JAMES COMER, KENTUCKY
CHAIRMAN

ONE HUNDRED EIGHTEENTH CONGRESS

JAMIE RASKIN, MARYLAND
RANKING MINORITY MEMBER

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

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

https://oversight.house.gov

Ranking Member Gerald E. Connolly
Subcommittee on Cybersecurity, Information Technology, and Government Innovation
Hearing on "Red Alert: Countering the Cyberthreat from China"
May 15, 2024

This past March, the Office of the Director of National Intelligence (ODNI) released their Annual Threat Assessment of the U.S. Intelligence Community. An excerpt from the report reads, "China remains the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks."

The Chinese Communist Party, or CCP, poses a significant threat to the safety and economic prosperity of the United States. Through a multipronged strategy that includes the Belt-and-Road initiative, economic coercion, and military buildup—the CCP has sought to challenge the American-led rules based international order. As part of their larger campaign to conduct asymmetric attacks on the United States, Beijing has turned to cyberattacks to steal American companies' intellectual property, undermine our civil society, and disrupt our critical civilian and military infrastructure.

Just two months ago, the Cybersecurity and Infrastructure Security Agency, or CISA, confirmed that CCP sponsored groups, like Volt Typhoon, have successfully infiltrated the federal government's civilian and military systems. What's more, some of those groups have been on our networks for up to five years and lay in waiting until the opportune moment to disrupt a military response or disable our water and power infrastructure.

Unfortunately, when it comes to cyber warfare, the threat extends beyond China. In fact, experts have identified that not just China, but also Iran and North Korea are using Russia's well-known disinformation playbook to disrupt our elections, infiltrate American companies, and cause mayhem. Although disinformation campaigns and cyberattacks are not identical, they are two halves of the same chaotic coin. They similarly seek to inject uncertainty into daily operations and undermine the foundations of our businesses, communities, and democratic tenets.

Last November, Meta released their third quarter Adversarial Report, which outlined the removal of nearly 5,000 fake accounts based in China. Meta removed these accounts for impersonating U.S. citizens and posting divisive rhetoric on deeply sensitive internal political issues with the intent to impact the upcoming U.S. 2024 presidential election.

But it is not just America at risk. Earlier this year, the CCP again employed Moscow's tactics of online disinformation campaigns to cast doubt about Taiwan's government and influence their elections. China has made a concerted effort to extend its power and influence across the world—especially in the Global South. As roughly half of the world's population heads to the polls in 2024, China will take this opportunity to expand their influence and disrupt democratic processes using all tactics at hand.

Fortunately, the Biden-Harris Administration has taken unprecedented steps to counter foreign cyber threats—both direct cyberattacks and disinformation campaigns. The White House also released the first ever National Cybersecurity Strategy in October 2022, directing both public and private

stakeholders to coordinate their efforts to address cybercrime as a national security threat. Last Monday, the State Department released a new ambitious plan called the International Cyberspace and Digital Policy Strategy, which seeks to work with allies to counter Russia and China's global election interference efforts.

I am also proud to have partnered with this Administration to safeguard our networks against harmful nation state actors. Historically, this Subcommittee has held hearings to conduct meaningful oversight of federal IT programs—including the Federal Information Technology Acquisition Reform Act or FITARA—and worked alongside the Government Accountability Office (GAO) to produce a biannual Scorecard. Agencies then receive grades based on their compliance with the law and other statutorily grounded IT priorities. The Scorecard assesses compliance with the Federal Information Security Modernization Act (FISMA), evaluating all 24 CFO Act agencies' cybersecurity postures.

For further transparency, and after years of congressional advocacy for metrics to replace the expiring Trump-era Cross-Agency Priority data, OMB finally began publishing quarterly Federal Cybersecurity Progress Reports on the Performance.gov website. These reports measure agencies' progress in achieving milestones and implementing key cybersecurity measures articulated in the Biden Administration's Executive Order on Improving the Nation's Cybersecurity. The Executive Order encouraged adoption of zero trust architecture, and I encourage the Administration to evolve the Performance.gov data and provide public metrics to assess agencies' implementation of those required zero trust capabilities.

To successfully stop our foreign adversaries, we need a whole-of-government approach with bipartisan Congressional support to bolster our federal workforce and its IT infrastructure. And we need a whole-of-nation approach to combat misinformation.

A report from the Center for Security and Emerging Technology found that quote "by 2025 Chinese universities will produce more than 77,000 STEM Ph.D. graduates per year compared to approximately 40,000 in the United States. If international students are excluded from the U.S. count, Chinese STEM PhD graduates would outnumber their U.S. counterparts more than three-to-one." For our country to compete with China, we need to implement the Office of the National Cyber Director's National Cyber Workforce and Education Strategy's recommendations and bolster our cyber workforce and cyber faculty pipelines. I will soon introduce new legislation to enhance the already highly successful CyberCorps program, which boasts an impressive 97% successful job placement rate. When passed, my bill will extend the scholarship cap of this program from three to five years and provide a pathway for more STEM trained Ph.D.s to serve in federal government, as well as increase much-needed faculty members at American universities.

We must also properly fund the cyber defenses and basic government IT by reauthorizing and properly funding the Technology Modernization Fund (TMF). In 2021, Democrats fought to secure a revolutionary $1 billion investment for the program. Today, the TMF has funded 11 zero-trust efforts as well as numerous other cyber projects that protect our military and sensitive information while retiring vulnerable legacy systems.

Congress usually sees IT as an easy thing to cut, but in most cases, IT modernization is a critical investment into our future. The pandemic exposed the cracks in the federal government's aging IT infrastructure. Upgrading those systems is not just a national security priority, it's common sense.

State-sponsored cybersecurity and disinformation campaigns seek to undermine the very fabric of our society. Cyberattacks wreak chaos and prove to be costly. Disinformation campaigns obscure the truth and threaten democratic principles. We must work to contain both.

I look forward to hearing from our witnesses and learning more about what Congress can do to combat these threats to the American people.

###

Contact: Nelly Decker, Communications Director, (202) 226-5181