U.S. House of Representatives
Committee on Energy and Commerce
Subcommittee on Communications and Technology

Hearing on

Safeguarding Americans' Communications: Strengthening Cybersecurity in a Digital Era

January 11, 2024

Questions for the Record

Mr. Clete Johnson, Senior Fellow, Center for Strategic & International Studies

The Honorable Earl L. "Buddy" Carter

1. Ever since the National Cybersecurity Strategy was released in March of 2023, there has been increased attention to cyber issues from various federal agencies which is a positive development. There is, however, the concern that we are "over-regulating" in this space. The last thing we want to do is create confusing and even conflicting regulations for the same industry. Given the growing fragmentation of cybersecurity regulation across government agencies, how can we help reduce the fragmentation and drive harmonization of guidance for each industry, so we can avoid conflicting mandates across government agencies?

Clete Johnson answer: Throughout my career on Capitol Hill, at the FCC, at the Commerce Department, and now in the private sector, I have worked to advance policies that harness the power and dynamism of private sector cybersecurity capabilities, including by seeking to streamline and harmonize or otherwise replace compliance-based regulatory requirements that in some cases can actually hinder cybersecurity performance. With this in mind, I strongly believe that any regulatory action or other government initiatives that seek to bring accountability on cybersecurity should focus primarily on (1) intentional collaboration between different network stakeholders (both government and industry) and (2) elevating dynamic, flexible preparedness and response capabilities.

I believe that a system of dynamic, proactive, collaborative accountability for security – particularly if it can harness powerful market drivers that are aligned with government security expectations – can prompt an ever-improving "race to the top" in security. In contrast, traditional prescriptive checklist compliance regulation too often leads to complacency at the lowest common denominator.

As I mentioned at the hearing, a good example of what this approach could look like in real life is the government-industry initiative on internet routing security. The various stakeholders in the internet routing ecosystem are diverse, complex and global, including entities such as cloud providers and enterprise network operators that are outside the reach of the FCC or other U.S. government agencies. Routing security is not conducive to one-agency oversight, so last year leading ISPs proposed that the U.S. government should undertake a broader collaborative approach to ensuring accountability in routing security. This process, underway now and convened by the Office of the National Cyber Director with the assistance of the FCC, includes multiple federal agencies such as NTIA, NIST, CISA, and the Dept. of Justice, along with a wide variety of internet stakeholders.

This is a "whole of government" and "whole of the internet" approach to security that has shown significant positive impact in its early months. It is based on performance and mutual accountability rather than a one-size-fits-all compliance checklist. I think this effort represents an especially effective approach to security that will be more dynamic and effective than a prescriptive compliance approach, which I fear would lead to companies replacing proactive solutions-oriented engineers with skittish lawyers hedging against regulatory risk.

The Honorable Lizzie Fletcher

Last fall, this Subcommittee held a hearing on artificial intelligence in our communications networks. Many members, including myself, focused on the potential harmful impacts of AI when biased or unrepresentative data is used as an input. I want to take that conversation a step further today to discuss the cybersecurity of common AI products like ChatGPT and the potential for malicious actors to hack these AI systems and manipulate outputs.

1. I want to open these questions to the whole panel. Are there specific conditions or issues to consider when developing cybercrime strategies for AI products? Do strategies differ for open-source AI versus closed source AI?

Clete Johnson answer: As a security professional, my expertise and focus regarding AI has centered on AI's many uses for enhancing network security (for instance, through advanced threat detection and anomaly detection) and also the AI capabilities that bad actors in cyberspace increasingly leverage for their own nefarious ends (for instance, advanced social engineering for spear-phishing attacks). However, even just within the communications sector, AI applications are numerous and diverse, meaning that cybersecurity risk management for each must consider the use case in which the AI product is deployed.

