JASON CHAFFETZ, UTAH
CHAIRMAN

ONE HUNDRED FOURTEENTH CONGRESS

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225-5074
MINORITY (202) 225-5051

http://oversight.house.gov

Opening Statement
Rep. Robin Kelly, Ranking Member

Joint Hearing on "Digital Acts of War: Evolving the Cybersecurity Conversation"
Subcommittee on Information Technology and Subcommittee on National Security

I'd like to thank Chairman Hurd and Chairman DeSantis for calling this hearing so that the Committee and the American people can get a better understanding of when a cyberattack should be considered an "act of war" and how the United States might respond when that happens.

The cyber threats facing the United States are increasing in severity, opening the nation to the possibility of extremely damaging cyber strikes that could potentially threaten the U.S. economy and endanger American lives.

General Alexander, in your 2014 testimony before the Senate Committee on Armed Services you warned, and I quote: "Those attacks are coming and I think those are near term and we're not ready for them."

In fact, we are already seeing the first salvos of digital attacks reaching beyond the cyber realm.

In March of this year, seven members of Iran's Revolutionary Guards Corps hacked into the control system of the Bowman Avenue Dam in Rye Brook, New York.

In response to the compromise of the dam's cyber network, Paul Rosenberg, the village's mayor said, quote:

"It's ridiculous how little that dam is, how insignificant in the grand scheme of things … We're not talking about something vital to the infrastructure of the country."

While May's attack may not have targeted the nation's vital critical infrastructure, it is almost certain that future attacks will.

And when that does happen, how do we react?

Do we hack the hackers or do we respond with physical force?

This isn't the first time Congress and the Intelligence Community have tried to answer that question.

During a September 2015 House Permanent Select Committee on Intelligence hearing, Representative Jim Himes asked, and I quote:

"Is stealing classified information from us an act of war? … What if that espionage leads to the death of Americans? At what point does it become an act of war that's responded to in the cyber realm? At what point is an acted of war responded to outside of the cyber realm?"

That decision shouldn't be made in a vacuum.

It is important that we recognize that the global nature of the Internet requires the United States to establish solid partnerships throughout the international community so that every nation understands that there are consequences for unacceptable cyber behavior.

The problem is that by laying out in a public forum what constitutes "unacceptable," we open the possibility that our adversaries know where the tripwire lies across which they can't step.

That's why I'm pleased the chairmen have arranged for Committee members to receive a classified briefing to better understand where that line is and how we respond when our enemies cross that line.

Again, I'd like to thank the chairmen for calling this hearing and our witnesses for being here today.

Contact: Jennifer Werner, Communications Director, (202) 226-5181.