paloalto®
NETWORKS

December 20, 2023

The Honorable Robert E. Latta
United States Representative
2125 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Latta:

Thank you for the opportunity to testify before the Energy and Commerce Subcommittee on Communications and Technology on "Leveraging Al to Enhance American Communications." Your interest in learning about the ways in which Palo Alto Networks leverages AI to dramatically improve cybersecurity outcomes was appreciated.

Enclosed are my responses to the additional questions for the record. Palo Alto Networks is proud to be an integrated national security partner of the federal government, and our strong working relationships with your office and the Energy & Commerce Committee are central to that. Please consider us an ongoing resource for any future questions, briefings, or hearings. We stand by to support your important work.

Sincerely,

Sam Rubin
Vice President – Global Operations, Unit 42
Palo Alto Networks

Questions for the Record

The Honorable Earl L. "Buddy" Carter:

1. **I am very interested in the capacity for AI to enable network defenders to discover vulnerabilities across their systems before adversaries exploit them. It's one thing to block attacks we've seen before. That's obviously important, but perhaps somewhat routine. How does AI help identify and block attack techniques that were previously unknown?**

   By leveraging AI-powered behavior threat prevention, we are able to identify never-before-seen attack patterns that have not previously been identified as malicious. In fact, every day Palo Alto Networks detects 1.5 million never-before seen new and unique attacks that weren't there the day before.

2. **In your testimony, you mention that Palo Alto Networks ingests 36 billion cyber events every day. Can you share who is predominantly conducting those attacks (i.e. domestic, international)?**

   Malicious cyber actors are widely distributed globally even though they often leverage virtual-private-networks (VPNs) to make it appear as though they are located in the United States. We see activity targeting our infrastructure from a variety of locations around the world.

The Honorable Randy Weber:

1. **How does your company use AI to harden your systems and implement safeguards including using "red-teaming?"**

   AI bolsters network defenders by identifying and eliminating attack surface exposure; maintaining cyber hygiene with automated real-time validation for critical vulnerabilities; applying the most current adversary techniques during penetration testing (e.g. red-teaming), tabletop exercises, and other risk assessments; and optimizing Security Operations Center outcomes.

   My team, Unit 42, assists organizations by enabling their security personnel to plan and execute drills that test their network monitoring and incident response processes using AI-powered tools. These drills include initial phishing simulations as well as the use of manual and automated techniques by Unit 42 to further exploit systems, elevate credentials, and move deeper into networks. Through such exercises, organizations receive tactical, action-oriented remediation steps to address the weaknesses, gaps, and vulnerabilities discovered during the engagement.

The Honorable Russ Fulcher:

1. **Mr. Rubin, can you give me an understanding of how well local power generators, utilities, and state cybersecurity offices communicate and coordinate when it comes to cybersecurity attacks that could cut off, surge, or otherwise disrupt the flow of power as it goes from generation to transmission, distribution, and to final consumption? You noted in your testimony that malicious cyber actors are using AI to "accelerate and scale attacks," along with hitting different operators with many more attacks to try and overwhelm them.**

   Close coordination and partnership between the federal government, state/local governments, and the critical infrastructure community is important for improving our overall collective defense. Electric utilities worldwide count on cutting-edge cybersecurity tools to prevent cyberattacks and safely modernize operational technology (OT) networks. Organizations and utilities should embrace AI-powered solutions to improve their visibility and response capabilities.

   We supported the establishment and implementation of the State Local Cybersecurity Grant Program (SLCGP), which serves as a forcing function in encouraging state-local collaboration and coordination. The program authorizes DHS, through CISA and FEMA, to award $1 billion in grant money over four-years to state and local governments and other eligible entities to address cybersecurity threats and risks to their IT networks and systems. To participate in the program, eligible jurisdictions must submit detailed cybersecurity plans to CISA, including details on a state's existing cybersecurity posture and how it would use funds to drive enhanced resilience, such as implementing threat mitigation practices and a continuous cybersecurity vulnerability assessments process. The SLCGP should enable jurisdictions across the U.S. to truly move the needle on improving their cybersecurity resilience.

2. **Mr. Rubin, you noted the importance of workforce development when it comes to cybersecurity. At Idaho National Labs for example, they mentioned dealing with a serious workforce shortage with the need to get more people in the cyber workforce pipeline. This is even though our universities and community colleges are actively participating with programs. Are there specific areas in need? Are there ways we can improve on attracting more students here?**

Palo Alto Networks prioritizes cybersecurity awareness and education so individuals of all ages and backgrounds have the tools to stay safe online. The cyber talent pipeline must receive high-caliber training that complements, withstands, and enhances the pace of tech innovation. Effective security automation can block most attacks without manual intervention and focus our most precious resource – people – on the most sophisticated attacks.

To that end, we believe policymakers should recognize that AI deployment and cybersecurity workforce investment are complementary activities. The cybersecurity jobs individuals are hired for today will not necessarily look the same in 5 or 10 years. There will be a greater demand for people to help defend networks as attack surfaces expand and the threat landscape changes. Someone who has AI-powered cybersecurity in their position will experience professional growth as the way they perform their jobs continues to evolve over time. We must continue to future-proof the cyber workforce by equipping individuals with the skill sets to navigate the evolving landscape of AI in cybersecurity.

