THE TRILATERAL COMMISSION
2011 WASHINGTON MEETING

SESSION ON CYBERSECURITY
Saturday, April 9, 2011

The International Context for Cybersecurity

James A. Lewis
Center for Strategic and International Studies

In the 1970s, a group of scientists and engineers developed a new technology that let computers connect reliably with each other across great distances. The technology, which became known as the internet, forms the basis of cyberspace by creating easy "connectivity" among networks and computers. Unfortunately, this initial emphasis on assured connectivity overlooked security. When the internet was composed of a few dozen research universities and military facilities, this oversight was not a problem. None of the designers of the new protocol expected it to become a globe-spanning network that connects billions of people and serves as the critical platform for businesses and governments.

The first computers were large expensive machines, splendidly isolated in glass-walled, air-conditioned rooms. This isolation was their protection from attack. Once the internet connected them to each other, they were no longer safe. Even high school students could break in – a famous incident in 1998 involved a penetration of Department of Defense (DOD) computers that DOD first ascribed to China, but found to be the work of three California high school students looking for notoriety among their peers. Skilled opponents quickly exploited network vulnerabilities, creating a "Golden Age" for espionage that continues to this day.

Policy decisions on the commercialization of the internet reinforced vulnerability. To encourage the spread of the new technology, the U.S. decided to minimize government's role in guiding it. This reflected the experience with 1980s telecommunications deregulation, which brought better performance at lower cost. It also reflected the belief, popular in the 1990s, that globalization would make borders disappear and national governments less effective. This belief turned out to be wrong. States are still the most powerful actor in the international arena, but cybersecurity policies are only now beginning to adjust to this. Cyberspace relied on market forces, voluntary action, and the informal efforts of a community of internet users to govern and secure itself. Unsurprisingly, as the internet has changed from a gadget to an essential global infrastructure, this communal, voluntary approach has failed to provide adequate security.

This puts us where we are today. Neither the internet nor the devices attached to it are secure. Major corporations, financial firms, and government agencies have all been victims of cybercrime and cyber espionage. Publicly reported events sin just the last few months give an idea of the extent of malicious activity in cyberspace. In January 2010, Google and at least thirty other U.S. Fortune 500 companies were hacked, allegedly from China. Morgan Stanley experienced a "very sensitive" break-in to its network, according to leaked e-mails. Major

American oil companies report the loss of exploration data worth millions of dollars. Since the 1990s, there have been dozens of incidents like these.

No country is immune. NATO and the EU warned that the risk of successful cyber attacks against their networks have increased significantly. The "Ghostnet" investigation found that government networks in 130 countries had been hacked in a search for information on Tibetan human rights activists. In December 2008, attackers were even able to penetrate the U.S. Central Command's classified networks. British Foreign Minister William Hague reported that attacks on the Foreign Office, an UK defence contractor, and other British interests succeeded by pretending to come from the White House. Last month, hackers penetrated French government computers and stole sensitive information on upcoming G-20 meetings. While China is a leading source of cyber-espionage, it is also a victim, and penetrations of Chinese government website increased by two thirds in the last two years. The digital world is a truly Hobbesian environment.

An incident that attracted considerable attention in 2010 involved "Stuxnet," a complex piece of malicious software that produced significant physical damage to the Iranian nuclear program. Stuxnet was hailed, loudly and inaccurately, as the dawn of cyber war. A single act of sabotage is not a war, and in fact, the U.S., UK, Russia, China and Israel have long had the ability to launch cyber attacks. Another thirty nations are building their own cyber attack capabilities. Eventually, every military will include cyber attack in its portfolio, just as every military eventually adopted airplanes or armored vehicles.

Even with this build-up, cyberwar is unlikely. No nation will frivolously start cyberwar – it faces the same risks as any other military action. Currently, only a few advanced powers have the ability to inflict serious destruction through cyber attack. These powers treat cyber attack as they would any other weapon – something to be used only in a larger conflict. While many nations are acquiring cyber attack capabilities, they are unlikely to launch frivolous cyber attacks.

Similarly, cyber terrorism is not a risk, at least for the time being. Terrorist groups and unstable nations do not yet have the capability to launch damaging cyber attacks. We know, however, that Iran and North Korea are trying to acquire cyber attack capabilities and groups like Al Qaida in the Arabian Peninsula or Pakistan's Lashkar e Taiba may eventually obtain cyber attack capabilities. When these groups or nations acquire the capability to launch a cyber attack, they will not wait long to do so, and the West is in no position to defend itself.

To date, we have seen perhaps only two incidents that would qualify as true cyber attacks – Stuxnet and an alleged Israeli attack on Syria. In contrast, espionage and crime occur every day. The perpetrators are dangerous nation-state actors in cyberspace bear the unwieldy acronym APT, "advanced persistent threat." We have gone from high school students and "social hackers," who penetrated systems to gain prestige, to well-organized professional criminals and intelligence agencies. Amateurs cannot defend themselves against these professional opponents – it would be like sending the company softball team against the New York Yankees.

