Testimony of Michael Sulmeyer
Director of the Cyber Security Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
House Foreign Affairs Committee
U.S. Cyber Diplomacy in an Era of Growing Threats
February 6, 2018

Chairman Royce, Ranking Member Engel, and distinguished members of the U.S. House of Representatives Foreign Affairs Committee, it is an honor to be with you today to discuss U.S. cyber diplomacy. I begin by noting my appreciation for the committee's bipartisan approach to cybersecurity. I note the bipartisan support for the Ukraine Cybersecurity Cooperation Act of 2017 and the Cyber Diplomacy Act of 2017, among others. As cybersecurity has become an increasingly important aspect of U.S. foreign policy, bipartisan support for keeping our country safe and protecting America's interests is essential.

I will keep my prepared remarks brief, focusing on three topics:

- The current international environment for cyber diplomacy,
- The challenges of deterring malicious cyber activity, and
- Cybersecurity and information operations in the context of our elections.

I. The current international environment for cyber diplomacy

To put it bluntly, we need diplomacy in cyberspace now more than ever. Our competitors and adversaries continue to refine their capabilities to conduct a range of cyber operations, from criminal extortion and gaining unauthorized access to networks of U.S. companies, to attempting to meddle with our elections and compromise our critical infrastructure. Despite our significant investments to develop offensive cyber capabilities and to harden defenses across the country, hackers keep hacking our systems, as well as those of our allies and partners.

Under Chris Painter's leadership, the State Department pursued international efforts to promote norms of responsible state behavior in cyberspace. This effort gained momentum during the latter years of the last administration, as did efforts to negotiate bilateral arrangements, like the U.S.-China agreement on cyber-enabled espionage for private gain against U.S. companies. The current administration has thus far pursued bilateral arrangements, like the one it announced with Israel last summer.

There are starkly divergent views among nations about the role of the Internet in society. Diplomacy and engagement is critical to ensuring the open, multi-stakeholder Internet prevails. The alternative is a closed system, governed by nations that police the content of what their own citizens express online. This is the Internet of Russia and China, not America.

Yet I do not believe there is a sufficient international appetite for a grand deal or treaty to restrain unwanted activity in cyberspace. My impression is that most state behavior—not state rhetoric—reflects a perception in international capitals that the benefits of unrestrained hacking outweigh the costs. For the time being, the United States will likely need to focus on discrete, bilateral arrangements while protecting U.S. interests in existing international institutions. Having a dedicated office at the State Department is crucial to pursuing both objectives. I also hope that such an office would take an active role in increasing the technical knowledge and training for the diplomats of today and tomorrow.

II. The challenges of deterring malicious cyber activity

For diplomacy to be successful, the United States needs to empower its diplomats with as much leverage as possible. One oft-discussed approach to creating more leverage and increasing U.S. relative power in cyberspace is to improve our ability to deter adversaries from hacking us. In an ideal world, it would be a tremendous help if these threats could be deterred by one common approach. However, the reality is far more complicated.

Not all hacks are the same, so we should not expect a one-size-fits-all model of deterrence to be successful. Attacks against critical infrastructure certainly warrant the threat of significant cost imposition, as the Obama and Trump Administrations have articulated. In some situations, deterrence in the criminal law context—which aims to minimize but not necessarily eliminate the incidence of crimes—seems more applicable to run of the mill malicious hacking, even by foreign governments, than an analogy to nuclear weapons.

I would not want to bet the cybersecurity of the United States on a policy of deterrence if I did not have to. Sometimes, like the prospect of defending against thousands of nuclear-tipped missiles, deterrence is the least bad option. That is not the case in cybersecurity. We have other options and we should employ them alongside deterrence. Pursuing strategies to prevent and preempt adversaries from being able to conduct serious cyber attacks against the United States is critical. Also, there remains so much to do to improve our defenses and our resilience in the face of incoming attacks. Success there, should, over time, bolster U.S. security and leverage for broader diplomatic efforts. However, we must be realistic about just how much we can expect from deterrence, and who we want to deter from doing what.

III. Cybersecurity and information operations in the context of our elections.

What does this mean when it comes to dealing with Russia, which launched a cyber-enabled influence campaign against us in 2016? Deterring a repeat of this conduct must be a priority for the entire U.S. government, and indeed for all nations whose elections are susceptible to Russian interference. The need to impose cost is clear, but the challenge is to impose it in ways that matter to the Russian regime—not in ways that are projections of what would matter to the United States. However, we cannot rely on deterrence alone: we need to ensure the United States has capabilities on the shelf to prevent and preempt this kind of behavior ahead of the midterms, and we must make ourselves harder to hack through improving our defenses and becoming more resilient.

I am proud to be part of a team at the Belfer Center that is releasing a new report this morning: a playbook for state and local officials with steps they can take to improve the cybersecurity of the systems they administer. It represents the culmination of months of fieldwork by the research team, including several exceptionally talented students, which developed 10 recommendations that state and local officials can consider as they prepare for the upcoming elections:

- Create a proactive security culture,
- Treat elections as an interconnected system,
- Have a paper vote record,
- Use audits to show transparency and maintain trust in the elections process,
- Implement strong passwords and two-factor authentication,
- Control and actively manage access,
- Prioritize and isolate sensitive data and systems,
- Monitor, log, and backup data,
- Require vendors to make security a priority, and
- Build public trust and prepare for information operations.

These recommendations complement our last playbook, which contained recommendations for political campaigns to improve their cybersecurity. Both reports can be downloaded from our website, belfercenter.org.

Implementing these recommendations will make our elections harder to hack. Also, proposals from both playbooks can be used by our allies and partners to bolster their defenses as well. Improving the cybersecurity of campaigns as well as at the state and local level, both at home and abroad, needs to be a core element of a broader strategy to push back against our competitors and adversaries who seek to undermine the confidence we have in the integrity of our elections.

There is every indication that foreign governments will try to sow confusion and chaos ahead of and during the next election. This should be of concern to every American, regardless of party affiliation. While I do not expect that the political divisions in Washington will be resolved by November, I hope there is growing agreement that we should not leave our elections vulnerable to foreign interference again.

Let me conclude my opening remarks by reiterating my appreciation for this committee's bipartisan approach to cybersecurity. I look forward to taking your questions.

###