Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats

Office of the Coordinator for Cyber Issues
May 31, 2018

Prepared pursuant to Executive Order 13800, Section 3(b)

During the past two decades, almost every aspect of life in the United States has become dependent upon sophisticated networked information systems with global reach and power. Increasingly, malicious cyber actors are learning to exploit these dependencies to steal from Americans, disrupt their lives, and create insecurity domestically and instability internationally. The United States has resolved to take clear and unequivocal actions, partnering with friends and allies when possible, to safeguard cyberspace and the benefits it offers.

Recognizing the urgency of this and other cyber policy challenges, Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, calls for a report "on the Nation's strategic options for deterring adversaries and better protecting the American people from cyber threats." This report suggests a new U.S. vision to help guide efforts to deter adversaries and better protect the American people from cyber threats and recommends follow-on work aimed at advancing these efforts; the following unclassified overview touches on these efforts in brief, which have been ongoing.

Assessment of Deterring Malicious Cyber Activities as a Policy Challenge
Strategies for deterring malicious cyber activities require a fundamental rethinking. Cyber capabilities can be used to carry out malicious acts in peacetime, periods of increasing international tensions, crisis situations as well as during armed conflicts. Both state actors and numerous non-state actors possess such capabilities.

Although the United States has achieved important successes in recent years in promoting a framework for responsible state behavior in cyberspace, the continued prevalence of state-sponsored cyber incidents that rise to the level of a national security concern has demonstrated that the framework is necessary but not sufficient to protect against cyber threats. To achieve the stability necessary to maintain and promote the U.S. vision for an "open, interoperable, reliable, and secure internet," the United States and its likeminded partners must be able to deter destabilizing state conduct in cyberspace.

The United States remains in a strong position to deter cyber attacks that would constitute a use of force because traditional tools of deterrence – including the responsive use of kinetic force – remain effective and potent. However, there are significant challenges in deterring the substantial increase in malicious state-sponsored cyber activity occurring below the threshold of the use of force. In accordance with the task outlined in Executive Order 13800, this report proposes developing a broader menu of *consequences* that the United States can swiftly impose following a significant cyber incident, and taking steps to help resolve attribution and policy challenges that limit U.S. flexibility to act.

In addition, the U.S. government must seek to deter malicious non-state actors. The U.S. government can impose significant consequences on such actors, but their strength as a deterrent partially depends on the actors' certainty that they will become subject to those consequences. Challenges related to attribution, obtaining evidence located abroad, and seeking extradition, expulsion, or foreign prosecution, impact U.S. efforts to deter malicious non-state cyber actors.

Efforts to deter state and non-state actors alike are also hindered by the fact that, despite significant public and private investments in cybersecurity, finding and exploiting cyber vulnerabilities remains relatively easy. Those defending networks must be near perfect in their efforts, while malicious cyber actors may only need to find a single vulnerability to gain a foothold in a network.

Strategic Options

Deterrence by denial through defense and protection of critical infrastructure and other sensitive computer networks and ensuring efficient mitigation and timely recovery from malicious cyber activities must be foundational to the U.S. deterrence approach. The United States will continue to enhance its efforts to deny adversaries the benefits of their malicious cyber activities.

At the same time, the United States recognizes that network defense alone will not be sufficient to deter determined and sophisticated state-sponsored adversaries. The United States will also undertake a new effort to increase deterrence of state actors through cost imposition and other measures.

The desired end states of U.S. deterrence efforts will be:

- A continued absence of cyber attacks that constitute a use of force against the United States, its partners, and allies; and

- A significant, long-lasting reduction in destructive, disruptive, or otherwise destabilizing malicious cyber activities directed against U.S. interests that fall below the threshold of the use of force.

The President already has a wide variety of cyber and non-cyber options for deterring and responding to cyber activities that constitute a use of force. Credibly demonstrating that the United States is capable of imposing significant costs on those who carry out such activities is indispensable to maintaining and strengthening deterrence.

With respect to activities below the threshold of the use of force, the United States should, working with likeminded partners when possible, adopt an approach of imposing swift, costly, and transparent consequences on foreign governments responsible for significant malicious cyber activities aimed at harming U.S. national interests. Key elements of the approach will include:

1. **Creating a policy for when the United States will impose consequences:** The policy should provide criteria for the types of malicious cyber activities that the U.S. government will seek to deter. The outlines of this policy must be communicated publicly and privately in order for it to have a deterrent effect.

2. **Developing a range of consequences:** The United States should prepare a menu of options for swift, costly, and transparent consequences below the threshold of the use of force that it can impose, consistent with U.S. obligations and commitments, following an incident that merits a strong response that can have downstream deterrent effects. As the United States develops these options, it should assess and seek to minimize the potential risks and costs associated with each of them.

3. **Conducting policy planning for imposing these consequences:** In addition to developing consequences themselves, the United States should conduct interagency policy planning for the time periods leading up to, during, and after the imposition of consequences. Such planning, which should include the development of appropriate interagency response procedures, will help ensure consistent responses to different incidents and assist in managing the risk of escalation.

4. **Building partnerships:** The imposition of consequences would be more impactful and send a stronger deterrent message if it were carried out in concert with partners. Partner states could, on a voluntary basis, support each other's responses to significant malicious cyber incidents, including through intelligence sharing, buttressing of attribution claims, public statements of support for responsive actions taken following an incident, and/or actual participation in the imposition of consequences against perpetrator governments.

As the United States further strengthens its ability to respond to states' malicious cyber activities, it should develop tailored strategies for deterring each of its key adversaries in cyberspace. These strategies should clearly articulate ends, ways, and means, leveraging declaratory policy, a more proactive approach, broader response options, and other essential features. The United States should also create a messaging and engagement plan to ensure that adversaries know they would face consequences for engaging in malicious cyber activities against the United States and to build legitimacy and support among other foreign governments, global companies, and the general public for this approach to deterrence.

Non-state actors are susceptible to both deterrence by cost-imposition and deterrence by denial. Criminal charges and prosecutions as well as tools such as sanctions can be used to deter most would-be malicious actors. However, because certain actors, including terrorists, may not be as sensitive to the threat of cost imposition, the United States must also focus on increasing the operational cost and complexity for non-state actors to achieve their goals, including through efforts to prevent and disrupt access to malicious cyber capabilities. The United States will explore new uses of current tools and authorities, identify ways in which existing authorities may need to be amended, and, when necessary, develop legislative proposals for new authorities.