This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

RPTR BRYANT

EDTR ZAMORA

UNDERSTANDING THE ROLE OF CONNECTED DEVICES IN RECENT CYBER ATTACKS

WEDNESDAY, NOVEMBER 16, 2016

House of Representatives,

Subcommittee on Communications

and Technology,

Joint with

Subcommittee on Commerce, Manufacturing, and Trade,

Committee on Energy and Commerce,

Washington, D.C.

The subcommittee met, pursuant to notice, at 10:05 a.m., in Room 2175, Rayburn House Office Building, Hon. Greg Walden [chairman of the subcommittee] presiding.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Present: Representatives Lance, Latta, Barton, Shimkus, Blackburn, Guthrie, Olson, Kinzinger, Bilirakis, Johnson, Long, Ellmers, Brooks, Mullin, Collins, Pallone (ex officio), Schakowsky, Eshoo, Rush, DeGette, Matsui, McNerney, Welch, Lujan, Loebsack, Kennedy, Burgess, and Walden.

Staff Present: Grace Appelbe, Staff Assistant; James Decker, Policy Coordinator, Commerce, Manufacturing and Trade; Paige Decker, Executive Assistant; Graham Dufault, Counsel, Commerce, Manufacturing, and Trade; Blair Ellis, Digital Coordinator/Press Secretary; Melissa Froelich, Counsel, Commerce, Manufacturing, and Trade; Gene Fullano, Detailee, Telecom; Giulia Giannangeli, Legislative Clerk, Commerce, Manufacturing, and Trade, Energy and Power; A.T. Johnston, Senior Policy Advisor; Grace Koh, Counsel, Telecom; Paul Nagle, Chief Counsel, Commerce, Manufacturing, and Trade; Dan Schneider, Press Secretary; Olivia Trusty, Professional Staff, Commerce, Manufacturing, and Trade; Gregory Watson, Legislative Clerk, Communications and Technology; Jessica Wilkerson, Professional Staff, Oversight and Investigations; Michelle Ash, Minority Chief Counsel, Commerce, Manufacturing, and Trade; Jeff Carroll, Minority Staff Director; David Goldman, Minority Chief Counsel, Communications and Technology; Lisa Goldman, Minority Counsel; Elizabeth Letter, Minority Professional Staff Member; Jerry Leverich, Minority Counsel; Lori Maarbjerg, Minority FCC Detailee; Dan Miller, Minority Staff

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Assistant; Caroline Paris-Behr, Minority Policy Analyst; Matt Schumacher, Minority Press Assistant; and Ryan Skukowski, Minority Senior Policy Analyst

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Mr. Walden. I will call to order the Subcommittee on Communications and Technology in our joint committee hearing with the Subcommittee on Commerce, Manufacturing, and Trade.

Good morning, everyone. I will start with opening statements for our side and for our subcommittee, and then I think we go back and forth. So we will work this out.

I want to thank the two subcommittees for coming together on this very important topic that I think we all share a deep concern about.

We live in a world that is increasingly connected. Our smartphones are now capable of locking and unlocking our front doors at home, turning on lights, checking the camera for packages left on the doorstep. We are able to measure our steps, check our baby monitors, record our favorite programs from wherever we have connectivity. We will soon be able to communicate -- or excuse me. We can communicate with our offices too, but commute to our offices in driverless cars, trains, buses, have our child's blood sugar checked remotely, and divert important energy resources from town to town efficiently.

These are incredible potentially life-saving benefits that our society is learning to embrace, but we are also learning that these innovations do not come without a cost. In fact, recently we encountered a denial of service attack on a scale never before seen. This attack effectively blocked access to popular sites like Netflix

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

and Twitter by weaponizing unsecured network connected devices like cameras and DVRs. Once these devices came under the command and control of bad actors, they were used to send a flood of DNS requests that ultimately rendered the DNS servers ineffective. As I understand it, at the beginning of this attack it was virtually impossible to distinguish malicious traffic from other normal traffic, making it particularly difficult to mitigate against attack.

So how do we make ourselves more secure without sacrificing the benefits of innovation and technological advances? A knee-jerk reaction might be to regulate the Internet of things. And while I am not taking a certain level of regulation off the table, the question is whether we need a more holistic approach. The United States cannot regulate the world. Standards applied to American-designed, American-manufactured, American-sold devices won't necessarily capture the millions of devices purchased by the billions of people around the world, so the vulnerabilities might remain.

Any sustainable and effective solution will require input from all members of the ecosystem of the so-called Internet of things. We will need a concerted effort to improve not only device security, but also coordinate network security and improve the relationships between industry and security researchers. We are all in this thing together and industry, government, researchers, and consumers will need to take responsibility for securing this Internet of things.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

So today we will hear from a very distinguished panel of witnesses on some of the approaches that can be brought to bear on this challenge. My hope is that this hearing will help to sustain and accelerate conversations on our collective security and foster the innovation that makes the Internet the greatest engine of communications and commerce the world has ever seen.

So I thank our witnesses for being here. We appreciate your willingness to come and share your expertise. It is very helpful in our endeavors, and I look forward to your testimony.

At this time, I would yield to Mrs. Blackburn for an opening statement.

[The prepared statement of Mr. Walden follows:]

******** COMMITTEE INSERT ********

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Mrs. Blackburn. Thank you, Mr. Chairman.

And I also want to welcome our witnesses, and we appreciate your time. You know, we did an Internet of things hearing in March 2015, and at that point I talked a lot about the convenience that this brings to us in our daily lives and about the opportunities that it will open for us. I think now as we look at it, as the chairman said, you look at the cost, you look at the maximized use that exists. I think that by 2020, the expectation is 3.4 billion devices that would be in this universe of connected. That means we have vulnerabilities that exist, entry points, and we will want to discuss some of those vulnerabilities with you today, get your insight, and see how we as policymakers work with this wonderfully exciting, innovative area in order to make certain that Americans have access, but they also know that there is, as the chairman said, security as we approach this.

And with that, Mr. Chairman, I yield back.

[The prepared statement of Mrs. Blackburn follows:]

******** COMMITTEE INSERT ********

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Mr. Walden. The gentlelady yields back the balance of her time. I will yield back the balance of my time as well.

We will now turn to my friend from California, the gentlelady, Ms. Eshoo, for opening comments.

Ms. Eshoo. Thank you, Mr. Chairman.