Palo Alto Networks also believes cybersecurity companies should play a central role in providing cybersecurity training, education, and awareness. A particularly strong model is an industry-generated curriculum that is continually updated, mapped to NIST's National Initiative for Cybersecurity Education (NICE) standards, and delivered on a platform that is easily accessible to interested individuals. Coupled with instructor training and hands-on lab access, this curricula enables academic institutions with no legacy cybersecurity program to launch one in short order, ultimately broadening the talent pool exposed to cyber education.

Innovating with modular lessons and other engagements that can be facilitated by anyone, regardless of their knowledge level, offer further opportunity to scale the reach of cybersecurity awareness to local schools and communities. Age-appropriate activities that highlight the core concepts of AI, responsible connectivity, privacy, online communication, and digital citizenship allow youth to understand and explore their interest in cybersecurity. Fun, engaging cybersecurity competitions also drive deeper learning and are an important tool for students who learn differently, including at the K-12 level. Public-private partnerships should be encouraged to expand the reach of such opportunities, which ultimately generate greater interest and familiarity in STEM fields.

The Honorable August Pfluger:

It is no secret that in recent years, cyber-attacks have been on the rise, and since more people have become increasingly reliant on technology and digital services, financial data, medical records, and sensitive personal information have become more at risk than ever

before. Recently, the Pentagon released the 2023 Report to Congress on the Military and Security Developments Involving the People's Republic of China on how the CCP is willing to use its cyber capabilities, including Artificial Intelligence, against the United States. One example would include targeting critical infrastructure sectors such as energy, defense, and telecommunications to attack military mobility and economic productivity. What is your take on this analysis?

1. **How do you think the United States stacks up against China regarding cybersecurity and Artificial Intelligence?**

   China-linked cyber aggression is something Palo Alto Networks tracks closely. In fact, early this year, Palo Alto Networks was a named contributor to a Joint Cybersecurity Advisory analyzing the adversarial tactics of a China state-sponsored cyber actor called Volt Typhoon.

   More recently, our Unit 42 cyber threat intelligence team published research which identified malicious Chinese Advanced Persistent Threat (APT) infrastructure masquerading as cloud backup services actively compromising at least 24 Cambodian government organizations. Targeted entities included Cambodian national defense, election oversight, human rights, treasury and finance, commerce, politics, natural resources, and telecommunications activities. Unit 42 researchers also observed Chinese APT campaigns targeting entities in the South Pacific, including the Philippines government, by leveraging legitimate software to sideload malicious files and creatively configured the malware to impersonate legitimate traffic for command and control (C2) connections.

   We maintain close information sharing relationships with our partners at CISA, the FBI, the Intelligence Community, and other allied nations to share situational awareness about the global threat landscape. The continued maturation of this voluntary partnership model is an area of strength for the United States' cyber defense posture. Importantly, in these forums, commercial competitors act as threat intelligence partners – and our national security is better off as a result.

2. **Your testimony includes a very impressive statistic about Palo Alto Networks' ability to fundamentally transform security operations - processing 36 billion cyber events each day and triaging just eight of those for human analysis - all because of AI. Automating routine security activity while freeing up human analysis for more proactive analysis seems like the exact formula that we need to protect our national security. Is it safe to say this is the kind of automation we need to stay ahead of**

sophisticated adversaries like China and Russia? How does the future of Artificial Intelligence play into fighting back against China's strategy for cyber dominance?

Yes, these AI-powered cyber tools are absolutely what network defenders need to stay ahead of increasingly sophisticated adversaries. These tools act as a much-needed force multiplier in today's threat environment.

As adversaries like China and Russia become increasingly sophisticated, it is critical to arm network defenders with state-of-the-art automated capabilities to streamline security operations, correlate security data to accurately detect and stop threats at scale, and accelerate incident response and remediation efforts.

3. **Making sense of hundreds of billions of pieces of data every day obviously requires automation and AI – you and your competitors certainly don't have enough employees to do this vital work manually. How do we ensure any legislative or regulatory actions the Federal Government may take combats the use of AI and Machine Learning for malicious and illegal purposes without impeding the work you and other network security companies are doing to protect our country's digital resiliency?**

Cyber adversaries are leveraging AI to advance their tradecraft and will continue to do so, whether it is for generating social engineering attacks, accelerating and scaling other threats, or identifying new attack vectors. This sobering backdrop only heightens the importance of fully harnessing the substantial benefits AI offers for cybersecurity. The integration of AI into cyber defense capabilities provides defenders a more capable and nimble toolkit to analyze network telemetry – yielding powerful insights that guide deployment of protective measures. As policymakers consider guardrails governing the development and use of AI, a risk-based and stakeholder-involved approach will help minimize harms without stifling necessary innovation. We offer the following considerations for policymakers as we look to encourage the deployment of AI-powered solutions for cyber defense:

- Build upon flexible, risk-based frameworks such as the NIST AI Risk Management Framework.
- Focus on securing AI systems themselves.
- Differentiate between use cases, impacts, and data types when determining risk.
- Avoid unintended consequences in disclosure requirements.
- Recognize and promote cybersecurity as a privacy enabler.

