A GRAND STRATEGY ESSAY

Managing the Cyber Security Threat

by Abraham Sofaer

Working Group on Foreign Policy and Grand Strategy
www.hoover.org/taskforces/foreign-policy

Cyber insecurity is now well established as a serious, unconventional threat. It is a far more serious threat to the United States than to any other state because the US economy and critical infrastructure are both more valuable and more dependent on cyber systems than those of any other state. The US government and US companies are spending billions of dollars each year to protect their information systems and operations, whether intelligence, military, or commercial, and the level of spending is growing faster than any other area of national security activity.

The cyber-security policies adopted thus far reflect a unilateralist, combative mentality, aimed at finding ways to protect the United States from cyber attack and to develop forms of cyber attack to deter or retaliate when appropriate. Congress has created a Cyber Command to lead the military dimension of this effort, which supplements a massive intelligence program at the National Security Agency, Homeland Security, and other agencies, in addition to huge increases in private spending.

Inherent Vulnerability

The US government and US-based companies must prepare for the increasingly threatening and growing number of cyber attacks emanating from China, Russia, and many other places in the world. The US government needs also to recognize, however, the limits of any unilateral cyber-security program. Cyber warfare is a low-cost area of conflict in which any state or group with modest resources can participate and have a true impact; even poor nations have talented people who can learn the tricks of the cyber-warfare trade and develop new ones.

working group on foreign policy and grand strategy

HOOVER INSTITUTION
STANFORD UNIVERSITY

Regulating the US critical infrastructure is complicated, moreover, because it is largely controlled by the private sector. Proposals to enhance cyber protection of such infrastructure, called recommendations, have been prepared by the US government, but the standards or practices recommended could render critical infrastructure more vulnerable both because any flaws would be widely applicable (reducing redundancy) and because the US government would likely seek continued access to systems through measures that could be exploited by attackers. The Obama administration has backed away from mandating standards, and its proposals are so general they provide no assurance as to what any particular company will do.

Transnational Dimension of the Problem

The cyber infrastructure of the world is transnational; thus it is illusory to expect it to be effectively managed by a single state, or even by a group of states' having dominant conventional military power and vast economic resources. Only a transnational framework, based on the consent of all participating states, could be effective in reducing the security threat posed by cyber activities. To the extent the Internet has security today, it is largely because the Internet Engineering Task Force (IETF) and other private, standard setting bodies have developed and mandated protocols that must be followed by users to gain access.

President Obama instructed his administration to develop international cooperation on cyber security. Congressional leaders have also pressed for progress. The United States has had meetings with a group of states designated by the UN General Assembly to lead discussions on the subject of cyber security, but these have led to nothing more than generalizations about the group's future plans to issue general statements of principle.

At the same time, the United States has blocked efforts to develop international cyber standards and protections in the International Telegraphic Union (ITU) but has participated in several, successful international efforts to enhance security in other areas of transnational activity. International civilian aviation, for example, has been protected through many treaties and regulations adopted by states acting through the International Civil Aviation Organization, a specialized (as opposed to political) agency, within which standards are developed by committees of experts. Similar processes are successfully used in maritime standards, telecommunications, weapons of mass destruction tracking, and health. International cooperation to enhance cyber security is less necessary in that private groups–such as the IETF and

industry-specific standard setting bodies–are available to craft and adopt new cyber standards. But private standards have proven inadequate.

The United States has legitimate concerns about attempting to enhance cyber security through the ITU, but they can be effectively addressed. For example, to minimize political influence within the ITU, the United States should insist on developing standards or protocols through privately controlled expert committees (such as the IETF itself). The United States should also insist that decisions related to cyber security are made by consensus. Majority voting is rarely (if ever) the method for implementing safety measures in specialized agencies; the ITU should be no exception.

Limited Objectives

The US government claims that international agreements to enhance cyber security would lead to unwanted limitations on the use of cyber technology for military and intelligence purposes, imposed on the United States by states that want to curb US capacities. The notion that international cooperation will lead to the regulation of military and intelligence functions is baseless, however. Although Russia has called for prohibiting all military uses of cyber weapons, this position is likely to fall away if the United States seriously pursues an agreement. None of the aircraft or antiterrorism treaties applies to military or governmental intelligence functions; those that prohibit the use of biological and chemical weapons, or that apply to actions during war, are all the product of conscious decisions to disallow such activities. Indeed, agreements related to the protection of critical infrastructure could be limited during armed conflict to those that are improper targets under international law.