First of all, I want to express our collective thanks from this side of the aisle to you for responding to our request to have this hearing. Mr. Pallone, Mr. McNerney, Ms. Schakowsky, Ms. DeGette, and myself all made the request, and we are grateful to you for holding the hearing, because we think that this is, obviously, a very large issue and something that concerns the American people.

In fact, Americans are connecting more devices to the Internet than ever before. Most of us carry at least one in our pocket, but as technology evolves, we are seeing a proliferation of everyday items and appliances that connect online. This is good. Today, everything from washing machines to light bulbs are now capable of connecting to the Internet. The business world also relies more and more on the Internet, in fact, Internet-enabled objects, to drive their efficiencies to produce lower cost.

There are as many as 6.4 billion -- billion with a B -- Internet of things products in use worldwide just this year. The growth in this market is expected to be significant, including estimates of over 20 billion Internet-enabled products connected worldwide by 2020. So

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

this is not a small market. It makes it a very large issue. It is an economic one, and we don't want to damage that, but it is something that needs our attention.

There is great potential for innovation as more devices become connected, but there is also the potential for serious risk if they are not properly secured. That is really what we are pursuing here. We need to look no further than the major attack on October 21st that crippled some of the most popular Web sites and services in our country. The distributed denial of service attack against Dynamic Network Services, known as Dyn, was made possible by unsecure Internet of things devices that attackers were able to infect with malware. This army of devices was then harnessed by the attackers to bring down Dyn's servers. Similar attacks in October targeted a journalist and a French card services provider.

These attacks raise troubling questions about the security of Internet-enabled devices and their potential to be used as weapons by cyber attackers. For example, it has been reported that some devices used in these attacks may have lacked the functionality to allow users to change the default username and password. We already know that an important way to prevent cyber attacks is to practice good cyber hygiene, which includes changing default usernames and passwords. When products lacking the commonsense functionality are manufactured, shipped, and eventually connected, they put users and the Internet as

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

a whole at risk. So it seems to me that this is an area that we need to explore with our witnesses.

There is also the issue of how long these unsecured devices can remain in use. The Dyn attack reportedly used infected devices that were first manufactured as early as 2004. Manufacturers may no longer update products that have been in use for so long, further exposing users and the Internet to security risks.

Finally, we have to recognize that this is a global issue. Level 3 Communications estimates that a little more than a quarter of these devices infected with the malware that was used in the Dyn attacks are located in the United States. One of the major manufacturer of products that appear to be particularly vulnerable is based in China. This is important to keep in mind as we explore how to address this problem going forward.

So this hearing, I think, is a very important step in helping us, first of all, to all understand what lessons we should take away from these recent attacks. The Internet of things offers exciting possibilities for innovation, but we can't afford to ignore the risks that come when devices are designed without security.

Whatever the ultimate solution is, I think industry must play a central role in the effort to address these issues, and I look forward to hearing from our witnesses today. You play a very important role in this.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

So, with that, thank you again, Mr. Chairman, for allowing this hearing to take place, and I yield back the balance of my time.

[The prepared statement of Ms. Eshoo follows:]

******** COMMITTEE INSERT ********

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Mr. Walden. The gentlelady yields back the balance of her time.

The chair now recognizes the gentleman from Texas, Dr. Chairman Burgess.

Mr. Burgess. Thank you, Mr. Chairman. And good morning to our witness panel today. Thank you, Mr. Chairman, for holding the hearing and allowing us to have this discussion about the recent cyber attacks.

Several popular Web sites were knocked offline for several hours on October 21 of this year. Hackers used malware to create a botnet, sort of a gargantuan, amorphous mass of connected devices, to flood a domain server with terabytes of traffic, overwhelming the system and preventing legitimate traffic from accessing those devices.

In this case, the result was brief, but the outages were on consumer-facing Web sites. The incident is unique in that it wasn't someone's desktop or laptop, but it was the armies of compromised devices that launched these attacks without the knowledge of the device owners. Many of the devices are regular household items, such as baby monitors, DVRs, Web cams. And many consumers do not realize they do need strong cyber protections on even these everyday devices.

But that is exactly why this attack and others like it has been so successful. The malware that created this botnet spread to vulnerable devices by continuously scanning the Internet for Internet of things systems protected only by the factory default manually generated usernames and passwords.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

The balance between functionality and security is not going to be resolved in the near term. Consumers want the newest and fastest device, they want it as soon as possible, and they have not employed adequate security protections. In fact, the most common password is the word "password." The culture surrounding personal cybersecurity must change to ensure that the Internet of things is not vulnerable to a single insecure device.

The Subcommittee on Commerce, Manufacturing, and Trade has explored cybersecurity through a number of hearings, including our Disrupter Series. Cybersecurity, the issue of cybersecurity has been raised and discussed at each of these hearings. The government is never going to be big enough to have the manpower and the resources to address all of these challenges as they come up, which is why it is so important and why I am grateful that we have industry here today to discuss this with us, because they must take the lead.

Recent attacks present a unique opportunity to examine the scope of the threats and the vulnerabilities presented by connected devices and to learn how stakeholders are considering these risks throughout the supply chain, as well as how consumers are responding in the market. We have learned about a number of best practices and the standard-setting projects that are ongoing with various groups.

It is an exciting time. And the growth of interconnected device, the growth of the Internet of things, it is really going to be

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

life-changing in so many industries, but we also need to see meaningful leadership from industry about how to address these real challenges.

Again, I want to welcome our witnesses, and then I am pleased to yield the balance of my time to the gentleman from Ohio, Mr. Latta.

[The prepared statement of Mr. Burgess follows:]

******** COMMITTEE INSERT ********

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Mr. Latta. Thank you very much, and I appreciate the gentleman for yielding. And I also appreciate both chairmen of both subcommittees for holding this very important subcommittee hearing today on the cybersecurity risks associated with connected devices.

As has been mentioned, that last month we witnessed one of the largest distributed denial of service attacks caused by devices connected to the Internet or the Internet of things. The attack against Dyn revealed the impact that a lack of adequate security measures in these devices can have on the broader Internet community. By simply exploiting weak security features, such as default usernames and passwords, hackers could easily leverage hundreds of thousands of networked devices and compromise several major Web sites.

That is why it is essential, under the Internet of things, device manufacturers build in security by design and have the ability to deploy patches or upgrades. Additionally, consumers must be vigilant in securing devices through good cyber hygiene practices in order to guard data and fully experience the benefit of the Internet of things.

