ELIJAH E. CUMMINGS, MARYLAND
CHAIRMAN

ONE HUNDRED SIXTEENTH CONGRESS

JIM JORDAN, OHIO
RANKING MINORITY MEMBER

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143

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

http://oversight.house.gov

Opening Statement
Chairman Stephen F. Lynch
Subcommittee on National Security
Joint hearing with the House Armed Services Committee Subcommittee on Intelligence, Emerging Threats and Capabilities on "Securing the Nation's Internet Architecture."
September 10, 2019

Before I begin my opening statement, I'd first like to thank my good friend, Chairman Langevin, for working collaboratively with me and my subcommittee on this critically important hearing. Mr. Langevin has been a strong advocate for improving the resiliency of our nation's critical infrastructure and ensuring that necessary cybersecurity safeguards are in place to protect the United States against the multitude of threats we face every single day. He has made this issue a priority, and it is one that I share with him as Chairman of the House Oversight Subcommittee on National Security.

Today's hearing will examine how federal departments and agencies work together to protect the critical architecture upon which U.S. internet and telecommunications systems depend. By working together on this issue, our subcommittees will be better positioned to identify and fill gaps and vulnerabilities across the various federal agencies and private sector entities responsible for protecting our nation's internet infrastructure.

Uninterrupted and secure access to the internet is critical to daily life in the 21st century. Our constituents rely on the internet to search for jobs, access bank accounts, read the news, and communicate with family and friends around the world. Companies in every industry, from Midwest manufacturers to the financial sector in New York, need the internet to participate in the national and international economy. The U.S. military requires reliable and secure access to the internet to conduct overseas operations and is also tasked with protecting our networks from cyber-intrusions by foreign actors.

Improving secure and reliable access to the internet is also vital to economic development and promoting livelihoods in less developed countries or areas. In fact, I just returned last week from leading a Congressional delegation to Jakarta, where I met with young entrepreneurs from the Indonesian financial technology sector who all highlighted the importance of expanding internet connectivity across Indonesia's more than 17,000 islands to bring additional customers into the digital financial market.

Given our growing dependence on the internet, even temporary disruptions, regardless of whether they are intentional or accidental, can have serious, cascading effects across industries and among the nation's critical infrastructure sectors. Yet, no single U.S. government entity is responsible for securing the internet and its underlying architecture. Instead, multiple departments and agencies have various jurisdictional roles, including the Department of Homeland Security, the Department of Defense, and the Department of Commerce – from which we are fortunate to have representatives before us today. In addition, the White House, the Department of Energy, the Department of Justice, and the Federal Communications Commission, all have a role to play in securing this infrastructure.

Adding to the complexity of their task is the fact that the physical components of our nation's telecommunications infrastructure -- such as fiber optic cables, data centers, and Internet exchange points -- are largely owned by the private sector. This means that coordination and communication within the federal government and across the public and private sectors are all crucial to the internet's security.

The challenge we therefore face is that when everyone is in charge, then nobody is in charge. And while internet activity appears to move seamlessly across digital pathways, this movement is cemented in real, physical infrastructure — the security of which has often been taken for granted. Physical fiber cables buried under our streets and under international waters carry this traffic from Point A to Point B. Data centers and Internet Exchange Points serve to store and transfer this traffic from network to network. All of these physical assets can be damaged by natural disasters, human-caused accidents, or intentional attacks by sophisticated, malign actors.

As former Director of National Intelligence Dan Coats highlighted in his 2019 Worldwide Threat Assessment, we know that our adversaries are already probing U.S. electric utilities, election systems, pipelines, and financial networks for any signs of weakness. China, Russia, Iran, and North Korea are all increasingly using cyber operations to steal data, disseminate misinformation, and "disrupt critical infrastructure." Russia, Director Coats said, is "mapping our critical infrastructure with the long-term goal of being able to cause substantial damage." Multiple open-source reports in recent years have also noted increased foreign military activity around undersea data cables, raising concerns hostile actors could be looking for ways to interfere with this critical infrastructure.

To our witnesses, I realize that some of today's questions may drift into topics not suitable for an open hearing. With that in mind, I ask that you do your best to answer Members' questions as candidly as possible, but you should not disclose any classified, or sensitive security information. Instead, please let us know that you would prefer not to respond for national security reasons, and we can move on to the next question. We will, however, reserve the right to request that information in a more appropriate setting at a later date.

Chairman Langevin, thank you again for holding this important hearing with me, and with that, I yield back.

Contact: Aryele Bradford, Communications Director, (202) 226-5181