Tulip's services. Korns and Kastenberg note that:

> During a cyber conflict, the unregulated actions of third-party actors have the potential of unintentionally impacting US cyber policy, including US cyber neutrality. There is little, if any, modern legal precedent.

The Estonia and Georgia cyber attacks serve as excellent examples of the havoc caused by cyber attacks and the uncertainty surrounding the legal frameworks that govern actions taken during such events. Theory falls way to reality in the chaos of such crises: neither NATO nor the countries that came to the assistance of Estonia had clear legal authority to engage in defensive measures to aid Estonia. *The Estonian and Georgian attacks highlight the need to revise the doctrines and laws that traditionally support diplomatic, policy, and military decisions in order to address cyber threats that often link national and economic security.*

More recent cyber attacks highlight the interconnected nature of cyber vulnerabilities and accentuate the need for an agreed upon level of geo-cyber stability. Researchers at the Munk Center for International Studies at the University of Toronto conducted a 10-month investigation into allegations of a Chinese computer network exploitation against Tibetans. The Information Warfare Monitor's March 2009 report on this investigation, *Tracking GhostNet*, indicated that the researchers uncovered a network of 1,295 infected computers in 103 countries that were controlled from commercial Internet accounts in China. According to the report, the GhostNet system commanded computers from ministries, embassies, news organizations, and NATO across Europe and Asia to download malware that enabled the attackers to "gain complete, *real-time* control" that included searching and downloading files and operating devices attached to the computers, such as microphones and Web cameras.

In early 2009, cyber researchers from 300 organizations and 110 countries joined together to fight the Conficker worm, which has infected at least five million systems in 211 countries. Conficker is contained for the moment, but not eradicated. The threat looms that those behind the worm could break through and take control of these systems. SRI International reported that Conficker first appeared in September 2008, and Chinese hackers were the first to market it. According to Rick Wesson, CEO of Support Intelligence and one of the researchers deeply involved in this effort, the sophistication of this worm is unprecedented and targets the infrastructure of the Internet. In part, Conficker has relied upon the inability of infected parties to collaborate – one of the gravest weaknesses in the international legal framework, yet one of the easiest to fix through international agreement.

As recent as July 2009, at least 35 government and commercial Web sites in South Korea and the U.S., including the Nasdaq and New York stock exchange, suffered denial of service attacks.

South Korea intelligence officials have unofficially blamed North Korea. Former U.S. officials have publicly named North Korea among nations perfecting cyber warfare capabilities.

In 1996, U.S. Government officials estimated that more than 120 countries either had or were developing computer attack capabilities that could seriously impact the nation's ability to deploy and sustain military operations. Countries certainly need to be able to protect their infrastructure, systems, and information from intrusion, attack, espionage, sabotage, unauthorized access or disclosure, or other forms of negative or criminal activity that could undermine national and economic security. They also, however, need some certainty regarding everyday operations and a legal framework upon which to rely in making decisions regarding national and economic security and the safety of their people. This is lacking in the cyber realm.

The political and economic shifts caused by the Internet and globalization have introduced considerations that impact traditional approaches to national security based on geo-political interests, spheres of influence, and correlation of forces. Foreign policy is far more complex in an interconnected world where cyberspace knows no borders, packets hop from country to country, and laws governing collective assistance and armed conflict were intended for traditional warfare, not cyber conflict. Although geo-political considerations still must be afforded great weight, threats to critical infrastructure must be evaluated in a broader policy paradigm that is based on maintaining global cyber stability.

Today, all countries need the certainty of a minimum level of cyber stability that is assured through international agreement. At its core, this minimum level of cyber stability means that a country's critical infrastructure shall not be disrupted in a manner inconsistent with the laws of armed conflict and other applicable treaties and conventions, such as the Hague Convention, which requires nations at war to respect the neutrality of other nations, and the Geneva Convention.

Legal and Policy Issues

The laws of armed conflict regulate the conduct of armed hostilities and are intended to prevent unnecessary suffering and destruction. Under the laws of armed conflict, combat forces can engage in only those actions necessary to achieve legitimate military objectives (principle of necessity), and they must distinguish between lawful and unlawful targets, such as civilians, civilian property, and the wounded and sick (principle of distinction). The amount of force cannot exceed that needed to accomplish military objectives (principle of proportionality). Lawful combatants are those authorized by the government to engage in military actions, and they must bear distinctive emblems and be recognizable at a distance. Unlawful combatants are those who participate in hostilities without authorization by government authority or under international law.

In a cyber context, the first obvious issue is: what constitutes an act of cyber warfare? Other issues concern the attack of communication systems and other critical infrastructures owned by the private sector that support civilian life, including hospitals and treatment for the sick, wounded, elderly, and very young. Should these and the systems of targets protected by the Geneva Convention be off limits? Are attacks on these systems really necessary to achieve military objectives? Is the damage to the networks proportional to the military objective? When an attack occurs, no one knows who is attacking until it can be tracked and attribution can be determined. Legitimate cyber soldiers are indistinguishable from script kiddies or any rogue actor on the Internet. How does one determine whether attackers are military combatants? What international cooperation is required? Likewise, how is it to be known if third parties are acting at the behest of a nation state? They certainly do not have distinctive emblems or are recognizable from a distance. Do cyber soldiers and engaged third parties need to wear cyber uniforms or have recognizable characteristics? What is excessive force in cyberspace?

