STATEMENT FOR THE RECORD OF

STEVEN GROBMAN, INTEL FELLOW & CHIEF TECHNOLOGY OFFICER, INTEL SECURITY GROUP

BEFORE THE UNITED STATES SENATE COMMERCE COMMITTEE

ON THE PROMISES AND PERILS OF EMERGING TECHNOLOGIES FOR CYBERSECURITY

March 22, 2017 10:00 AM

Good morning, Chairman Thune, Ranking Member Nelson, and members of the Committee. Thank you for the opportunity to testify today. I am Steve Grobman, Intel Fellow and Chief Technology Officer, Intel Security Group, part of Intel Corporation.

I am pleased to address the Committee on how emerging fields like Artificial Intelligence (AI), Internet of Things (IoT), quantum computing, and Blockchain not only create tremendous value for American citizens, but also present new opportunities for both attackers and defenders in the field of cybersecurity. My testimony will address Intel and Intel Security's commitment to cybersecurity and the state of the above emerging technologies. I will conclude with some policy recommendations.

First, I would like to provide some background on my experience and Intel's commitment to cybersecurity. I am the Intel Security Group Chief Technology Officer (CTO), responsible for leading technical innovation and thought leadership related to cybersecurity at Intel. I have been focused on the field of cybersecurity for over two decades in a wide range of positions.

INTEL SECURITY'S COMMITMENT TO CYBERSECURITY

Intel is a global leader in computing innovation, designing and building the essential foundational technologies that support the world's computing devices. Combining Intel's decades-long computing design and manufacturing experience with Intel Security's market-leading cybersecurity solutions, Intel Security brings a unique understanding of the cybersecurity challenges threatening our nation's digital infrastructure and global e-commerce. Governments, businesses and consumers face a cybersecurity threat landscape that is constantly evolving with each new technology that is brought to market at a faster pace than ever before. The sharp rise of internet-enabled devices (known as "Internet of Things" or "IoT") in government, industry and the home exacerbates this already difficult challenge. The increasing advancement of artificial intelligence provides real promise for society but at the same time provides a tool for malicious actors as well. Emerging areas such as quantum computing have repercussions we need to be addressing now, and blockchain is a strong technology that can be used to solve fundamental problems in security such as trusting a central authority. The challenges we face are too significant for one company or entity to address on its own. Real change in cybersecurity requires a true public-private partnership with industry.

Collaboration will be the driving force behind what soon will be the new McAfee (currently known as Intel Security) — planned to be a standalone company this year. It's also why we recently announced a whole new ecosystem of integrated platforms, automated workflows and

orchestrated systems based on an open communications fabric that will enable all of us in cybersecurity to work together in ways never before thought possible.

Emerging Technological Areas of Value and Concern

With every advancement in technology, new challenges are introduced. The mass adoption of automobiles and air travel fundamentally transformed every element of life in the 20th century, yet these innovations also caused us to look at new concerns and challenges related to auto and air safety. The technologies we will discuss today are very similar. Technologies related to the Internet of Things, artificial intelligence, quantum computing and blockchain are foundational technologies with the potential to improve health, cure disease and add new levels of automation and efficiency to our economy and everyday life. These same building blocks will be valuable tools to both offensive and defensive participants in the cybersecurity domain. This discussion will focus on how these capabilities are pivotal to building new security defensive architectures, but also examine what we need to recognize related to new threats and risks the technologies facilitate.

Internet of Things (IoT)

The combination of Moore's law[1] and pervasive connectivity have lowered the barrier of entry in building and enabling "smart and connected" devices in almost every aspect of business and consumer life in America. Collectively we are referring to these devices as the "Internet of Things," or IoT.

IoT is defined as endpoint devices such as cars, machinery or household appliances that connect to the internet and generate data that can be analyzed to extract valuable information. There are three sub-definitions emerging out of the IoT space; however, all three definitions overlap. The "Mobile IoT" comprises devices like cars, wearables, sensors and mobile phones, which all connect directly through broadband wireless networks. The "Industrial IoT" connects devices in industrial environments like factory equipment, security cameras, medical devices and digital signs. These devices are able to connect to the internet and into the datacenter (cloud) through an industrial "gateway."[2] Finally, the "Home IoT" connects devices like game consoles, smart TVs, home security systems, household appliances and thermostats through a gateway to the internet.