The most serious threats come from Russia and China (and the Chinese would say that their most

serious threat comes from U.S. military and intelligence). Russia and China share an approach to malicious cyber activities. Government agencies engage in cyber espionage, but they also use irregular forces drawn from advanced cyber criminals and hackers, often trained and funded by government agencies.

Russian proxies were responsible for the cyber attacks launched against Estonia and Georgia at the behest of the Russian government. While Russia denies that the attacks were officially sanctioned, the attacks on Georgia were coordinated with Russian military actions and carried out by the same computers responsible for the attacks on Estonia. However, most malicious Russian cyber activities focus on financial crime, siphoning millions of dollars from western banks. Cybercriminals are incorporated into the larger Russian criminal enterprise, with its intricate and directive interconnections between organized crime and the Russian government.

China's situation is more complex, as it combines a very aggressive government effort with extensive hacking by companies and individuals. Chinese cyber espionage has two goals. The first is to gain asymmetric advantage over the U.S. military. The second, and more important, is to acquire technology and business information. The larger problem of intellectual property protection in China shapes that nation's activities in cyberspace. Illicit acquisition of technology from foreign companies to help "catch up" with the West has been part of China's industrial strategy since the decision to open its economy in the 1980s. That strategy has been extended into cyberspace. China does not have the same degree of control over its hacker community as does Russia. Chinese citizens, companies, and government agencies acting on their own, steal intellectual property from Western firms and from each other. Chinese officials realize that weak IP protection damages their own economy, and they fear that Chinese hackers may turn on the Party.

We can best describe the response by western governments, particularly the United States, as feeble. There is very little risk for malicious activity in cyberspace if you live in one country and commit crimes in another. Even rebukes are rare. Cybercriminals exploit the transborder nature of the internet, committing crimes in one jurisdiction while residing in another. Weak cybersecurity is the result of indecision over goals and responses in democratic societies. This period of indecision may be ending, but there are still significant obstacles to developing an adequate response.

We can now identify measures that could improve cybersecurity. Some require multilateral cooperation. Others are national measures. The common elements are an expanded role for government and the creation of rules and institutions appropriate for a global infrastructure. But implementing these measures will require addressing four sets of interconnected issues: military security, law enforcement, trade, and the political effects of the internet.

A more stable military environment in cyberspace requires common understandings among potential opponents of how laws of war apply, where restraint in the use of the new capability is possible, or where redlines or thresholds for escalation might exist. It is routine to make comparison of cyberwar and nuclear war. This analogy is misleading. Unlike nuclear weapons, the destructive capacity of cyber attack is far smaller and the tactical use of these techniques is inevitable. Strategic arms control is an insufficient precedent for negotiations. A treaty,

particularly an arms control treaty, makes little sense. What is a weapon in cyberspace? A child with some programming knowledge and a laptop can build and launch an attack in a few weeks. Verification is impossible. A treaty based on technological constraints would be meaningless.

Deterrence is of limited value. Nations can deter attack by other nations, including cyber attack, by threatening military retaliation, but they cannot deter espionage or crime. These actions do not rise to the level of the use of force and do not justify a military response. Additionally, deterrence will not work well against new classes of opponents, including politically motivated non-state actors or against less responsible states. Since deterrence will provide incomplete protection, adequate cyber defense raises two issues. The first is how to protect critical infrastructures. The second is how best to use military capabilities to influence potential opponents.

A "cybersecurity" treaty makes no sense. An alternate approach could be modeled on nonproliferation, where nations developed multilateral norms that define responsible behavior. The simplest norm would extend existing law and practice to say that a state is responsible for the behavior of those on its territory – this would constrain the use of proxies and "patriotic hackers."

The most important national action would be to increase protection for critical infrastructures – telecommunications, the electrical grid, the financial system and a few other key economic sectors. These are the most likely targets for future cyber attacks and they are vulnerable. Companies are reluctant to spend on cybersecurity – there is little return on investment in securing networks. The emerging consensus is that the only solution is government mandates that would require companies to comply with a basic set of measures to would make their networks harder to damage or disrupt.

There is immense hostility to regulations, for reasons both good and bad. Too much regulation is clearly not in the national interest. At the same time, few would recommend abolishing the Federal Aviation Authority and rely solely on airlines to do what is needed to ensure aircraft safety. Some companies will always do the right thing, some will usually do the right thing, and some will cut corners. Critical infrastructure protection will require some minimal level of regulation, but the U.S. may be at a disadvantage in this compared to other nations that do not face the ideological hurdles to government playing a more directive role in the economy.