As the cochair of the committee on the Internet of Things Working Group, I am all too familiar with this issue. Cybersecurity is among one of the most common things that is mentioned in all of our working group briefings. No matter what type of IoT, from health to energy applications, securing devices and protecting consumer data is a top priority.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Today, we are reminded again that there is a need for IoT security guidelines that keep pace with rapidly evolving technologies. However, there is a delicate balance between oversight and regulatory flexibility, and we must encourage the industry to establish best practices that will not hinder innovation and protect consumer privacy and security.

And, with that, I appreciate the gentleman for yielding, and I yield back.

[The prepared statement of Mr. Latta follows:]

******** COMMITTEE INSERT ********

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Mr. Walden. The gentlemen yield back their time.

We will now turn to the gentlelady from Illinois, Ms. Schakowsky, for opening comments.

Ms. Schakowsky. Thank you, Mr. Chairman.

With each report of a new cyber attack, Americans increasingly realize how vulnerable their devices are. On October 21, Americans lost access to sites such as Twitter, Amazon, and Spotify because of a massive distribution denial of service, or DDoS, attack against Dyn, a domain naming system company.

In the wake of that cyber attack, I joined with Representatives Pallone, Eshoo, DeGette, and McNerney in requesting a hearing like this -- and I appreciate it very much that we are having it -- on this important issue. We need to better understand our vulnerabilities and update Federal policy to stop such attacks in the future.

The motivations of hackers vary from identity theft to actually undermining public trust. They go after consumers, businesses, and even Presidential elections.

The U.S. intelligence community found that hackers supported by the Russian Government put their thumb on the scale in 2016. I strongly believe that use of cyber attacks by a foreign actor to manipulate our democracy should be troubling to everyone. This problem does not go away now that the 2016 election is over.

The day after the election, a wired article reported, quote, "That

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Russia perceives those operations as successful, experts say, will only encourage similar hacks aimed at shifting elections and sowing distrust of the political processes in Western democracies," unquote. Everyone, whether your candidate won or lost last week, must grapple with this threat, and I hope that we will work on a bipartisan basis to protect our democracy from foreign interference.

Russian hackers exploited holes in security on computers and servers. The hackers that carried out the October 21 DDoS attack directed their attack through the Internet of things.

The Internet of things is uniquely vulnerable to cyber attacks. IoT devices often have less protection from malware and manufacturers are often slower to install security patches. Manufacturers put consumers at further risk by using default passwords or hard-coded credentials. Once hackers find out what those passwords are, they can hack hundreds, thousands, or even millions of devices. That is what happened in the Dyn attack.

Hackers accessed an army of IoT devices by exploiting default passwords. They then used that army to attack Dyn. Traffic from the IoT devices overwhelmed the service and shut it down, which, in turn, cut off Americans' access to many popular Web sites. You don't have to be a tech expert to see the terrifying potential for future cyber attacks. So it is time now for action.

Two weeks ago, Ranking Member Pallone and I called on the Federal

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Trade Commission to work with IoT manufacturers to patch vulnerabilities on their devices and require the changing of default passwords. We also called on the FTC to alert consumers about potential security risks. We need stronger cybersecurity standards for all devices that could be attacked or used to launch a cyber attack.

Given the nature of cyber attacks, we cannot count on IoT manufacturers to do the right thing on their own. They have little financial incentive to improve security, and their customers may not even realize when their devices are being used to harm others. Consumer watchdogs, like the FTC, must take a leading role in promoting cybersecurity and holding companies accountable when they fail to provide adequate protections.

Unfortunately, at the same time that the threat to consumers from cyber attacks are rising, the Republican majority is pushing legislation to reduce the FTC's authority and cripple its enforcement capabilities. Stopping irresponsible behavior by companies requires strong consent orders and the ability to pursue privacy cases. The so-called, quote, "process reform," unquote, bill that Republicans reported out of committee would threaten the FTC's ability in those areas. Instead of rolling back consumer protections, we need to face today's cyber threats head on. Consumers can't afford to be left vulnerable. And in the long run, manufacturers can't survive a pattern of high-profile cyber attacks that undermine consumer trust in their

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

products.

In Mr. Schneier's written testimony, he called the Dyn attack, quote, "as much a failure of market and policy as it was of technology," unquote. We should not be content with failure any longer.

I want to thank the chairman for listening to our request for a hearing, and we have to continue our work on this issue in the months and years to come.

[The prepared statement of Ms. Schakowsky follows:]

******** COMMITTEE INSERT ********

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Mr. Walden. The gentlelady yields back her time. We thank you very much for your request. We share in this concern, obviously. It is a bipartisan issue.

We look forward now to the testimony from our expert witnesses. We are glad you are all here, and we will start with Mr. Dale Drew, who is the senior vice president/chief security officer for Level 3 Communications.

Mr. Drew, welcome. Thank you very much. Turn on your microphone and have at it.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

STATEMENTS OF DALE DREW, SENIOR VICE PRESIDENT, CHIEF SECURITY OFFICER, LEVEL 3 COMMUNICATIONS; KEVIN FU, CEO, VIRTA LABS, AND ASSOCIATE PROFESSOR, DEPARTMENT OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE, UNIVERSITY OF MICHIGAN; AND BRUCE SCHNEIER, ADJUNCT LECTURER, KENNEDY SCHOOL OF GOVERNMENT, HARVARD UNIVERSITY, AND FELLOW, BERKMAN KLEIN CENTER, HARVARD UNIVERSITY

STATEMENT OF DALE DREW

Mr. Drew. Chairmen Walden and Burgess and Ranking Members Eshoo and Schakowsky, thank you for the opportunity to testify on behalf of Level 3 Communications regarding the recent cyber attacks on our Nation's communications landscape and the risks posed by vulnerabilities found in IoT devices.

Level 3 is a global communications company serving customers in more than 500 markets in over 60 countries. Given our significant network footprint and the amount of traffic we handle on a daily basis, Level 3 has a unique perspective on threats facing our communications landscape. Several years ago, Level 3 established the Threat Research Labs to actively monitor communications for malicious activity, helping to detect and mitigate threats on our networks, our customers, and the broader Internet. Every day our security team monitors more

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

than 48 billion security events, detecting over 1 billion unusual or suspicious pieces of traffic.

The proliferation of IoT devices represents tremendous opportunities and benefits for consumers by connecting devices such as cameras, light bulbs, appliances, and other everyday items to the Internet. However, the lack of adequate security measures in these devices also poses significant risks to users in the broader Internet community.