IoT presents staggering economic opportunities for the U.S. and the world. Market research firm IDC estimates there will be 50 billion connected devices in the marketplace by 2020[3], and Morgan Stanley forecasts 75 billion in that same time period.[4] These estimates would equate to

---

[1] In 1965, Gordon Moore, one of Intel's co-founders, made a prediction that would set the pace for our modern digital revolution. From careful observation of an emerging trend, Moore extrapolated that computing would dramatically increase in power, and decrease in relative cost, at an exponential pace – from 50 Years of Moore's Law Intel article -- http://www.intel.com/content/www/us/en/silicon-innovations/moores-law-technology.html

[2] A gateway is a node on a network that serves as an entrance to another network.

[3] Business Strategy: The Coming of Age of the "Internet of Things" in Government, IDC (April 2013), http://www.idc.com/getdoc.jsp?containerId=GIGM01V

[4] Morgan Stanley: 75 Billion Devices Will Be Connected To The Internet Of Things By 2020, Business Insider (Oct.2 2013) http://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013-10

six to 10 connected devices for every person on earth. Whether the exact number of devices is 50 billion, 75 billion or something more, one thing is for certain: The number of connected devices will explode in the next five years. In just the automotive industry alone, it is projected that 250 million (or one in five) cars worldwide will be connected to the internet by 2020 – via technologies like LTE, satellite and 5G communications networks.[5] To put this in perspective, there were roughly 250 million cars on U.S. roads in 2013.[6]

This explosion of devices and technological revolution that is IoT is projected to have a staggering positive impact on the U.S. and global economy. McKinsey projects IoT will have a $2.7 trillion to $6.2 trillion global economic impact by 2025.[7] And what should most excite U.S. policymakers is that the U.S. and other developed economies are expected to capture a remarkable 70 percent of this economic impact, if we develop a leadership position.

On the other hand, with the growth of IoT, we are rapidly approaching 50 billion connected devices (with varying degrees of security) that are becoming more and more valuable to attackers. We have already seen the beginnings of this trend, as cyberattacks against physical assets – from cars to electric power stations – move from science fiction to reality.

It is critical to recognize why IoT devices are interesting targets for a cyber attacker. Incentives may range from a cybercriminal monetizing an attack by holding a manufacturing facility for ransom or a terrorist or nation-state actor executing an attack on critical infrastructure or business assets to harm the US economy or cause loss of life. As we will see, a key incentive for the bad actor may be to expand the attack infrastructure and weaponry they have at their disposal.

One of the major issues in consumer IoT is weak market incentives to drive manufacturers to build strong architectures, as the consumer buying the device currently places little value on security, especially with tight margins in the consumer IoT industries. More worrisome is that manufacturers generally don't maintain the security of a device throughout its entire practical life. Although a smart TV or thermostat may have a three-year warranty, the device will likely function for many years beyond that. If security vulnerabilities are identified in year five, is the manufacturer compelled to release a fix? What about manufacturers that no longer exist? With the rate and pace of the creation of smart and connected devices, it is inevitable there will be millions of vulnerable orphaned devices that will be ripe for exploitation.

One thing critical to understand is that this is not just a consumer problem. One of the questions I'm often asked is why someone should care if their light bulb is hacked. What data are they really going to steal? And the thing is, they're not going to steal data. That's not the concern. The concern is weaponizing that lightbulb to become part of the larger attack

---

[5] Gartner Says By 2020, a Quarter Billion Connected Vehicles Will Enable New In-Vehicle Services and Automated Driving Capabilities, Gartner Inc. (Jan. 26, 2015), http://www.gartner.com/newsroom/id/2970017.

[6] Average Age of Vehicles on the Road Remains Steady at 11.4 years, According to IHS Automotive, IHS (June 2014) (253M cars on US roads in 2013), http://news.ihsmarkit.com/press-release/automotive/average-age-vehicles-road-remains-steady-114-years-according-ihs-automotive.

[7] Disruptive Technologies: Advances that will transform life, business, and the global economy, McKinsey Global Institute (May 2013), http://www.mckinsey.com/insights/business_technology/disruptive_technologies.

scenario. And that attack scenario can impact infrastructure, it can impact organizations and it can impact companies. The impact of insecure consumer devices is an issue that needs to be comprehended well beyond just the consumer who purchased the device.

