Cyber War and Cyber Defense: We Depend on the Kindness of Strangers

James A. Lewis
Director and Senior Fellow
Technology and Public Policy Program
Center for Strategic and International Studies

No one expected the Internet, originally a set of new communications protocols designed to make telecommunications more efficient and survivable, to reshape business, politics and military conflict. The Clinton administration commercialized the Internet in the early 1990s. There was an immensely rapid uptake by businesses and consumers, followed shortly thereafter by a strong interest among militaries and intelligence agencies as to how to exploit the new technology.

While a 1995 cover story for *Time Magazine* was entitled "Onward Cyber Warriors," the desire to use the Internet as a weapon outpaced the ability of the new technology to cause damage. We did not depend as much on networks in 1995, and we were not as connected globally. This has changed markedly in the last five years.

Businesses found that using the new Internet protocols let them be more efficient and lower costs. Companies could replace critical infrastructure control systems, which once ran over dedicated telephone lines and used proprietary programs, with commercially available software that ran over the Internet. There were large savings, but also a large increase in risk. It is difficult to break into a dedicated telephone line and decipher proprietary programs. It is much simpler, as we have discovered, to "hack" into the Internet.

The developers of the Internet did not pay attention to security. It was a closed military project used by a small community of scientists, engineers, and military officials. Some of the Internet pioneers also had strong views on the role of government and its relations to innovation, and they sought to build a system that was open, encouraged easy connectivity, was non-hierarchical in its makeup, and did not use a strong, organized system of governance based on nation-states. The intent would be a self-organizing community where innovation would flourish.

This vision has been hugely successful in creating a new global infrastructure to which hundreds of millions of people and devices connect and, increasingly, rely upon. But the lack of emphasis on security also created huge new vulnerabilities. The technology of the Internet was not built with network security in mind. Computers were once large, expensive, machines, unconnected to anything else. Secure the building that housed them, and they were secure. Then came the personal computer, small, cheap, but also not connected to anything else. Secure the building and the computer was secure. In both cases, an attacker needed physical access.

The Internet changed that. You no longer need physical access to share data, communicate, or attack. The global spread of high-speed fiber optic networks increased both benefit and risk. These networks use light pulses to communicate. At the speed of light, Beijing is as close as the house across the street. Distance is no longer a barrier or a protection.

Militaries began to plan for how to attack over the Internet more than a decade ago. Today, perhaps half a dozen countries have advanced cyber capabilities—the United States, United Kingdom, Russia, China, Israel and one or two others. These countries could, if they wished, launch cyber attacks against an opponent's critical infrastructure.

Of course, they will not do this, any more than they would randomly shoot a missile or launch an aircraft against a potential opponent. We are likely to see a cyber attack by an advanced nation state only as part of some larger conflict. Even then, there may be a degree of hesitation. It is one thing to attack the networks of US military forces, for example, and something else to attack civilian targets in the American homeland. Cyber attack carries political risks that constrain its use.

Additionally, a cyber attack will not be decisive. Large industrial countries are not easily defeated by a single strike unless it involves nuclear weapons, and cyber attack carries nowhere near the punch of an atomic bomb. There is military value in cyber attack, but not enough to justify random actions or stand-alone assaults. Governments will be cautious to avoid any action in cyberspace that could justify the use of force in response.

Cyber war is unlikely, but cyber espionage is routine. Stealing information from opponents by penetrating their computer networks is a daily occurrence. The Internet allows the extension of the collection of signals intelligence, a long-standing mode of technical collection, and advanced nations do not hesitate to use it. The United States, being the most reliant on computers and the nation that most rapidly adopted and incorporated the new technologies into daily practice, is in some ways the most vulnerable, and the losses of government and military data and from industrial espionage have been immense.