These and numerous other legal and policy questions arise in the context of cyber warfare. The two principal legal instruments that govern nation state action in a conflict situation are the NATO Treaty and the UN Charter. Each document is more than 50 years old and their provisions do not accommodate cyber scenarios. They both use similar language and are equally ambiguous regarding cyber attacks. The NATO Treaty's use of terms such as "armed attack," "territorial integrity and political independence," and "territory, forces, vessels, and aircraft." The terms self-help, mutual assistance, and collective assistance are used only in the context of an "armed attack." Estonia's defense minister, Jaak Aaviksoo, pinpointed the gaps in the NATO treaty with respect to cyber attacks by stating, "Not a single NATO defense minister would define a cyber-attack as a clear military action at present."

Article 12 of the NATO Treaty allows for consultation of NATO members for the purpose of reviewing the Treaty with respect to "factors then affecting peace and security." Thus, this Article could be used as the mechanism by which cyber attacks, collective defense, and geo-cyber security are considered by NATO nations.

The UN Charter serves as the foundation in international law for state conduct, including armed conflict. The language in the UN Charter is closely aligned with that in the NATO Treaty, using terms such as "territorial integrity and political independence," "the use of armed force," "action by air, sea, or land forces," and "armed attack." The self-defense provisions confuse more than clarify. Article 51 states that nothing shall block a nation or group of nations from engaging in collective self-defense if an armed attack occurs, raising the question of whether a cyber attack could be deemed to be an "armed attack." Even if the attack came from a branch of the armed forces, Article 41 cuts against that interpretation because it specifically lists actions that are deemed *not to be* armed force and may be taken to enforce Security Council decisions. The allowed actions specifically include the complete or partial interruption of communications, which could apply to cyber attack scenarios.

Quite simply, the UN Charter and NATO Treaty do not accommodate the electronic capabilities of the 21st century. The need to update these legal instruments to govern the actions of nation states with respect to cyber warfare and attack capabilities has never been more urgent. The rule of law is already in a precarious state due to the disruptions caused by terrorist activities. The ominous threat of cyber attacks by nation states and rogue actors has become a reality, and this issue can no longer be ignored by countries that find it more desirable to war-war than to jaw-jaw. Governments, the private sector, and multinational organizations must begin an international dialogue in this area to accommodate new military capabilities, collective action, and geo-cyber considerations.

If left unattended, by 2015 cyber *instability* will pose a significant threat to the national and economic security interests of all countries. Although some action has been taken by NATO, it falls woefully short of assuring any sort of geo-cyber stability. Following Estonia, NATO adopted a Cyber Defence Policy and created a Cyber Defence Management Authority to coordinate cyber defense among NATO allies. NATO's Cyber Defence Policy does not address whether a cyber attack can trigger collective defense under Article V. Response centers are necessary, but they are soft options. The steps taken by NATO make an important contribution, but they do not help define what level of cyber stability is sacrosanct and how cyber actions fit within the NATO framework.

Where to Begin

Countries need to begin the dialogue on global cyber stability by addressing international cooperation. Such cooperation is almost always needed in tracking and tracing cyber communications simply due to the interconnected nature of the Internet and the manner in which the Internet Protocol breaks a communication into packets and routes them across many networks – and countries – before reassembling them at their destination point. Assistance from other nation states is also needed in *defending* against cyber attacks.

The Council of Europe Convention on Cybercrime, which contains excellent provisions regarding mutual cooperation and assistance, was originally believed to be the best vehicle for reaching such agreement. However, it only has been signed by 46 countries and ratified by 26 since it opened for signature in 2001. Considering that over 200 countries are connected to the Internet, the CoE Convention hardly appears to be the answer.

The UN clearly needs to take the lead in working toward an international agreement on cooperation and containment of cyber conflict. Although the U.S. invented the Internet, it is unlikely that it will step up to take a leading role at the UN in any such effort. The U.S. has openly criticized the ITU for addressing cybercrime in its Global Cybersecurity Agenda and has refused to support the *ITU Toolkit for Cybercrime Legislation*, which contains sample language for cybercrime laws and provisions for mutual cooperation and assistance (consistent with the CoE Convention). U.S. opposition to UN activity in the cyber realm has gone on for over a decade, with U.S. delegates continuing to push the CoE Convention and arguing that defensive action and cybercrime laws are the solution.

Ironically, Russia – one of the most active countries engaging in cyber warfare – has shown the greatest leadership in this area. Since 1998, Russia has introduced an annual UN resolution concerning "Developments in the field of information and telecommunications in the context of international security" calling for multilateral consideration of threats emerging in the field of cyber security, the definition of basic notions related to the unauthorized interference of information and telecommunication systems, and consideration of international principles to help combat cybercrime and terrorism. The 1999 resolution included the military potential of ICTs. These resolutions have regularly been adopted by the General Assembly, and the U.S. has regularly voted against them. Russia's 2008 resolution was adopted by both the UN's First Committee and the General Assembly – over the sole objection of the United States.

Conclusion

The international community must come together and realize that the enormous benefits of the Internet are at risk if it is used as an instrument of harm outside the rule of law. Governments have an obligation to help protect the Internet and systems that support their economies, enrich the lives of their citizens, and support government and military operations. They also have an obligation to assist in tracking and tracing cyber activities. A legal framework applicable to cyber conflict that assures a minimum level of geo-cyber stability must be developed, lest the Wild Wild Web become the 21st century tool of destruction and impede on the rule of law regarding armed conflict, human rights, and friendly relations among nation states.