NSI THE NATIONAL SECURITY INSTITUTE
At George Mason University's Antonin Scalia Law School

CYBERSECURITY AGENDA SETTING FOR THE 2019 NDAA

February 26, 2018 - U.S. Senate Visitor Center

As the National Defense Authorization Act for FY 2019 begins to take shape in Congress, the National Security Institute co-hosted a panel with the R Street Institute to discuss how to best promote national security in cyberspace. The panel—consisting of Tara Swaminatha, a partner in the Data Privacy & Cybersecurity Practice at Squire Patton Boggs; Klon Kitchen, Senior Fellow, Technology, National Security & Science Policy at the Heritage Foundation; Dr. Betsy Cooper, Executive Director of the UC Berkeley Center for Long-Term Cybersecurity; NSI Founder Jamil N. Jaffer; and NSI Visiting Fellow Megan Reiss (moderator)—proposed a variety of policy recommendations to strengthen America's cybersecurity while also promoting innovation.

Use of Cyber Tools at the Tactical Level and the Need for Clear Rules of Engagement. Both Mr. Kitchen and Professor Jaffer discussed the need for the development of rules around the use of cyber capabilities on the battlefield. Mr. Kitchen focused on cyber capabilities on the tactical level, arguing that in a highly-connected environment, not allowing our broader, consistent access to basic cyber tools forces soldiers in conflict zones to take unnecessary risks. Mr. Kitchen noted that determining the appropriate scope of such authorities and setting appropriate limitations on the use of electronic warfare capabilities is difficult. To start, he suggested providing special forces operators involved in local operations in conflict zones with authority to use cyber tools that have temporary effects with limited scope. Professor Jaffer raised the question of having consistent rules of engagement in place in the event of a larger cyber conflict and argued that we are already engaged in a "very real shooting war in cyberspace." He warned that if a full-fledged cyber conflict were to break out, the public would take the government and industry to task for not being prepared to respond effectively and that having clear rules of engagement in place ahead of time could help address the speed and effectiveness of any response needed.

SPEAKERS

Dr. Betsy Cooper
Executive Director, Berkeley Center for Long-Term Cybersecurity

Jamil Jaffer
Founder, National Security Institute

Klon Kitchen
Senior Fellow, Technology, National Security & Science Policy, Heritage Foundation

Tara Swaminatha
Partner, Squire Patton Boggs

Moderator:
Dr. Megan Reiss
Senior National Security Fellow, The R Street Institute

Information Sharing. Speaking to the government's role in cyberspace, Mr. Kitchen pointed out that the government "is not *the* stakeholder but *a* stakeholder," and that with that in mind, industry and the government must work together to address potential national security threats. Professor Jaffer argued that the only way to get industry buy-in on public-private cybersecurity information sharing at scale is to show companies a clear return on investment for sharing information with the federal government in the form of real intelligence sharing back from the government. Dr. Cooper suggested that one way to get buy-in from industry is to expand the scope and funding for the Defense Innovation Unit Experimental (also known as DIUx), a Department of Defense organization focused on accelerating the provision of commercial technologies to the U.S. military. Additionally, Dr. Cooper argued that allowing for more regular input from industry leaders in the form of advisory boards or similar groups could help build both industry and the government's capacities to deal with cybersecurity threats.

Supply Chain and Regulation. Ms. Swaminatha discussed the critically important role of proper supply chain management in corporate and government cybersecurity and highlighted the recent controversy over the use Kaspersky Labs software by government agencies. Ms. Swaminatha raised the question of how Kaspersky software was authorized for use on government computers not withstanding federal supply chain controls. Mr. Kitchen detailed the breadth of Kaspersky's usage, pointing out that Kaspersky had root access into some of the government's most secure systems and arguing that such access should only be provided to companies that have cleared the highest levels of scrutiny. However, both Mr. Kitchen and Ms. Swaminatha voiced concern over focusing too heavily on the nationality of product manufacturers as a proxy measure for security controls and procedures. Ms. Swaminatha suggested that NIST could play a useful role in fleshing out appropriate guidance and standards to help address supply chain issues while promoting cybersecurity and innovation. Professor Jaffer pointed out while a voluntary framework promulgated by NIST might certainly be useful, "regulations are where the disaster is [in cybersecurity]." According to Professor Jaffer, the federal government—which has traditionally been weak at protecting its own networks—is in no position to prescribe solutions for the private sector and could easily make things worse by putting in place strict regulations that are hard to change as technology rapidly evolves. Dr. Cooper suggested that if a more regulatory-style framework was necessary in this space, any rule should come through an iterative peer-review process and that such a process should be required to continue through the life of any such regulation thus providing for regular updates and limiting the possibility of the enforcement of outdated cybersecurity solutions.

Workforce Development. Dr. Cooper discussed the government's ongoing difficulties in recruiting highly qualified staff and highlighted a recent white paper from UC Berkeley's Center for Long-Term Cybersecurity which argues for the creation of a cyber workforce incubator in Silicon Valley, where federal employees could work for one to two year terms side-by-side with private sector employees also seconded for such medium-term assignments before returning to their respective positions. This would allow government and industry to break down the barriers of geography and culture which limit collaboration and often keep many potential employees away from the public sector. Dr. Cooper also argued that such a public-private joint workforce could reduce the potential brain drain from the government.