Pursuant to the recent Executive Order on Safe, Secure, and Trustworthy Development and Use of AI, work is underway at the National Institute of Standards and Technology (NIST) to support industry standards for AI development and deployment that will consider what common cyber risk management strategies are appropriate for AI models. One challenge ahead will be to balance security equities regarding AI products to ensure that even as we manage risks related to developing and deploying AI, we also empower

stakeholders to leverage AI-supported cyber defense capabilities to meet and outpace emerging/evolving threats.

2. Do you have any recommendations for minimum security measures for new AI models before they become open sourced?

Clete Johnson answer: While the myriad and diverse applications of AI have unique security considerations based on their risk posture (e.g., based on their function, context, use case, etc.), existing tools like the NIST Cybersecurity Framework and new AI Risk Management Framework can help stakeholders develop and deploy AI in responsible ways. In particular, these tools can help clearly communicate the security risk decisions that are built into a particular AI model so that entities who build on and deploy that model can factor those decisions into their own security risk management and communication with end users. Pursuant to the recent Executive Order on Safe, Secure, and Trustworthy Development and Use of AI, the National Telecommunications and Information Administration (NTIA) recently launched an effort to assess the risk and benefits of open source AI. I am hopeful that through efforts like these we will mature our expectations for open source AI model security.

The Honorable Debbie Dingell

1. I'd like to touch on risks associated with the reliance on foreign suppliers sourcing materials for our networks — a major supply chain vulnerability and a matter of national security. I was proud to see bipartisan supply chain legislation pass through Committee earlier this Congress that gives the federal government the authorities and tools needed to strengthen our industrial base and support supply chain resilience, which is vital for our competitiveness as a country.

   Mr. Johnson, how can we reduce the barriers for American companies trying to manufacture these materials? What safeguards need to be implemented to ensure that projects funded by American taxpayers result in domestic manufacturing and job creation?

Clete Johnson answer: For decades dating back to the end of the Cold War, the revolution in global shipping that came along with the proliferation of RFID tags and standardized shipping containers combined with dramatic advances in data analysis and advent of the internet to create unprecedented efficiencies in global supply chain and inventory management. The downside of those efficiencies, particularly in the ICT sector, was that hardware and related materials made in China and/or by PRC-backed companies flooded the market, often for predatory economic, strategic, or espionage purposes, creating supply chain vulnerabilities regarding untrusted suppliers like Huawei and ZTE. Then, in this broad context, the severe supply chain disruptions of the Covid-19 global pandemic added significant problems regarding supply chain availability and access – on top of the untrusted supplier challenge.

The United States and its allies are generally responding with aggressive new supply chain strategies based on promoting trusted suppliers, including and regionalized supply chains focusing on domestic and allied suppliers. This Committee has played an important role in advancing legislation to this effect, namely the Secure Networks Act, the Secure Equipment Act, and the CHIPS and Science Act, and also by working to free up spectrum for commercial uses. All of these initiatives are crucial to establishing a secure ICT supply chain from trusted domestic and allied vendors.

The Committee should continue to ensure that the Administration and the FCC identify untrusted suppliers and help eliminate them from our market, with clear government processes that are as transparent as possible and provide appropriate transition periods for affected U.S. industries. Of course, this must also include full funding of the "rip and replace" program to reimburse smaller networks for replacing untrusted equipment designated on the FCC's Covered List.

The Committee should also promote innovation among trusted suppliers in both the United States and our allies, which collectively constitute an extremely large, robust, and competitive global market to which U.S. suppliers can sell their products and from which U.S. network operators can procure trusted equipment. First, the Committee should ensure that grants from NTIA's Wireless Innovation Fund are issued in a timely fashion, particularly the large grants that will meet Congress's intent to accelerate the trusted supplier market for open and interoperable Radio Access Network deployments. Second, as we discussed in depth in a hearing in March 2023, it is imperative that Congress restore the FCC's spectrum auction authority and replenish the U.S. spectrum pipeline for commercial 5G. In short, if the United States lags China in spectrum availability for 5G, China's "national champion" companies – not trusted U.S. and allied-based companies – will supply the 5G services of the future. A shortage of commercial spectrum means a shortage of trusted suppliers, particularly in the United States.