This sort of statement always sounds like an exaggeration, and much of the discussion of cyber conflict is marked by hyperbole and hysteria. But informational losses can be documented. The State Department lost terabytes of information in a 2007 penetration probably launched by China. (A terabyte is the electronic equivalent of thousands of pages of documents.) The Department of Defense also lost similar amounts of unclassified data, as did the Departments of Commerce and Energy, and NASA. More troubling, an unidentified foreign intelligence agency was able to penetrate in December 2008 a classified Defense Network used by Central Command.

Part of the espionage activities of our potential opponents includes reconnaissance and targeting of critical infrastructure, such as the electrical grid, to prepare for attack in the event of war. This is not unusual. Russia has long-range missiles and has used satellite imagery and other intelligence from the United States to target them; it has done something similar for cyber attack. The difference is that while only a few nations can afford long-range missiles, many nations can afford cyber attack.

So our major opponents have done the reconnaissance necessary to launch cyber attacks against critical infrastructure in the event of war. We have done the same. The electrical grid is a prime target for such attacks. We know that Warsaw Pact plans for an attack against Europe made strikes against the grid one of the initial moves. Planning for strategic bombing always targeted electrical power generation, going back as far as the RAF raids on the Ruhr dams in World War II. And guerrilla groups make it a priority to attack substations, pull down transmission lines and otherwise strike electrical power generation and supply. Cyber war will be no different.

The good news for our opponents is that we have done very little to defend ourselves. Some of this reflects ideology—Americans prefer market-based solutions and are slow to regulate new technologies, but the market has failed to deliver the level of protection necessary when it comes to national security. Some of this reflects the sad state of American politics, where partisan ideology and powerful business interests make it hard to launch new initiatives. The long era of deregulation that culminated in the Wall Street crash also shaped our approach to cyber security, but hopefully without the same dramatic denouement.

Nor will it be easy to secure critical networks. We are all familiar with the successful penetration of Google at the beginning of 2010. One of the most sophisticated technology companies in the world was no match for foreign militaries and intelligence services. This should not be a surprise. We do not ask airlines to protect our airspace against foreign militaries, and we should not ask companies to defend us from sophisticated foreign opponents if we expect to succeed.

Our answer to the question as to whether we should regulate critical infrastructure to ensure better cybersecurity depends in part on when we would like to be secure. Left to its own pace, industry and technology may well be secure in a decade or two. If we are willing to remain vulnerable for that period, let nature take its meandering course.

But there is a problem. Nations are unlikely to attack randomly or at a whim (North Korea being perhaps the only exception to this statement). The same is not true for jihadis, and this could include organized groups like Hamas, Hezbollah or al-Qaeda, or chance collections of disaffected youths in Hamburg, Lahore or Detroit. They would like to strike the United States, electrical grids are a normal target, and when they get the capability, the chance of an attack will increase significantly.

It is likely that jihadis do not have this capability now. If they did, they would use it. But one thing we know about cyber attack is that it gets easier every year. There is a thriving black market in cyber crime tools and the attack techniques developed by nations eventually flow out into this black market—call it the commodization of cyber attack. Judging from earlier episodes, we could expect to see reasonably effective attack techniques reach commodity status in perhaps five to ten years.

There is the race. Perhaps ten to twenty years for better security if there is no government intervention. Five to ten years for opponents who are unlikely to be deterred from acquiring the capability for a strike. Some in the cybersecurity community talk about a “cyber 9/11” and how the United States will not do what it needs to do to secure itself until this occurs. Again, this smacks of hyperbole and exaggeration, but there is not enough hyperbole and exaggeration in this statement for us to reject it entirely. It is possible that we can avoid a damaging cyber attack if there is no conflict with China or Russia in the next decade. But hoping that your opponents do not attack you is not the best approach to national defense. While the United States has perhaps the best cyber attack capabilities in the world, it is also the nation most vulnerable to cyber attack. Changing this will require both resolve and focus from the administration and Congress, and a willingness to give up our old, market-based approach to security for a strategy that, as we do in all other areas of national defense, assigns government the lead role.