The United States vociferously objects to military and intelligence intrusions emanating from other states, but it is not about to give up its own foreign intelligence and surveillance activities or even what it regards as the lawful use of cyber attacks. The issue, therefore, is not whether the United States is prepared to give up cyber-related intelligence and military activities but whether it is prepared to agree to an international regime in which all states refrain from cyber attacks or interference with such activities as energy distribution, finance, and health.

That the US government is not yet ready to curb its international cyber activities, even in areas beyond military and intelligence, is reflected in the fact that its

domestic surveillance policies remain, however well-intentioned, a major source of insecurity. Efforts to develop more resilient Internet protection through strong encryption and open source software have been blocked by US government opposition.

We are in a situation today analogous to having a local government decide that, because it has developed keen night-vision technologies to track crime in the dark, it should prevent its citizens from lighting up their neighborhoods despite the well-established deterrent effect. Policies that insist on a cyber environment in which the US government can monitor the cyber world are likely to cause more crime and insecurity than the monitoring allowed can conceivably prevent. The US government should be helping actively to secure all computer systems from all intrusions, everywhere, instead of using its authority and ingenuity to insist on being able to monitor such systems.

Impact on Liberty

It is incorrect to assume that enhancing cyber security through international agreements would help tyrannical governments more effectively deny their peoples political, religious, or economic freedoms. The United States has joined several international regimes designed to protect transnational activities from conduct universally regarded as improper and harmful. Civil aviation is a good example. The United States agreed with some 180 other states that hijacking civilian planes should be treated as criminal everywhere, regardless of motive. The United States realized in ratifying such treaties that it would not want to return a person charged even with hijacking to a place that is in fact a tyranny. To solve this problem such treaties are written to require states either to extradite or to prosecute the criminals involved.

We should be willing to agree with all states, including China, Russia, even Iran, that cyber attacks on certain infrastructure should be treated as illegal everywhere, regardless of motive. We can readily square enforcing such rules with our concern for the lack of freedoms or due process in those countries by building in reciprocal remedial options.

The US government appears to believe, however, that domestic security is most effectively achieved by ensuring pervasive access to metadata to monitor both foreign and domestic activity. This policy has aggravated cyber insecurity and is an ongoing threat to privacy and political freedom.

Conclusion

In sum, the cyber threat cannot be entirely overcome, however much the United States spends to defend against it. Cyber attacks originating in foreign countries are part of a transnational game being played by many states, with low barriers of entry, increasing sophistication, increasing cost, and without the slightest chance that any state will at any time be victorious in any sense of the word.

The cyber threat needs to be managed through a combination of being realistic and honest about our willingness and capacity to guarantee security in this area; accepting multilateral arrangements to protect commerce and critical infrastructure and leaving traditional forms of intelligence and military activities unregulated; and allowing private companies and individuals to use strong encryption or open-source software without built-in vulnerabilities. The United States has barely begun to consider let alone implement these principles.

Copyright © 2014 by the Board of Trustees of the Leland Stanford Junior University

The publisher has made an online version of this work available under a Creative Commons Attribution-NoDerivs license 3.0. To view a copy of this license, visit http://creativecommons.org/licenses/by-nd/3.0.

First printing 2014
19 18 17 16 15 14 13 7 6 5 4 3 2 1

About the Author

Abraham D. Sofaer
Abraham D. Sofaer, who served as legal adviser to the US Department of State from 1985 to 1990, was appointed the first George P. Shultz Distinguished Scholar and Senior Fellow at the Hoover Institution in 1994. Sofaer's work focuses on the power over war within the US government and on issues related to international law, terrorism, diplomacy, and national security.

Working Group on Foreign Policy and Grand Strategy

The certainties of the Cold War, such as they were, have disappeared. The United States now confronts several historically unique challenges, including the rise of a potential peer competitor, a rate of technological change unseen since the nineteenth century, the proliferation of nuclear and biological capabilities, and the possible joining of these capabilities with transnational terrorist movements. There has been no consensus on a grand strategy or even a set of principles to address specific problems. Reactive and ad hoc measures are not adequate.

The Hoover Institution's Working Group on Foreign Policy and Grand Strategy will explore an array of foreign policy topics over a two-year period. Our goal is to develop orienting principles about the most important policy challenges to better serve America's interests.

For more information about the Working Group on Foreign Policy and Grand Strategy, visit us online at www.hoover.org/taskforces/foreign-policy.

HOOVER INSTITUTION
STANFORD UNIVERSITY