This is exactly what we saw in October 2016 with the Mirai attack. You may also hear it called the Dyn attack because it was targeting the Dyn DNS infrastructure. Mirai was a botnet that spread by finding generally inexpensive internet-connected consumer devices. These devices didn't have traditional vulnerabilities; they were vulnerable because the manufacturers had left integrated privileged accounts with weak passwords. The botnet grew by having compromised devices play two roles. They would search for other vulnerable devices and "recruit" them to join the botnet as well as check in with a command and control infrastructure to see if there were any attack actions they needed to take. The attackers who launched this attack issued a set of commands that flooded the Dyn infrastructure, resulting in major technology sites falling off-line for the better part of a day. The attackers could use this infrastructure to attack any organization, and we should think of the October incident as merely the beginning of this type of scenario.

To prove this out, my team ran a test in January, months after this attack. The experiment consisted of placing a simulated vulnerable device on an open network to see how long it would take a device to get compromised by this botnet. Literally at the one minute, six second mark, it was exploited. If this were a real device it would now be part of the broader botnet infrastructure.

When we think about attack scenarios it comes down to understanding one thing – risk. Security upgradability and patching are critical. Vendors need to design these critical capabilities into the products they offer to consumers. They also need a plan to deal with critical security vulnerabilities discovered even after devices are out of warranty. We also need to raise consumer awareness so that buying decisions have people consider security the way they think about other things today (e.g., is this device from a reputable manufacturer? How long will it last?, What is the warranty?).

There are a number of technologies and approaches to device initiation and on-boarding that Intel, its partners and customers are working on. We look forward to working with organizations like NIST to standardize where appropriate. However, the issue of legacy devices is more difficult to resolve, especially since it is likely in the hands of consumers to address.

Artificial Intelligence

Artificial intelligence (AI) comprises a broad field of technology that is enabling everything from our search engines to future self-driving cars and everything in between. It is important to think of AI as a set of technologies as opposed to one thing. Just as with every other technology in computer science, the attacker and defender communities analyze how AI can be used to enhance the capabilities of their solutions.

Attackers are using capabilities in AI to perform a wide range of tasks. AI can be used to automate capabilities that formerly required human analysis for high levels of effectiveness.

For example, in spear-phishing the attacker's objective is to craft a message that the victim will trust or interact with. AI also can be used to build customized content automatically for a specific user based on content found within their social media information or other feeds. This customized content has a much higher success rate than a generic phishing interaction that is not user specific. Additionally, in the past the attacker had to choose between sending a high-volume of low-quality phishing interactions or a low volume of high-quality interactions that were crafted by a human. AI allows the attacker to have the best of both – a high quality phishing interaction that can be sent to a large number of users.

Another area where AI is an asset to cyber attackers is in victim selection. One capability AI is very well suited for is classification and scoring based on input data. One use case would be determining which of a set of potential targets or environments would be viable to breach. Attackers can train their data based on attributes about their environments and the effectiveness of past attacks and then focus their efforts where they will attain the highest return on their efforts and investment.

By the same token, the characteristics of AI make it a powerful tool in defensive tools and technologies for the cybersecurity industry. A large portion of a defender's job is processing massive quantities of data within an organization and identifying threats. There are also many elements in cybersecurity that are ultimately classification problems: Is a file malicious? Is behavior malicious? Is a user acting differently than the tasks they normally perform? All of these questions require data inputs, analysis and a predictive conclusion. AI has numerous classification capabilities and algorithms that make it a perfect tool for these sorts of tasks. For example, Intel Security has recently launched products such as our RealProtect technology[8] that can analyze both the structure and behavior of an application using AI techniques to classify it as malicious or benign.

