Follow/Mention
@HouseForeign

Opening Statement of the Honorable **Ed Royce (R-CA), Chairman**
Committee on Foreign Affairs Hearing:
"U.S. Cyber Diplomacy in an Era of Growing Threats"
February 6, 2018

(As prepared for delivery)

"Cyber-attacks and other malicious activity by foreign governments, terrorists and criminals are a serious threat to U.S. national security and economic interests around the globe.

As the Intelligence Community made clear in its 2017 Worldwide Threat Assessment, 'Our adversaries are becoming more adept at using cyberspace to threaten our interests and advance their own, and despite improving our cyber defenses, nearly all information, communication networks, and systems will be at risk for years.'

Cyber threats have real world impact. In 2015, Chinese hackers stole the personnel files of 20 million current and former Federal employees in a massive data breach. Last year, North Korean hackers crippled hospitals in the U.K. and halted international shipping in India. Russia exploits cyberspace to attack its neighbors, including Estonia and Ukraine, and to attempt to undermine Western democracies – including the United States.

Yes, our military does have some very unique offensive and defensive capabilities in cyberspace and other agencies protect critical infrastructure, but it's our diplomats who work with our allies and partners to develop a common response to these threats while engaging our adversaries to make clear that cyber-attacks resulting in real world consequences will be viewed as a use of force. The importance of the State Department's work cannot be understated.

Indeed, the department's role becomes essential when you consider that it's not just computer networks and infrastructure that the United States needs to protect. The open nature of the internet is increasingly under assault by authoritarian regimes, like China, that aggressively promote a vision of 'cyber sovereignty,' which emphasizes state control over cyberspace. This obviously could lead to a totalitarian dystopia and runs counter to American values of individual and economic liberty.

We saw this recently in Iran, where the regime shut down mobile internet access and blocked – or pressured companies to cut off – social media tools used to organize and publicize protests. Authoritarian regimes would love to globalize this censorship that they have long imposed at home. It falls to our diplomats to help ensure the world rejects this limited version of cyberspace and that the American vision of an open, secure and innovative internet wins out over George Orwell's premonitions.

Coordination among allies is critical. In response to different understandings of privacy between the United States and Europe, the State Department worked with the Department of Commerce to successfully negotiate the E.U.-U.S. Privacy Shield Framework, which ensures data – and business – continues to flow across the Atlantic. This week, the House will pass a bill strengthening our cyber coordination with Ukraine. But there is still much more to be done.

That’s why, last month, the House passed the Cyber Diplomacy Act. This bill, which I introduced, ensures that the State Department has a senior diplomat charged with leading this effort that brings together our security, human rights and economic priorities. I am encouraged to hear that the administration has heard our concerns and is working to elevate this position.

Today, we are joined by three experts with experience in cyber diplomacy, technology and defense – including the Department’s former Coordinator for Cyber Issues. We look forward to discussing how Congress can best support strong cyber diplomacy.”