Testimony of Michael Sulmeyer
Director of the Cyber Security Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
Senate Armed Services Committee, Subcommittee on Cybersecurity
Department of Defense's Role in Protecting Democratic Elections
February 13, 2018

Chairman Rounds, Ranking Member Nelson, and distinguished members of the committee, it is an honor to be with you today. The need to protect the foundations of our democratic system is of vital importance, and there are several potential roles the military can play.

I am proud to be part of a team at the Belfer Center that is releasing a new report in the coming days: a playbook for state and local election administrators with steps they can take to improve the cybersecurity of the systems they administer. Regardless of what roles the Department of Defense assumes, these defensive improvements we recommend are essential. These 10 recommendations reflect months of fieldwork by the research team, including several exceptionally talented students. They are:

- 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. It is essential that we make our elections harder to hack and to improve resiliency in case critical systems are compromised. Bolstering federal capacity to provide the kinds of support that state and local administrators request should be a priority.

In addition to improving defenses and becoming more resilient, we should also consider how best to counter threats abroad before they hit us at home. To that end, let me transition to how I see some potential roles for the military in protecting our elections. I will focus my remarks on roles that the military could play outside of the United States.

There are two necessary conditions of posture that I see as critical:

1. **Reconnaissance Posture**: Our cyber mission forces should be constantly conducting reconnaissance missions abroad to discover election-related threats to the United States and provide indicators and warnings to our forces and decision-makers. There will never be sufficient resources to prioritize all threats equally, so prioritizing threats to our elections and our democratic processes is crucial. If we do not prioritize collecting information abroad about election-related threats, than we cannot hope to disrupt them.
2. **Force Posture**: Our cyber mission forces must be sufficiently ready to strike against targets abroad identified by reconnaissance as threats to our election. Readiness is a critical issue for our armed forces today, and I would encourage the Senators on this committee to ensure they are asking tough questions about the readiness of our cyber mission forces just as they would about any other area of our military. Our forces must be ready to create different effects against a range of targets. Sometimes, they will not have much notice, so developing tactics that can be employed on the fly is important.

If the military's reconnaissance and forces are postured to focus on threats to our elections from abroad, there are four objectives that our forces should be prepared to pursue. It should go without saying that undertaking these actions would need to be consistent with international law and other relevant U.S. commitments.

1. **Preventing Attacks from Materializing**: Based on election-focused reconnaissance, U.S. cyber mission forces should develop options to disrupt the activities of those planning to meddle in our elections, and those who are in the early steps of doing so. Because these would be actions conducted by U.S. forces with a relatively long lead time, scenario-based plans should be developed and socialized with decision-makers so they are aware of the viability, risks, and benefits of different options.
2. **Preempting Imminent Attacks**: Reconnaissance abroad may provide indicators and warnings of an imminent cyber attack against election-related infrastructure, campaigns, and media and social media platforms. Our forces can prepare to neuter those attacks before they commence. Such actions would need to be undertaken rapidly as opportunities to strike may be fleeting, so developing options in advance to deliver effects promptly when so ordered is essential.
3. **Halting Attacks in Progress**: There may be situations when an adversary has already established access to a system, is in the process of denying access to data by legitimate users in the United States, or is already conducting operations to inject misinformation or steal information. In these cases, our cyber forces should provide options to decision-makers to disable these attacks by taking actions outside of the United States at the source of an attack.
4. **Retaliating after Attacks**: If the United States suffers an attack on its election infrastructure and democratic processes, policymakers may request options to respond in a timely manner. I would place emphasis on timely retaliation, since the more time that elapses after the adversary's initial attack, the harder it will be to communicate that our action is a direct response to that attack.

Across all of these objectives, proper training, thorough rehearsals, and coordination with other parts of our government are essential. Bringing military capabilities to bear, inside or outside of cyberspace, is always a serious matter, so making sure that rules of engagement and questions about authorities are settled in advance of any order to strike is critical. Here, I would note that some of our closest allies like the United Kingdom and Israel have undertaken some national-level organizational reforms to streamline responsibilities for cyber issues. We may at some point want to consider something similar.

I always appreciated how the Armed Services Committee has been a champion of supporting the Department of Defense's cyber mission force. Through the last several National Defense Authorization Acts, this committee, and its counterpart in the House of Representatives, has empowered Cyber Command with unique authorities and has engaged in necessary civilian oversight. One of the best cyber-related investments the nation has made is in the National Mission Force, an elite group of network operators under the command of the Commander of U.S. Cyber Command. According to the 2015 DoD Cyber Strategy, their mission is to defend the nation from a cyber attack of significant consequence. I think it is very much worth considering what role the National Mission Force could play to accomplish the objectives I described.

Senators might note that I have not discussed deterrence in this testimony. I very much support calls to deter adversaries from meddling in our elections. However, I would not want to bet the cybersecurity of U.S. elections 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, like the ones I described previously, and we should employ them alongside deterrence.

Let me conclude with one final proposal for the military: when possible, relevant information derived from the reconnaissance it conducts should be shared with relevant parties at home. At times, some of this information may be useful to officials at the state and local level. I want to commend the Department of Homeland Security for working hard to promote information sharing over the last several years, and more recently to provide clearances to state officials so they have greater access to important information.

That concludes my prepared testimony. I look forward to taking your questions.