Vulnerabilities in IoT devices stem from several sources. Some devices utilize default and easily identifiable passwords that hackers can exploit. Others utilize hard-coded credentials that users are not able to change. Many devices also lack the capability of updating their firmware, forcing consumers to monitor for and install the updates themselves.

The global nature of the IoT device marketplace means many products are manufactured in and shipped to foreign countries that have yet to embrace sound and mature cybersecurity practices. IoT devices are also particularly attractive targets because users often have very little way to know when they have been compromised. Unlike your personal computer or phone, which have endpoint protection capabilities and the user is more likely to notice when they perform improperly, compromised IoT devices may go unnoticed for longer periods of time.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

In September of 2016, Level 3's Threat Research Labs began tracking a family of malware targeting IoT devices. The bad actors were leveraging the infected devices to create DDoS botnets, impacting not just those devices but potentially anyone on the Internet. The new malware, known as Mirai and its predecessor BASHLITE has affected nearly 2 million devices on the Internet. Mirai resulted in multiple major Web sites going offline, and the new attacks are alarming for their scope, impact, and the ease in which the attackers have employed them.

Also worrisome is that these attackers relied on just a fraction of the total available compromised IoT nodes in order to attack their victims, demonstrating the potential for significantly greater havoc for these new threats. Level 3 detected, for example, approximately 150,000 IoT devices were used to generate more than 500 gigabits per second of traffic, a significant amount of bandwidth that threatens the fabric of the global Internet.

The primary motivation for these attacks appear to be financial. Hackers utilize DDoS to overwhelm businesses, threatening to take their business offline unless they pay a ransom for the attacker. In other cases, attackers are simply out to create mischief.

Although Level 3 has not been a direct victim of these attacks, we are proactively taking steps to address these. We have contacted manufacturers of compromised devices to inform them of the problem and

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

for them to take appropriate action, such as firmware updates or recalls. We have engaged in a public awareness campaign to educate consumers and businesses about the risk of IoT botnets and steps they can take to protect themselves. We are also working collaboratively with our industry partners to monitor this evolving threat and implementation of mitigation techniques.

With the exploding proliferation of IoT devices, so too will the threats they pose continue to expand and evolve. It will be imperative for all relevant stakeholders to continue to work collaboratively and address and mitigate IoT security risks so that we can reap the benefits of this exciting and transformative technology.

Thank you again very much for the opportunity to testify, and I look forward to taking your questions.

[The prepared statement of Mr. Drew follows:]

******** INSERT 1-1 ********

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Mr. Walden. Mr. Drew, thank you for taking time out of your schedule to be here as well. We greatly appreciate it.

I now turn to Mr. Bruce Schneier, a fellow at the Berkman Klein Center at Harvard University; lecturer and fellow, Harvard Kennedy School of Government; and special adviser to IBM Security.

Mr. Schneier, thank you for being here. We look forward to your testimony, sir.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

STATEMENT OF BRUCE SCHNEIER

Mr. Schneier. Thank you, Chairman Walden, Chairman Burgess, Ranking Members Eshoo and Schakowsky. Committee members, thank you for having me and thank you for having this, I think, very important hearing.

I am Bruce Schneier. I am a security technologist. And while I have an affiliation with both Harvard and IBM, I am not speaking for any of them and I am not sure they know I am here.

Mr. Walden. It is a secret. Nobody on the Internet knows either.

Mr. Schneier. As the chairman pointed out, there are now computers in everything, but I want to suggest another way of thinking about it, in that everything is now a computer. This is not a phone, this is a computer that makes phone calls; or a refrigerator is a computer that keeps things cold; an ATM machine is a computer with money inside. Your car is not a mechanical device with computers, but a computer with four wheels and an engine, actually, a hundred-computer distributed system with four wheels and an engine. And this is the Internet of things, and this is what caused the DDoS attack we are talking about.

I come from the world of computer security, and that is now

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

everything security. So I want to give you four truths from my world that now apply to everything.

First, attack is easier than defense for a whole bunch of reasons. The one that matters here is that complexity is the worst enemy of security. Complex systems are hard to secure for an hour's worth of reasons, and this is especially true for computers and the Internet. The Internet is the most complex machine mankind has ever built by a lot and it is hard to secure. Attackers have the advantage.

Two, there are new vulnerabilities in the interconnections. The more we connect things to each other, the more vulnerabilities in one thing affect other things. We are talking about vulnerabilities in digital video recorders and Web cams that allowed hackers to take down Web sites. There are stories of vulnerabilities in a particular account.

One story. A vulnerability in an Amazon account allowed hackers to get to an Apple account, which allowed them to get to a Gmail account, which allowed them to get to a Twitter account. Target Corporation, you remember that attack. That was a vulnerability in their HVAC contractor that allowed attackers to get into Target. And vulnerabilities like these are hard to fix because no one system might be at fault. There might be two secure things come together and create insecurity.

Truism three: The Internet empowers attackers, attack scale.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

The Internet is a massive tool for making things more efficient, and that is also true for attacking. The Internet allows attacks to scale to a degree impossible otherwise. We are talking about millions of devices harnessed to attack Dyn, and that code, which somebody smart-wrote, has been made public. Now anybody can use it. It is in a couple of dozen botnets right now. Any of you can rent time on one on the dark Web to attack somebody else. I don't recommend it, but it can be done. And this is more dangerous as our systems get more critical.

The Dyn attack was benign, a couple of Web sites went down. The Internet of things affects the world in a direct and physical manner: Cars, appliances, thermostats, airplanes. There are real risks to life and property and there are real catastrophic risks.

The fourth truism: The economics don't trickle down. Our computers are secure for a bunch of reasons. The engineers at Google, at Apple, at Microsoft spent a lot of time at this, but that doesn't happen for these cheaper devices. Ms. Eshoo has talked about this. These devices are lower profit margin, they are offshore, there are no teams, and a lot of them cannot be patched. Those DVRs, they are going to be vulnerable until someone throws them away, and that takes a while. We get security, because I get a new one of these every 18 months. Your DVR lasts for 5 years, your car for 10, your refrigerator 25. I am going to replace my thermostat approximately never.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

So the market really can't fix this. The buyer and seller don't care. And Mr. Burgess pointed this out. The buyer and seller want a device that works. This is an economic externality. They don't know about it and it is not part of the decision. So I argue that government has to get involved, that this is a market failure, and what I need are some good regulations. And there is a list of them, and Dr. Fu is going to talk about some of them, but this is not something the market can fix.