4. **Modern Information Technology and networking are no longer defined exclusively by wired connections and static networks. I understand that AI and Machine**

Learning are vital to ensuring efficient 5G wireless connectivity and in creating and operating software-defined networks. How can we ensure that anything we do to regulate or legislate on AI or telecommunications doesn't interfere with these important networking functions and the availability of reliable and affordable IT and communications for the public?

One sector I care a lot about, the food and agriculture industry, has become more connected through technology and is more vulnerable to cyberattacks. This Congress, I introduced the Food and Agriculture Industry Cybersecurity Support Act, that would incentivize public-privacy collaboration in the agriculture sector to assist farmers and ranchers in securing their technology, equipment, and hardware. As we all know, the legislative branch rarely moves with the speed of relevancy, especially regarding technology.

AI-powered cyber defense tools are critical for ensuring the resilience of 5G and Next Generation wireless communications. In fact, Palo Alto Networks is now providing key security components in the nation's first cloud-native, open RAN-based 5G broadband network.

To continue this important work, we support risk-based approaches to developing AI guardrails that minimize harms without stifling needed innovation. Policies and frameworks need to ensure that organizations can nimbly leverage security data for defensive cybersecurity purposes. We urge policymakers to carefully consider the varied nature of AI use cases to ensure that any new guardrails or policies do not unintentionally inhibit the continued and expanded use of AI-powered tools for 5G security and cyber defense at large.

Palo Alto Networks appreciates your interest in promoting cybersecurity resilience across the Food and Agriculture Sector. A reality of today's threat landscape is that no sector is immune to cyber attacks, and we would welcome the opportunity to continue collaborating with your office on these issues.

5. **Can you talk about what legislative efforts this committee can take to better incentivize public-private coordination in cybersecurity now and into the future to keep up with the ever-changing world of cybersecurity? What other sectors should we focus on first?**

Palo Alto Networks commends the committee's commitment to exploring the role of AI across every sector of the economy. Cybersecurity attacks continue to grow in scale and complexity across all sectors, and I can confidently say that the risky outcome for society is *not* deploying AI for defensive cyber purposes. No sector is immune to cybersecurity vulnerabilities and threats, and AI-driven cyber defense tools will be critical to securing all sectors and organizations.

One historically "target rich, resource poor" sector where the committee might be well-served by promoting further investments is education institutions, particularly K-12 schools. Modernizing E-Rate or other FCC programs would help secure K-12 schools in delivering *and* maintaining connectivity to stay ahead of the constantly shifting threat landscape.

The Honorable Anna Eshoo:

1. **Your written testimony discusses how artificial intelligence (AI) has been deployed extensively in the cybersecurity arena. You discuss how it has been leveraged by cyber adversaries to enhance social engineering attacks, accelerating and scaling attacks, and finding new attack vectors. You also discuss how AI is a "game changer" to help cyber defenses ward off cyber-attacks by helping them anticipate, track, and thwart attacks on an unprecedented scale.**

   For the record, what should Congress be doing to encourage innovation and adoption of AI for cybersecurity defenses? What approach should Congress take to regulation to ensure innovation and adoption of AI for cybersecurity defenses is not stifled?

   We believe policymakers should employ a risk-based approach when considering AI guardrails that takes into account differences in the use cases, the data processed in those use cases, and the potential resulting impacts on individuals. There are fundamental differences in risk between AI systems that, for example, leverage consumer data to make or facilitate decisions with consequential impact on individuals, as compared with those that leverage security data to ensure the robustness and resilience of networks. When AI is used to make decisions about credit, housing, employment, health care, or insurance, for example, those decisions have a significant impact on individuals. By contrast, when AI is deployed to enable cybersecurity tools to stitch together security data much more quickly and effectively than before, the result is that society as a whole is better protected and all individuals benefit.

   We urge policymakers to carefully consider the varied nature of AI use cases to ensure that any new guardrails do not unintentionally inhibit the continued and expanded use of AI-powered tools for cyber defense.

<u>The Honorable Lizzie Fletcher</u>:

1. **What would you recommend we be thinking about when it comes to fashioning digital privacy legislation in the context of AI? When we are thinking about how to put together a framework, what are the AI considerations that we should be taking into account in that process?**

   As a cybersecurity leader, we see the fundamental role that AI-powered cybersecurity plays in protecting data privacy on a daily basis. Palo Alto Networks believes any federal privacy standard must appropriately recognize that to avoid unintended consequences in global cyber defense. We encourage the Committee to develop a framework that:

   1. Provides clear and consistent requirements and expectations for individuals and businesses;
   2. Recognizes the use of security data for legitimate business purposes, such as cybersecurity;
   3. Fosters innovation by focusing on decisions with consequential impact on individuals; and
   4. Encourages the use of automation in data security.