One reason the U.S. has made so little progress, despite a Presidential announcement in May 2009 that cybersecurity would be a priority, is because of the fear that better cybersecurity means less innovation. These concerns reflect a fundamental misunderstanding of how innovation actually works. Access to information technology is one factor that contributes to innovation, but it is not the most important. An educated workforce, appropriate fiscal and tax policies that create the financial resources needed for investment, balanced protection of intellectual property rights, and minimal regulatory impediments (at all levels of government) are key, along with adequate infrastructures, and openness to trade. Better cybersecurity is not an obstacle, but the combination of an ideological desire for a smaller government role and little regulation combined with fuzzy notions about protecting innovation have hampered the building of cyber defenses.

Critical infrastructure protection will also require redefining the role of large telecommunications companies and internet service providers. As we move into a "cloud computing" environment, where mobile devices like the iPad replace desktop computers, service providers will be better placed to manage cybersecurity for their customers. Having service providers intervene when their customers' computers are infected is startlingly effective. Germany, Australia, Turkey and other countries are adopting this approach. The U.S. lags in this because of its litigious regulatory system.

Critical infrastructures can also be defended by intelligence agencies in what is known as "active defense." Active defense would let these agencies work with major telecommunications companies to detect incoming attacks from foreign sources and stop them. Active defense is not perfect, but it works and nations are deploying it. The U.S. lags here as well, because of concern over the political risk related to an expanded role for military or intelligence agencies on the internet.

Cybersecurity would be significantly improved if "havens' for cyber criminals were eliminated. These havens allow criminals to connect via the internet to commit transborder crimes. Improved law enforcement in cyberspace requires international agreement to prosecute cybercriminals. This is currently lacking, as it raises issues of sovereignty, extraterritoriality and the linkage of cybercrime and state-sponsored espionage. There is an international agreement – the Council of Europe Cybercrime Convention – but Russia and China are not signatories and other important nations, such as India and Brazil, say they will not sign because they were not involved in its drafting. A few weak alternatives to the Council of Europe Convention have been floated – the UN's International Telephony Union has a "toolkit" for cybercrime that some call "Council of Europe Lite," and Russia and China have included cybercrime cooperation as part of their Shanghai Cooperation Organization.

Cybersecurity is a trade issue, particularly in regard to protection of intellectual property. Nations have been reluctant, however, to push for stronger enforcement of World Trade Organization agreements on intellectual property protection. In the case of Google, for example, an individual at a Chinese institution has been identified as the perpetrator – no action has been taken against him or against China for sheltering him. An overly legalistic approach by the U.S. and others has created an opportunity for unfair trade practices that nations like china have been quick to exploit.

Supply chain security for information technology products is another trade issue. If you have a laptop computer, it incorporates hardware and software from a dozen countries. Many nations, including both the U.S. and China, are worried that other nations may succumb to the temptation to ask their companies to "corrupt" the components they sell. While it is easy to overstate the problem, countries are trying to control supply chain risk by developing individual inspection regimes that could become non-tariff barriers to trade. The best solution to supply chain risk would be to come to some international agreement on how to ensure that hardware and software are safe, but reaching agreement on supply chain security faces both technical and political difficulties.

Cybersecurity is part of a larger political problem. The internet has changed politics, creating virtual communities and organizations that challenge existing governments. The internet unleashes a flood of information that reshapes opinion. The result is powerful new political forces that challenge all governments. It is easier for democratic governments to adjust, as they are able to absorb and manage dissent. Authoritarian regimes lack this ability, and see the internet as creating an almost existential threat by undermining their control of information and by allowing dissidents to communicate and organize. Russia, China and others say that the internet is an "information weapon" that the U.S. uses to destabilize their regimes. Authoritarian countries invest heavily in technologies that control their citizens' ability to use the internet for political purposes – this is their priority for "cybersecurity."

This creates a negotiating environment where the U.S. seeks concessions on cybersecurity that would weaken potential opponents without offering compromises that address their political concerns. The U.S. further complicates the prospects for cooperation with announcements that it will "dominate" cyberspace and by investing (through the State Department) in technologies designed to undermine authoritarian regimes' control of the internet.

We may ultimately choose not to compromise on political issues, but this limits the prospects for better cybersecurity. Options are sparse: the U.S. could pursue a minimalist approach to cooperation; it could demand unilateral concessions from other cyber powers, which would probably lead to stalemate; or it could work only with like-minded nations to develop norms and institutions and then encourage others to join it. This approach has succeeded, albeit over a period of years, with issues as disparate as missile technology and money laundering.

The political challenge of cybersecurity comes at time when western influence on global institutions is waning. The U.S. could once dictate the course of the internet, but this is no longer the case. Since 1945, the U.S. and its partners have created rules and institutions for global activities in finance, telecommunications, trade, and air travel. The same now needs to be done for cyberspace, but the scope of a new approach is still ill defined and in dispute. There are contending visions for how to make cyberspace more secure. Unilateral domestic measures for cyber defense are inadequate. Absent international agreement, cyberspace will remain insecure. Progress is not impossible, but these are complex issues and we are unlikely to see serious improvement anytime soon.

James A. Lewis is director and senior fellow, Technology and Public Policy Program, at the Center for Strategic and International Studies, Washington, DC.