And to speak to Mr. Walden's point, I mean, yes, I am saying that a U.S.-only regulatory system will affect the products in the world, because this is software. Companies will make one software and sell it everywhere, just like, you know, automobile emissions control laws in California affect the rest of the country. It makes no sense for anybody to come up with two versions. And I think this is going to be important, because for the first time, the Internet affects the world in a direct and physical manner.

And the second point I want to make very quickly is we need to resist the FBI's calls to weaken these devices in their attempt to solve crimes. We have to prioritize security over surveillance. It was okay when it was fun and games, but now, you know, already this stuff on this device that monitors my medical condition, controls my thermostat, talks to my car, I mean, I have just crossed four regulatory agencies and it is not even 11 o'clock.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

This is going to be something that we are going to need to do something new about. And like many new technologies in the 20th century, new agencies were created: Trains, cars, airplanes, radio, nuclear power. My guess is this is going to be one of them, and that is because this is different. This is all coming. Whether we like it or not, the technology is coming. It is coming faster than we think. I think government involvement is coming, and I would like to get ahead of it. I would like to start thinking about what this would look like. And we are now at the point, I think, where we need to start making moral and ethical and political decisions about how these things worked.

When it didn't matter, when it was Facebook, when it was Twitter, when it was email, it was okay to let programmers, to give them the special right to code the world as they saw fit. We were able to do that. But now that it is the world of dangerous things, that is, cars and planes and medical devices and everything else, that maybe we can't do that anymore. And I don't like this. I like the world where the Internet can do whatever it wants whenever it wants at all times. It is fun. This is a fun device. But I am not sure we can do that anymore.

So thank you very much, and I look forward to questions.

[The prepared statement of Mr. Schneier follows:]

******** INSERT 1-2 ********

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Mr. Walden. Mr. Schneier, thank you very much. I appreciate your comments.

We will now go to Dr. Kevin Fu, CEO of Virta Labs and associate professor, Department of Electrical Engineering and Computer Science, at the University of Michigan.

Dr. Fu, thank you for joining us. Please go ahead.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

STATEMENT OF KEVIN FU

Mr. Fu. Good morning, Chairmen Walden, Burgess, Ranking Member Eshoo and Schakowsky, and distinguished members of the joint committee.

My name is Kevin Fu. I represent the academic cybersecurity research community. I am at the University of Michigan, where I conduct research on embedded security. My laboratory discovers how to protect computers built into everyday objects, ranging from mobile phones and smart thermostats to pacemakers and automotive airbags. I am also CEO and cofounder of the healthcare cybersecurity startup Virta Labs.

I am testifying before you today on the insecurity of the Internet of things as related to the recent attacks on Dyn. I will provide a perspective on the evolving cybersecurity risks framed in the broader societal context. In short, IoT security remains woefully inadequate. None of these attacks are new. None of these attacks are fundamentally new, but the sophistication, the scale of disruption, and the impact on infrastructure is unprecedented.

Let me make some observations. We are in this sorry and deteriorating state because there is almost no cost to a manufacturer for deploying products with poor cybersecurity to consumers. Has a consensus body or Federal agency issued a meaningful IoT security

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

standard? Not yet. Is there a national testing lab to verify and assess the premarket security of IoT devices? No. Is there tangible cost to any company that puts an insecure IoT device into the market? I don't think so.

So I would like to highlight eight observations about this IoT insecurity.

Number one, security needs to be built into IoT devices, not bolted on. If cybersecurity is not part of the early design of an IoT device, it is too late for effective risk control.

Two, good security and bad security look the same at the surface.

Three, the healthcare community does not issue different advice for flu transmitted by cough versus flu transmitted by sneeze. Similarly, both connected and disconnected IoT devices carry significant cybersecurity risks, so it is important to consider both conditions.

Four, the millions of insecure IoT devices are just a small fraction of what the IoT market will resemble in 2020, and it will get much worse if these security problems remain unchecked.

Five, unlike inconvenient security problems for your tablets or notebook computers, IoT's insecurity puts human safety at risk, and innovative systems will not remain safe if they are not secure.

Six, I consider security a solution, not a problem. Better cybersecurity will enable new markets, promote innovation, and give

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

consumers the confidence to use new technologies that improve the quality of life.

Seven, it may be surprising, but there are over 209,000 unfilled cybersecurity jobs in the USA, and that is just this country.

And eight, the Nation lacks an independent testing facility at the scale of a federally funded research and development center as a proving ground for testing premarket IoT cybersecurity crashworthiness and for testing embedded cybersecurity defenses.

Let me conclude with five recommendations to protect our national infrastructure.

Number one, incentivize built-in basic cybersecurity hygiene by establishing meaningful milestones encouraging use of strong cryptography in these products.

Two, support agencies such as the National Science Foundation, the National Institute of Standards and Technology, to advance our understanding of IoT security and to train the hundreds of thousands of students necessary for a robust cybersecurity workforce.

Three, study the feasibility of standing up an independent national embedded cybersecurity testing facility modeled after, for instance, post-incident initiatives, such as the National Transportation Safety Board; incident prevention initiatives, such as the National Highway Traffic Safety Administration, NHTSA; and then more unusual places like the survivability and destruction testing at

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

the Nevada National Security Site.

Number four, I recommend leveraging the existing cybersecurity expertise with an agency such as NIST, NSF, DHS, and DARPA.

And finally, five, I believe that universities, industry, and the government must find the strength and the resolve for protecting our national infrastructure through partnerships, and that investments in embedded cybersecurity will pay great dividends to our society and our economy.

I would like to close, just thank you for the invitation to testify on what I think is a very important subject for our country. The committee can also find photos of illustrative IoT problems in water treatment facilities, hospitals and more in the appendix of my written testimony. And I would be happy to take your questions. Thank you.

[The prepared statement of Mr. Fu follows:]

******** INSERT 1-3 ********

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Mr. Walden. Dr. Fu, thank you.

And thank you to all of our witnesses. This has been very enlightening. We greatly appreciate your testimony and your recommendations for our consideration.

I guess I will start with a couple of questions as we try and wrestle this issue. Over the last 6 years, we have done multiple hearings on cybersecurity threats to the United States. We have had multiple panels come before us and testify. And I think almost entirely they said, first, do no harm. Be careful when you lock things into statute because you can misallocate our resources and our opponents will know what we have to go do and we can't get out of it and they will just go do a workaround.

