Testimony of Congresswoman Anna G. Eshoo (5 minutes)
Select Committee on the Modernization of Congress
Member Day Hearing
H-313, U.S. Capitol
March 12, 2019

Chairman Kilmer, Vice Chairman Graves, Members of the Committee. Thank you for the opportunity to testify today before the Select Committee on the Modernization of Congress.

Congress has a rich and illustrious history tied to some of the most important events in our nation's history. But this great institution is very much stuck in the past when it comes to how it conducts its business.

That must change, and this Committee is the tip of the spear to make this change possible.

I'm here today because Members of Congress and Congressional staff need a wake-up call. We need to wake up to the reality that we are being targeted by foreign adversaries for hacking and electronic surveillance.

We are all high-value targets because of the important—and often confidential—work we do. Our adversaries want to exploit us to weaken and destabilize our democratic institutions.

Like most Americans, Members of Congress and staff spend a large part of our day communicating through digital means. We email, text, use apps and social media, and store our personal and sensitive information online.

The House has protections for official accounts, requires staff to complete basic cybersecurity training, and secures digital information. However, many Members and staff do not realize that communications on our personal devices are also valuable and vulnerable.

We know that major cyber-attacks have been carried out by foreign adversaries against campaign committees like the DNC hack in 2016 and the NRCC hack in 2018. Members of Congress have also been targeted individually in their official capacity and their unofficial capacity by a complex set of foreign actors and adversaries.

Last year, the Department of Homeland Security publicly acknowledged the existence of International Mobile Subscriber Identity (IMSI) catchers, known as Stingrays, in Washington. These devices can eavesdrop on our calls, track our location, and plant malware on our devices.

These attacks are not isolated to the United States. In January, hundreds of German lawmakers and public figures were hacked and had their personal information published online, and in 2015, Germany's government network was breached by hackers.

Last month, the computer network of the Australian parliament was breached by what Australian authorities believe was a "sophisticated state actor" ahead of Australia's federal elections which are scheduled to be held in May.

While Congress currently has dedicated personnel in place to monitor and address cyber vulnerabilities, I'm concerned that many members and staff are still relying on non-secure technology.

Encrypted messaging, multi-factor authentication, and regular and advanced cyber-hygiene training, should all be basic standards for Members and staff.

I urge this Committee to closely examine how Congress currently protects our institution and those who work here from increasingly complex cyber threats, and identify steps we can take to strengthen these protections and implement them.

This includes providing existing cybersecurity offices and staff in Congress with more resources, or establishing a permanent Select Committee to monitor evolving threats, identify new vulnerabilities, and provide guidance and recommendations to Congress.

As FBI Director Christopher Wray said last week at RSA's annual cybersecurity conference, "the scope, the breadth, the depth, the sophistication, the diversity of the threats is unlike anything we've had in our lifetimes."

I want to make sure Members of Congress and their staff have the resources, expertise, and awareness to stay ahead of these threats. This Select Committee can play a critically important role in guiding our efforts to do this.

Thank you again for the opportunity to testify today and I look forward to working with you and following your efforts closely.