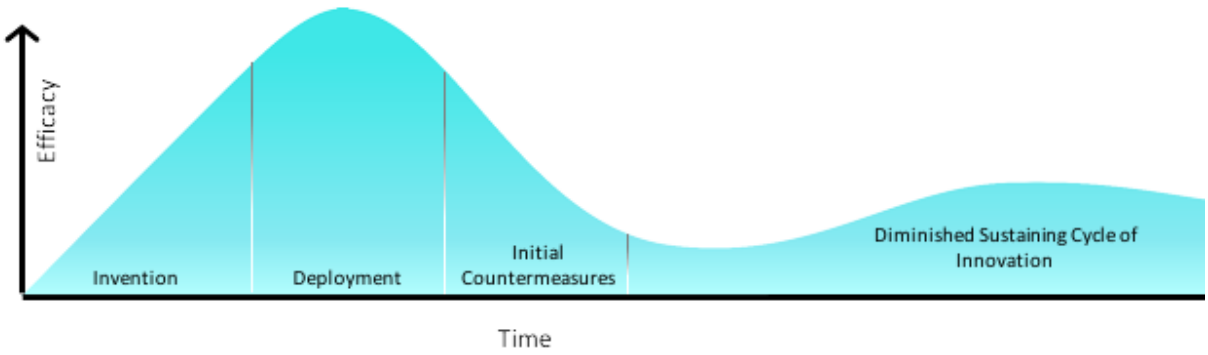
We do need to be mindful that our current state of the art in AI and analytics capabilities have limits, both in the field of cybersecurity as well as in other fields. Simply having massive quantities of data does not necessarily mean there is an underlying signal that can be teased out by an algorithm. We have radically improved how we do analytics on hurricane forecasting. For example, three days before a hurricane makes landfall we can predict where it will land to roughly 100 miles of accuracy, whereas 25 years ago, we could predict accuracy only to 350 miles.[9] Yet, although we have massive quantities of seismic data, we have not yet found a way to reliably predict that a major earthquake is about to occur. The same issue occurs in cybersecurity; sometimes there is not a way to detect a threat based on the data available.

There is one element of AI in cybersecurity that separates it significantly from AI in other fields. In cybersecurity, there is a human bad actor who creates evasion tactics and countermeasures with the intent to have the algorithm fail. We don't have this issue in other forms of goal-based

[8] https://www.mcafee.com/us/resources/white-papers/wp-real-protect-dynamic-application-containment.pdf
[9] https://en.wikipedia.org/wiki/The_Signal_and_the_Noise

analytics (e.g., water doesn't choose to change the way it evaporates as we get better at hurricane forecasting).

In addition, in cybersecurity we see a trend where every new defensive technology loses effectiveness once deployment in the market drives adversaries to build countermeasures and evasion tactics. The cycle looks like this:



As we are on the leading edge of the deployment curve with many of the industry AI-based solutions, it is critical to use forethought into how bad actors will work to circumvent AI-based capabilities. Examples of techniques we are analyzing and tracking include machine learning poisoning and forcing defenders to recalibrate models or raise the noise floor. In the field of cybersecurity defense there is never a silver bullet defense, but rather a constant pipeline of innovation for both the attacker and defender.

Blockchain

Blockchains have gained a lot of attention as they provide key benefits across a wide range of applications. Blockchains first emerged as the technology behind the cryptocurrency Bitcoin. Blockchains, however, have much broader use cases, including identity management, marketplaces and supply chain management. The potential of the technology is considered disruptive and has been described as potentially impacting transactions in the same way the Internet affected communications.

Blockchain makes use of cryptographically supported immutable ledger and distributed consensus protocols to facilitate the exchange of assets between two untrusted parties, eliminating the need for intermediaries. Any networked ecosystem with a central authority for transaction authorization could potentially use a blockchain in the future as a replacement. In more detail, blockchain ensures the integrity of the ledger. It is an immutable series of transactions shared by all participants in the ledger. Cryptographic signatures ensure correctness and guarantee "non-repudiation" (that is, once a transaction is committed to the blockchain, it cannot be un-committed). Distributed consensus algorithms ensure all participants see the same series of transactions even if bad actors try to compromise the system.

Blockchain technologies can provide a significant contribution to the improvement of efficiency and integrity in transactions in a variety of areas, including finance and healthcare. In addition, elements of blockchain technologies have been tested in a variety of use cases and contexts, including e-government and health data protection, notary services, supply chain; secure contracting and document delivery; identity; real estate systems, and many more. In order to ensure successful incorporation of blockchain in various technology ecosystems, it is necessary to improve reliability, scalability, security and privacy.

These goals cannot be achieved without the support of the features in hardware. Intel has been paying close attention to the developments in blockchain. Intel is developing products for blockchain and participating in blockchain ecosystem development via a number of initiatives, including the Linux Foundation's Hyperledger[10], the Ethereum Enterprise Alliance and an Intel's open source distributed ledger[11]. Intel is testing its open source distributed ledger in proof-of-concept (POC) environments in partnership with various external companies to improve the integrity and applicability of the technology. Intel's focus has been on developing hardware functionality that will make it possible to operate blockchains on a commercial scale with greater security and support for privacy, thus creating promise for commercial deployment in several segments.