So how do we establish a framework that would both be appropriate here but have an effect internationally, because we don't make all the devices and we may have market power, but we are not the biggest market anymore? But how do we create a national framework where the stakeholders really are driving this in realtime and we don't do something stupid like lock certain requirements into statute?

Mr. Drew, can I start with you, and we will just work down the panel?

Mr. Drew. I think the best place to start is with standards. I think the best place to start is for us to define how we intend on solving this problem on the devices themselves. Industries have a number of

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

standards with regards to how they operate these platforms once they purchase them, but they don't have standards on how they are supposed to be manufactured to be secure premarket.

So I believe if we were to start with standards and then apply pressure -- so as an industry, I am under pressure to implement standards in order to be able to serve businesses and serve the consumers. I think if we start with that standard, then we are able to apply that pressure. And to the extent that pressure can be applied globally, I think that we can get some traction and some momentum before we have to start regulating.

Mr. Walden. All right.

Mr. Schneier?

Mr. Schneier. I am also a fan of standards. And I think your question is a really important one, how do you do it properly as to not stifle innovation?

Mr. Walden. Right.

Mr. Schneier. And I think the answer is to make them technologically invariant. And I tend to look at the pollution model as something -- what works and what doesn't. And what works is, you know, here is the result we want. Figure out how to do it in the most cost-effective way possible, rather than legislate here's the process, here's the technology. The standard has to be technologically invariant.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

And I heard, you know, you had a driverless car hearing yesterday, and I think it is somewhat similar. We are going to make standards on the driverless car manufacturers to do things properly, but we are going to assume an environment where there exists, you know, malicious cars out to get you. So we will have to deal with the rogue devices. We can't assume that everything on the Internet, or everything on the roads, is going to be benign and secure. But standards will raise the tide, but yes, we have to do them properly, because you do them wrong and it will stifle innovation. Do them right, I think it will help innovation.

Mr. Walden. All right.

Dr. Fu?

Mr. Fu. Yes. I think there are ways you can do this effectively without stifling innovation. In fact, I believe that a well-designed cybersecurity framework will actually promote innovation. I will try to avoid the technical side, but I will just say, you know, of course, encoding mechanism would be unwise. For instance, if you decide to encode that all forms must be signed in blue ink, that didn't, you know, assume the existence of e-signatures in the future. So you should be very careful of encoding mechanism.

However, principles I think you can encode. I would actually say that NIST has done a relatively good job at encoding principles. There is no perfect standard. But it will be very difficult to build in

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

security if we don't have these principles set in place. And it needs to have buy-in from industry. It needs to have government leadership as well. But it is all about setting those principles, which many of which are already known for over 30 years in the cybersecurity community.

Mr. Walden. All right. Most helpful. The extent to which you all can think about this some more and give us kind of your ideas on how to actually get it to the right place. Because this is my concern, that if we are not careful, we lock something in, it is so hard to change statute.

And we don't want this to be an innovation killer in America. We actually want to lead on this and get it right. But, you know, I don't think I want my refrigerator talking to, you know, some food police somewhere, you know. It just is what it is. So we need to get this thing right. So thank you for being here.

At this point, I will return the balance of my time and turn to my friend and colleague who has been very involved in this, Ms. Eshoo, from California.

Ms. Eshoo. Thank you, Mr. Chairman.

And thank you to each one of you, the witnesses. I think you were absolutely terrific.

I have legislation that I introduced that speaks to this issue. It hasn't really gained much traction. But what you said today I think

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

puts some wheels on it, because it is about security without damaging innovation.

We talk a lot about the attacks that take place, but we don't really focus on prevention. Throughout the Valley, Silicon Valley, no matter who I have met with, I have asked them the same question: What would you do about this? And to a person, they have spoken about hygiene, the lack of hygiene in systems, number one; and number two, the lack of good solid security management.

I don't think -- let me put it in a positive. I think we need a Good Housekeeping Seal of Approval on this, and I think that -- and my bill called for NIST to set the standards, not the Congress, because we really don't know anything about that. And we miss the mark, we will miss it by a wide mile. Exactly.

So I also think in listening to you, especially Mr. Schneier, that this is an issue that should be included in national infrastructure legislation, because this is part of our national infrastructure. And it deserves the kind of protection that you spoke to, because, as you said, everything is a computer, everything. It is not just the computers over at the DOD. We are carrying them around in our pockets, we are driving them, et cetera, et cetera.

So given that, what is the framework for it? How would both -- Mr. Schneier and Dr. Fu and Mr. Drew, what would it look like? What would it look like? I am giving you a blank slate. What would

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

you write on that slate to be placed in a national infrastructure bill? So whomever wants to start.

Mr. Schneier.

Mr. Schneier. I actually think we need a new agency. The problem we are going to have is that we can't have different rules if the computer has wheels or propellers or makes phone calls or is in your body. That is just not going to work, that these are all computers and we are going to have to figure out rules that are central.

Ms. Eshoo. We have a continuing new new majority. So I don't think they want to create an agency, honestly, but this thing needs to get done.

Mr. Walden. For every one we create, we delete two.

Ms. Eshoo. They don't like that stuff.

Mr. Schneier. I think you are right.

Ms. Eshoo. You know, new agencies, new regulations, we are dead in the water. But we can't leave this issue to be dead in the water. Our country deserves much better. And so I am really not joking. I mean, it is a little bit of fun, but, you know.

Mr. Schneier. I understand. But I actually think it is not going to go that way. I mean --

Ms. Eshoo. Oh, good.

Mr. Schneier. -- because I think the government is getting involved here regardless. The risks are too great and the stakes are

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

too high. And, you know, nothing motivates a government into action like security and fear.

In 2001, we had another small-government, no-regulation administration produce a new Federal agency 44 days after the terrorist attacks. Something similar happens in the Internet of things, and there is no cybersecurity expert that will say, well, sure, that could happen. I think you are going to have a similar response.

So I see the choice is not between government involvement and no government involvement, but between smart government involvement and stupid government involvement. I would rather think about it now, even if you say you don't want this, because when something happens and the public says something must be done, what do you mean, a thousand people just died, that we have something more than a I don't know, let's figure it out fast. So I agree with you. I am not a regulatory fan, but this is the world of dangerous things. We regulate dangerous things. So --

Ms. Eshoo. Dr. Fu, can you do something, in 5 seconds? Thank you.

Mr. Fu. I would say just we are going to have some serious trouble if we don't answer these questions. I fear for the day where every hospital system is down, for instance, because an IoT attack brings down the entire healthcare system.

