

The Cyber War Has Not Begun

James Andrew Lewis

Center for Strategic and International Studies

March 2010

Expanded attention to cybersecurity is a good thing, but it seems that it is difficult to discuss this topic without exaggeration. We are not in a ‘cyber war’. War is the use of military force to attack another nation and damage or destroy its capability and will to resist. Cyber war would involve an effort by another nation or a politically motivated group to use cyber attacks to attain political ends. No nation has launched a cyber attack or cyber war against the United States.

Indeed, it would be a bold nation that would do so. A deliberate attack on the United States could trigger a violent if not devastating response. No nation would be foolish enough to send a missile, aircraft or commando team to attack critical infrastructure in this country. The same logic applies to cyber attack. Foreign leaders will not lightly begin a war with the United States and the risk of cyber war is too high for frivolous or spontaneous engagement.

Weak attribution could allow an opponent to attack covertly, but this would require accepting the risk that the Americans would not eventually determine the source of the attack. Uncertainty about how much the Americans know and how good they are at attribution makes attackers cautious. Fear of retaliation, including kinetic retaliation, for attacking the American homeland is a threshold that no nation has been willing to cross. Call this deterrence if you like.

Even in a conflict – with China over Taiwan or Russia over Georgia – our opponents would be constrained in launching some kinds of cyber attack. Attacks on civilian targets in the continental United States could trigger a much stronger reaction than attacks on military targets and deployed forces. Moving from deployed forces in theater to civilian targets in the homeland risks unmanageable escalation. These risks and uncertainties create implicit thresholds in cyber conflict that nations have so far observed. Just as with missiles and aircraft, our nation-state opponents have the ability to strike the United States using cyber attacks, but they have chosen not to do so because of the risk of retaliation. While there are parallels to other weapons systems, cyber attack is unlikely to be decisive against a determined opponent.

Politically motivated groups, such as terrorists or other non-state actors likely do not feel the same degree of constraint. It remains intriguing and suggestive that they have not launched a cyber attack. This may reflect a lack of capability, a decision that cyber weapons do not produce the violent results terrorists crave, or a preoccupation with other activities. Eventually terrorists will use cyber attacks, as they become easier to launch, but for now we can find no example of terrorism – acts that produce fear and terror to affect political change – produced by cyber attack.

Pronouncements that we are in a cyber war or face cyber terror conflate problems and make effective response more difficult. In essence, we face four kinds of threats:

- Economic espionage, where foreign governments, companies and citizens steal

intellectual property and confidential business information from American companies (and of other developed nations). This probably happens on a daily basis, both as part of nationally directed collection programs and by individual efforts. The problem might be best thought of as a digital counterpart to the struggles over protecting intellectual property that has marked the growth of a globally connected economy.

- Political and military espionage. Cyber espionage is an expansion of traditional efforts to collect information on an opponent's intentions and military capabilities.
- Cyber crime. Directed primarily against the financial system, these illegal acts seek to extract money rather than intellectual property.
- Cyber war, where foreign militaries or other armed opponents attempt to damage or destroy U.S. military capabilities (including our informational advantage), critical infrastructure, or other civilian targets. Cyber attack is just another weapons system, similar to missiles that can be launched from a distance and strike rapidly at a target. Existing international laws of war can be applied without much strain to cyber warfare.

Cyber war is a risk, a possibility. Espionage and crime in cyberspace are routine occurrences, but they are not acts of war and do not justify the use of military force in response. Talking in terms of war, terror, attack, weapon constrains the range of action that the United States (or others) can take in response. One size does not fit all when it comes to cybersecurity, and possible responses differ by the category of threat.

Economic espionage should be approached as an economic and trade issue. It is the theft of intellectual property using cyber tools. Trade negotiations have done a good job of making the protection of intellectual property a priority- when it is on paper or a disk. We now need to extend this to digital formats and data stored on networks. Just as the United States has pressed China, for example, to improve its intellectual property laws and to take action against piracy, we need to now press them on the theft of intellectual property in cyberspace. Approaching economic cyber espionage as a trade matter offers a range of possible responses including action in the World Trade Organization (and any U.S. action would likely be supported by other nations). Nations should find ways to extend the penalties and mitigations that now apply to traditional intellectual property cases into cyberspace.