While the core capabilities of blockchain add tremendous efficiency and de-centralized authorization of transactions, these same properties, like many other innovations, have also been used for nefarious purposes. Blockchain enabled crypto-currencies, such as Bitcoin, are the preferred financial instrument of cybercriminals focused on executing ransomware. Ransomware is an efficient cybercrime in which criminals are paid directly by the victim. From the cybercriminal's perspective, there is no need to digitally fence stolen data or worry about data becoming devalued (such as stolen credit card numbers being canceled).

A typical ransomware scenario occurs when a cybercriminal gains access to a victim's (individual or organization) system and encrypts data that has value to the victim. The victim is then informed that their data is being cryptographically held hostage, and if they want their data back, they must pay a ransom. Ransom is typically paid in cryptocurrency based on blockchain, such as bitcoin, as it is easy to move the funds multiple times and difficult to map the underlying holder of a bitcoin wallet to a true individual. Ironically, market forces encourage cybercriminals to uphold their end of the bargain and typically do provide keys after payment to uphold the reputation of the ransomware model. Ransomware became practical when the usability of cryptocurrencies reached a level that victims were technically competent enough to use the system to make a payment.

---

[10] https://www.hyperledger.org/

[11] http://intelledger.github.io/0.8/

We see an interesting phenomenon in ransomware in that cybercriminals appear to be moving to harder targets as profit pools dry up on soft targets. Ransomware started by targeting consumers, then moved to soft target organizations such as hospitals, police stations and universities. We now see ransomware impacting corporations and organizations. This is a worrisome trend in that critical infrastructure now presents incentives to not only be targeted by terrorists and nation-states, but also by cybercriminals. Nation states are cautious about actively attacking critical infrastructure as an attributed response could cause an undesirable reciprocal response. As it becomes more difficult to monetize consumers and organizations, cyber criminals could see a path to hold power, water or other critical systems for ransom by demanding payment by the government. We should understand these scenarios and work to understand potential policy impacts and coordinated responses prior to these scenarios playing out.

Quantum Computing

Quantum computing is a form of computing that relies on the principles of quantum physics to solve specialized classes of mathematical problems that are not practical to solve on traditional computers. Quantum computers use quantum bits (qubits), unlike digital computers, which are based on transistors and require data to be encoded into binary digits (bits). These qubits can exist in multiple states simultaneously, offering the potential to compute a large number of calculations in parallel, speeding time to resolution.

It should be noted that quantum computers will not replace traditional computers, as they are only effective on certain classes of problems, and in many cases perform worse than traditional computing. However, quantum computing holds the promise of solving complex problems that are practically insurmountable today, including intricate simulations such as large-scale financial analysis and more effective drug development. It is an area of research Intel has been exploring because it has the potential to augment the capabilities of tomorrow's high performance computers.

Another type of mathematical task that quantum computers are uniquely qualified to focus on relates to being able to break certain cryptographic algorithms. Today, data protection relies on a set of algorithms that secures everything from web connections to critical data stored or transferred in organizations or governments around the world. Some of these algorithms are called "quantum safe," meaning the mathematics of the algorithm are not subject to attack by a quantum architecture. An example of a quantum safe algorithm is the symmetric AES algorithm used for bulk data encryption. Algorithms that are "quantum unsafe" have properties that would create high levels of risk that a future quantum architecture could break the encryption. An example of a quantum un-safe algorithm is the public key algorithm RSA. Unfortunately, most encryption uses these algorithms in combination, and being able to break either one places data at risk.

One might ask why we need to think about this now if the ability to have a practical quantum computer is still years off. The reason is that encrypted data today can be "put on the shelf" by enemy nations and bad actors who will wait for the technology to mature. We must start to

ask, “how long must data remain secure or secret?” If the answer is one or two years, we are fine using current algorithms. For data that must be kept secret for decades or longer, now is the time to start the transition to quantum safe algorithms.

No one company or organization will succeed alone in unlocking the path to advanced quantum computing. Instead, partnerships – such as the one between Intel and the QuTech institute in Delft, The Netherlands – in addition to industry collaboration will help realize the promise of such a technically complex issue.

Quantum computing is promising, but there are significant challenges to overcome. It is a subatomic scenario that requires suspending conventional wisdom around basic physics, where an electron can actually be two places at once, spinning clockwise and counterclockwise at the same time. This ambiguity is both promising and enormously complex – and of course, an incredibly exciting challenge to anyone who loves physics, as many at Intel do. How do we connect thousands of quantum bits, or qubits, together? How can we control them? How can we reliably fabricate, connect and control many more qubits? Even measuring qubit signals is going to require an entirely new class of low temperature electronics that don’t exist today.