I do think you need to spend more time on the premarket. I know

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

from my working with manufacturers that the engineers there are brilliant, but they often are not given the time of day from their executives. They are often not given the resources to do their jobs. What you need to do is give those people who can do a good job at those companies the ability to do so and incentivize their executives.

Ms. Eshoo. Thank you very much. Most helpful.

Thank you, Mr. Chairman.

Mr. Walden. Thank you. I would just point out we are all engaged in this on both sides. My friend and I have some back-and-forths from time to time. She likes to characterize what we are for or against, which we may or may not be, but we are all committed to trying to figure out how to find a solution, and this is bipartisan.

So we appreciate your testimony. We scheduled this hearing back in October right after the attack, and as soon as we were back in town we are having it, and we will continue to march forward.

With that, I would turn to the gentleman from Texas, Mr. Burgess.

Mr. Burgess. Thank you, Chairman Walden.

And it has been a fascinating discussion back and forth. Many years ago before I knew about the Internet of things, I was invited up to Microsoft in Washington and they showed me the house they had. In fact, the house was named Grace. And, you know, you walk up to the door and Grace knew you were coming to the door. Grace turned the lights on, set the thermostat for the temperature that you wanted. As

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

you came into the kitchen, Grace might suggest a meal for you. Like Mr. Walden, I worried that Grace's refrigerator would communicate with the bathroom scale and lock down the Blue Bell ice cream on me. So it is an interesting world in which we have arrived.

Mr. Drew, I am really fascinated by your comment in your written testimony about the incentive for someone to do this in the first place. And we have all heard, since 9/11, that sometimes you have got to think like a criminal or think like a terrorist in order to outsmart them. And you referenced the monetization. I don't even see -- I mean, I get on ransomware when you lock down a hospital and you have got to come up with so many thousands of dollars in bitcoins to some dark Web site, but how do you monetize that your doorbell is conversing with Twitter? I mean, I don't know how that works.

Mr. Drew. What we are seeing in these botnets is the botnet operators are operating, you know, hundreds of thousands of nodes and then renting out a small portion of those nodes to people to be able to attack Web sites and hold those Web sites for ransom. So if you don't pay me $20,000, your Web site will be offline for the next 3 days. So a very successful enterprise. It is 40 to 45 attacks a day at 16 grand an attack. So --

Mr. Burgess. That is happening right now?

Mr. Drew. It is happening right now.

Mr. Burgess. I know you are not in law enforcement. What is the

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

response of our law enforcement agencies that are supposed to be enforcing the laws?

Mr. Drew. They are working very diligently to identify the operators of the botnet as well as the renters of the botnet, as well as making some arrests in those cases to be able to curtail this. But what we have seen is the IoT of things has changed the nature of the game of this to where it is much easier to break into those devices and they go unnoticed for longer periods of time.

Mr. Burgess. And, you know, here -- this is one of the things that bothers me about this, because until we had this headline-grabbing attack because it was just so massive, you don't hear about someone being busted for holding someone hostage for $17,000 so you unlock their hospital records or whatever was going on.

I mean, one of the things that is talked about is making the public aware. You got to change, you got to practice good hygiene, you can't have your password as password or 1234. But you also -- there needs to be a societal understanding of reporting the crimes when they occur and, to some degree, these need to be publicized much more than they are.

I mean, I have heard from folks in the FBI that, yeah, there is a risk that a hospital that gets stuck with one of these things, they are just simply embarrassed and they don't want to go public with the fact that they were hacked. Pay the $17,000. You are given

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

instructions on how to get the bitcoins and where to deliver them. So that is actually easier than going to law enforcement and dealing with all of the things that would happen with law enforcement. But that is absolutely critical.

And then never in any of the discussion of this, that I have seen so far, has there been really the discussion of what happens to people who are caught who perpetrate this, and it should be swift and severe and public. I suggested at another hearing, shot at sunrise. And I am not trying to be overly dramatic, but if you lock down an ICU's medical records and an ICU's worth of patients die as a consequence, I mean, that is a capital crime.

So anyway, I know we are not going to solve all of the problems today, but I just wanted to put those concepts out there. This is relatively new for most of us.

I think one of the things that I like about -- you know, Mr. Chairman, one of the things I like about what the Commerce, Manufacturing, and Trade Subcommittee did on data security was -- on data breach notification was we will set the standard, but we don't prescribe the technology, because the technology changes much faster than the Congress.

Yeah, I am nervous too about creating new Federal agencies. The concept that we could delete two Federal agencies for every one we create, I have got two to recommend to leave very quickly. They deal

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

with health care. But I know the standards need to be there.

And the other thing is we have got a massive job as far as informing the public, and that is part of this hearing today and I hope we all carry that forward quite seriously.

Thank you, Mr. Chairman. I will yield back.

Mr. Walden. The gentleman yields back.

The chair recognizes the gentlelady from Illinois, Ms. Schakowsky.

Ms. Schakowsky. So let me ask actually all of you, but let me start with Mr. Schneier. You talked about how markets have failed us and that government has to play a role. But I am wondering, from you and from anyone, given that computers are ubiquitous -- and your example that got into Target through the HVAC system is just shocking to me. But is there a role for consumers, for consumer education, for consumer action, or is this beyond us now for individuals to actually play a role in security?

Mr. Schneier. Yeah. I think there is a role for some, but, really, we are asking consumers to shore up lousy products. It shouldn't be that there are default passwords. It shouldn't be that you have to worry about what links you click on. Links are for clicking on. I mean, these devices are low profit margin. They are made offshore. The teams that -- after they make them disband. And the buyer and seller don't care. I mean, so this -- I might own this DVR,

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

you might own it. You don't know if it was used. You don't know if it is secure or not. You can't test it. And you fundamentally don't care. You bought it because of the features and the price. It was sold to you because of the features and the price.

And this is an externality. The fact that it was used by this third party, not him but, you know, by the third party to attack this other site, and it is something that the market can't solve because it is not a market -- the market isn't involved in that. So I don't think I can educate the consumer. It is putting a sticker on that says, you know, this device costs $20 more and is 30 percent less likely to annoy people you don't know. I am not sure I am going to get a lot of sales.

Ms. Schakowsky. So in 2015, the Federal Trade Commission suggested best practices for device manufacturers to address security vulnerabilities. For example, device manufacturers should test security measures before releasing their products, minimizing the data they collect and retain.