Nations should treat political and military espionage in cyberspace as they treat it in the physical world. There is a range of responses developed during the Cold War to signal displeasure with espionage. This could entail high-level contacts where the United States tells the perpetrator that they have gone to far and we will take unspecified action if they do not draw back. This will not work with some opponents – the Russians have always said that they will do in espionage what best serves their national interests. Additional punitive measures need to be contemplated. These could involve public embarrassment, expelling attachés, warrants for arrest, recalling or expelling an ambassador, and other retaliatory measures, such as restrictions on visas, financial activities or other cooperative programs. We have done nothing to signal displeasure or increase risk for cyber espionage and this needs to change.

Cybercrime is the threat that has seen the most robust response. A variety of cooperative mechanisms constrains cybercriminals in many countries. However, a few countries act as sanctuaries. The benefit is that they can use cyber criminals as a proxy force, irregulars who can engage in espionage or attack opponents at the government's behest, while providing a degree of plausible deniability. Stripping away this deniability is essential. The first step is to make clear – probably through some kind of international agreement – that a nation is responsible for the actions in cyberspace of individuals who are resident in its territory. No more, “it was patriotic hackers, not me,” excuses.

Achieving this responsibility will probably require some sort of penalty for noncompliance and the most useful model here might be the Financial Action Task Force (FATF). FATF began as a group of nations opposed to money laundering. They established practices and rules for banks and for banking authorities to make money laundering more difficult. Nations that did not comply faced greater difficulty in participating in the global financial networks – higher costs, longer delays, more impediments. A similar approach to nations that tolerate cybercrime could be to make it more difficult for them to connect to the global network, or to have their national networks face additional scrutiny and impediments. These constraints would not be foolproof but they would increase the cost to nations that act as sanctuaries and provide incentives for changed behavior.

While we have not seen cyber war or cyberattack, a number of nations have the capability to wage cyber war (at a minimum, the U.S., U.K., Russia, China and Israel) and will use these attacks in the event of a conflict. The state of American defenses is inadequate and erratic and we can only hope that there is no cyber attack while we lurch slowly toward some higher level of cybersecurity in critical infrastructure.

The problem of defense, involving as it does questions of ideology, domestic regulation, self-interest and painful issues like identity management, will not see rapid progress. There are, however international measures that the Executive Branch can take to reduce risk. First, the United States needs to establish thresholds, signals, and public doctrine on cyber warfare. This will let our opponents better judge the risk of attack and may perhaps have some deterrent effect. The President's statement on May 29, 2009 that cyberspace was a critical national asset that the United States would use all means to defend was an important first step, but there has been no following action. It is time to consider moving further. For example, the United States could announce that it sees a distinction between a cyber attack on a deployed military force and an attack on civilian targets in the American homeland and would treat the latter as a strategic threat. Exchanges of information on doctrine and national sensitivities with potential opponents (such as occurred in the Cold War) would reduce the risk for miscalculation in the use of cyber attack.

The risk of miscalculation could also be reduced by international agreement on norms for cyber conflict. Common understandings on how the existing laws of war applied, on the nature of escalation in cyber conflict, and on the responsibilities of states before and during conflict would help to create an international framework to constrain cyber conflict and define the potential consequences for differing levels of hostile action. Some norms would need to be tailored to fit a specific threat; others could apply generally. Norms will not appear magically (although there

are implicit thresholds that could be expanded and made explicit) and cyberspace will continue to be a Hobbesian environment until nations engage to cooperatively define what is responsible behavior in this new domain.

The one caveat to the rejection of cyber war hyperbole is that the damage from espionage is often invisible and difficult for the public to perceive. The goal of intelligence is to gain advantage without being detected or caught. Our opponents are skilled at this. Nations do not realize the harm until some distant reckoning, and in the interim, are only puzzled or amazed at the insights of their competitors and their rapid progress. The costs of cybercrime is also invisible, as they are usually concealed by the victims, who wish to avoid damage to brand and stock price. Some analysts believe that without exaggeration we may never see the United States take this threat seriously. Other analysts, even gloomier, believe we will not take the threat seriously until there is some cyber disaster, whatever that would be.

There is some merit to these arguments. Appeals to emotions like fear can be more compelling than a rational discussion of strategy. But the danger is that the most likely outcomes are either overreaction or miscalculation, or a blasé dismissal of risk after hearing “wolf” cried too many times. Neither is preferable. We are not in a cyber war but that does not mean the nation is not being damaged through espionage and crime. The circumstances of American politics suggest that we are unlikely to see any rapid improvement in our defenses, but there is still a range of activities that the United States can undertake to make cyberspace more secure. The most important action is to begin to assert consequences for bad behavior in cyberspace. Why are we surprised that nations and criminals exploit cyberspace when there is no penalty for them doing so? We can begin to change this now.