Follow/Mention
@HouseForeign

Opening Statement of the Honorable **Ed Royce (R-CA), Chairman**
House Foreign Affairs Committee Hearing:
Cyber War: Definitions, Deterrence, and Foreign Policy
September 30, 2015

(As prepared for delivery)

This hearing will come to order. This morning we consider the growing threats to U.S. national security in cyberspace.

It is no exaggeration to say we are at the dawn of a new age of warfare. Computers and the Internet have connected people around the world. However, reliance on these technologies has also made us vulnerable to cyberattacks from other countries, terrorists and criminals. So much so that the Pentagon now counts cyberspace as the “fifth domain of warfare,” - alongside land, air, sea and space.

Whether or not an all-out cyberwar occurs, it is clear that we are in a state of ongoing cyber conflict. The White House, the State Department, and the Department of Defense have all been hacked. And of course, the Office of Personnel Management had the sensitive information of more than 21 *million* Americans compromised. In the private sector, hackers have crashed the computers of Sony executives, seized the personal information of more than 78 million people from the nation’s second largest health insurer and stole the credit and debit card information of more than 40 million customers of a major retailer. The magnitude of this theft is staggering. Yet it is said that it takes companies an average of 205 days to even realize their system has been breached.

Across the globe, Estonia found itself at the opposite end of a crippling Russian-backed “denial of service” attack. A computer “worm” shut down the air force and navies of France and Great Britain for a time. And an attack from North Korea coined “Dark Seoul” crippled South Korea’s banking system.

In the coming years, it is likely that Iran will pour more resources into cyber-weapons. These have already been used against the U.S. Navy, American banks, a Las Vegas casino and Saudi Arabia’s largest oil producer – all without setting off significant retaliation. Indeed, it has been said that it is exactly the lack of international norms in responding that makes cyber-weapons so attractive to Russia, China, Iran and North Korea.

So we have work to do. Our top intelligence officer told Congress earlier this month that the U.S. lacks “both the substance and the mind-set of deterrence.” Indeed, last spring, the President issued an Executive Order that would allow him to target individuals or organizations deemed responsible for computer attacks. But this new order - similar to the way in which terrorists or nuclear proliferators are targeted – has *yet* to be used.

So the President's recent comment that "offense is moving faster than defense" is putting it mildly. From the private sector to government, our county is taking body blow after body blow in cyberspace. Why aren't we hitting back? As one observer notes, "we have a deterrence deficit."

The new agreement between the United States and China on economic espionage would be a step forward if China actually abides by it. And others like Iran and Russia will be watching closely how the United States responds to what is perhaps the greatest theft in history.

We look forward to hearing from our witnesses. What is "cyber war" and how does it differ from "cyber conflict" and "cyber espionage"? Could better attribution techniques be developed to help the United States deter cyber attacks? What is the role of diplomacy in containing cyber conflict? Do the international norms surrounding traditional warfare apply? And what are the foreign policy implications of continued cyber infiltrations and espionage?

We look forward to our witnesses' testimony as we consider U.S. responses to one of the most urgent problems facing the United States.

I now turn to the Ranking Member for any opening comments he may have.