This research is on the cutting edge of silicon, architecture and software. As Intel’s entire history has been built on driving innovations in the very leading edge of all three of these, we’re excited about the role that our and other great minds can play in shaping this technology – which has the potential to shape the world for the better and solve problems we cannot solve today.

Policy Recommendations

Be wary of hard regulations – In cybersecurity the threat landscape changes very rapidly. The threat we deem the most serious today may not be the most important tomorrow. If regulation were to force manufacturers to guard against today’s threats, tomorrow’s might very well slip through the cracks. Additionally, if the government were to impose technology mandates, the result would likely be mere compliance rather than true security. Regulating in an area like cybersecurity is very tricky, and the unintended consequences could outweigh any benefits of the regulation.

Encourage public-private collaborations – It is far better for policymakers to collaborate with the private sector on a voluntary basis to develop risk-based, flexible frameworks to enhance the security of emerging technologies. A best-in-class example is the Framework for Improving Critical Infrastructure Cybersecurity, known as the NIST Cybersecurity Framework. It is widely acknowledged as a highly successful model of public-private collaboration that is being adopted by government agencies and critical infrastructure companies. The NIST approach succeeded because policymakers and the private sector defined a real need, improving the security of critical infrastructures; the process was open, NIST listened to the private sector, built trust with key stakeholders; and the final product, a flexible framework, was based on voluntary

collaboration, not rigid regulations. Policymakers should keep in mind the recent successes of the NIST framework as a positive way to get to their desired outcome.

Implement Security and Privacy By Design – In addition to partnering with the private sector to develop and adopt flexible, voluntary security frameworks, policymakers should likewise champion the principle of security and privacy by design to help incent broad adoption by the key parts of the IoT, AI and quantum computing ecosystem. Proper protection of individual privacy in products does not just happen. It needs to be designed and engineered in from the beginning of the product development process. Security by design also means designing security in right from the start. Adding or 'bolting on' security features to a system, network or device after it's already up and running has inherent weaknesses and inefficiencies. IoT is a great example where security and privacy protections need to be designed in from the start. Attributes such as location, activities, health monitoring, finance, etc. need protection from access and disclosure unless granted by the owner. AI applications need an architecture from the beginning that allows access to high valued data while protecting the private information it may be based upon. The use of AI for genetic medical research is an example where privacy considerations are critical to both protecting patients' privacy, while allowing researchers' access to valuable data for them to validate hypothesizes.

Cybersecurity and privacy must be built into the innovative equipment, systems and networks at the very start of the design and manufacturing process. Both privacy and security must be intrinsic to a product development organization's thought processes, its business processes, and its design, development, and manufacturing processes. Both privacy and security must be embedded in a product or network element so they become integral parts of the product's or element's functioning. This approach is not only more effective; it is less cumbersome and less expensive than trying to lock down systems that are leaking personal information or are inherently insecure.

Revise Vulnerabilities Equities Process – As with all technologies and more so with emerging technologies, vulnerabilities will arise that need to be corrected to assure proper operation of the solution, assuring its safety and security. The issue of vulnerability disclosure has been a subject of debate for some time. Currently there are concerns about how the U.S. government deals with zero-day vulnerabilities that its agencies, and those acting on its behalf, discover. The government should revise its vulnerability equities review and disclosure policies to allow greater transparency on how the government is implementing the vulnerabilities equities process. A revised policy would do much to enhance trust in the IT eco-system, something particularly important in the context of the emerging technologies we have been discussing today.

Conclusion

It has been an honor to testify before such a distinguished panel of legislators. We face a cybersecurity threat landscape that is constantly evolving with each new technology that is brought to market at a faster pace than ever before. Rapid advances in hardware and software

are creating new categories of innovative technologies such as the Internet of Things, artificial intelligence, quantum computing, and blockchain algorithms.

All of these innovative technologies merit attention from policymakers given their potential to solve complex problems, grow new markets and create high wage jobs. At the same time, these innovations can also create new security challenges and opportunities that need to be addressed in a thoughtful, prudent manner. Toward that end, we encourage policymakers to partner with the private sector to develop flexible, voluntary and market-based solutions, rather using regulatory models to address the challenges of emerging, innovative technologies. Policymakers are in a position to incent the ecosystem of emerging technology providers to adhere to the principle of security by design. By working together, policymakers and the private sector can harness the benefits of innovation while also addressing its challenges.