And, frankly, it seems surprising to me that manufacturers are not already taking these steps. But you are saying that right now there are no real incentives. So is that what we need to focus on?

Mr. Schneier. I think we should. I think if we get the incentives right, the technologists will figure this out. I mean, this isn't -- some of it is rocket science, most of it isn't. But these

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

are solvable problems. The incentives just aren't there to build the security in. We incentivize price. We incentivize time to market. We incentivize features. I mean, that is what we buy, that is what we want, because that is what we can see.

I don't think I can get consumers to pry open the hood and look at the details. It is beyond the consumers I know and it shouldn't be their problem. It shouldn't be something they have to worry about.

Ms. Schakowsky. So let me ask Mr. Drew and Dr. Fu if you want to comment on that.

Mr. Drew. I would largely agree with my colleague here. I would say that, from a business perspective, there is a lot of incentive for me to make sure that the products that I buy, the software that I buy follow specific standards, have been manufactured correctly before I put them in the network.

I would like to see more in that area. I would like to see more responsibility put on the manufacturer than there is today, but I do provide that incentive to those manufacturers.

Consumers, on the other hand, don't have that incentive. What they do have is the incentive of public events, right, and the Internet has been very adaptable and very flexible to that, that when there is a large sort of trip over -- or a mistake over security that they become more aware, and then they push those requirements and those demands back to the manufacturers by purchasing products they feel more

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

comfortable with.

So I am going back to standards. I am going back to certifications and standards. You see that seal of approval on the device and you know that is a device that is going to be more protected than another device, because you don't want your refrigerator talking to your scale or you don't want your thermostat talking to your doorbell. And so I think --

Ms. Schakowsky. Let me just interrupt you because my time is running out, but I would like Dr. Fu to be able to join in.

Mr. Fu. Sure. I would just paint a darker picture. Even if a consumer wants to have -- so not many consumers are aware they need security, but when they even want security, it is hard to get. Let me take the example of the hospitals, asking questions about why ransomware gets into hospitals. It is not because they are not clueful about it. They can't get the manufacturers to provide them with these IoT medical devices that can withstand the threats of malware.

And it comes down to plain old economics. The question is, well, how much will you pay for it? Well, we think it should be built in. We think it is a public good. Well, how much are you going to pay for it? So everything is going to be driven by the economic factors. And I think the problem is, you know, the consumer group thinks that, you know, it ought to be a public good. And then from the manufacturing standpoint the question is, well, how much are you going to pay for

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

it? And that is a question that needs to be resolved.

Ms. Schakowsky. Thank you.

Thank you. I yield back.

Mr. Walden. The gentlelady yields back.

And the chair now recognizes the gentlelady from Tennessee for 5 minutes.

Mrs. Blackburn. Thank you so much, Mr. Chairman.

I want to go back. I mentioned the Cisco stats, and I think they rolled out of my mouth the wrong way. I want to clarify that for the record.

We are currently at 3.4 IoT devices per person, and by 2020, we are going to be at 50 billion IoT devices. And that is the magnitude of this vulnerability that we have, because we are seeing it across our entire economy as we move from a physical application in so many arenas to the virtual space.

And, Professor Fu, I want to come to you. And Ms. Schakowsky just mentioned hospitals. Let's stay with that medical device component, because of the area that I represent, Nashville area, there is a lot of healthcare informatics and work that is done utilizing IoT devices in the medical field. And as you look at the security, of course, that is a concern. You look at information share, you know, you get vulnerabilities.

But you mentioned in your testimony, going back on pages 5 and

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

6, IoT devices tend to have safety consequences or involve physical manipulation of the world that could easily lead to harm. And then you go on to say a number of hospitals expressed concern about the IoT devices.

So talk to me about mitigation strategies and what you see with these devices, and then what special considerations must be given to healthcare technology and to the medical devices, and how should we go about addressing that?

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

RPTR HUMISTON

EDTR ZAMORA

[11:06 a.m.]

Mr. Fu. Thanks for the question. Unfortunately, I don't think I will be able to give a satisfying answer, because at the moment, if you were to be a fly on the wall in the boardroom when the hospitals are discussing the topic of how does IoT security affect their assurance of the clinical operations being continuous, at the moment, it is -- they don't have a plan. It is more, well, we need to get a plan, what can we do. And it is usually some of the security officers saying, well, the problem is we don't really know what devices we have in our hospital, we don't have a very good inventory, we get a lot of contraband coming in. This contraband is known as shadow IT. It has got a great acronym. But the shadow IT that comes in, typically it is a clinician who accidentally connects a device to a very important network, but maybe it is a music player that is simply providing comfort to the patients during surgery, and they don't realize it is introducing new safety and security risks, because they don't have the security baked into these devices.

So the IoT risk is more about having unvetted assets coming in to a very safety critical arena. They don't have a good answer right now and that is because it is not built in.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Mrs. Blackburn. Okay. Well, then let me go to Mr. Drew. And the article in the New York Times yesterday that I am sure you all saw and are aware of, "Secret Backdoor in Some U.S. Phones Sent Data to China."

Mr. Schneier. Yes.

Mrs. Blackburn. And, Mr. Schneier, I assume you read that. Looks like you did. But this is the kind of thing where consumers are unaware. And if you take a device like that and then you have the concerns if it does get into an environment such as a hospital or a medical facility with patient information, things of that nature.

So these malicious actors are out there, and with the vulnerability of these IoT devices, you have some of these concerns that are going to manifest themselves. So how do we make sure that the consumers and the users are alerted to the vulnerabilities in the software and in these devices when they purchase them so that if they get something like this, they know to get rid of it? So, Mr. Drew?

Mr. Drew. I would say that the biggest sort of benefit of IoT devices -- the reason IoT devices can get compromised so quickly is because they all look the same. So at a device manufacturer, all the devices look the same, the users are not really configuring the operating system at all, that is why devices can get compromised very, very quickly, very wide scale.

Having those devices ability to auto patch so when a new exposure

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

comes out, that that device can call home, get a new software update and automatically update, that -- that is getting the thing that keeps that infrastructure healthy.

Mrs. Blackburn. Thank you. I yield back.

Mr. Latta. The gentlelady, the vice chair of the full committee, yields back.

The chair now recognizes the gentleman from New Jersey, the ranking member, for 5 minutes.

Mr. Pallone. Thank you, Mr. Chairman.

I wanted to ask Mr. Schneier a couple of questions. Looking at the attack on Dyn 3 weeks ago, I am concerned some people may dismiss it as only a few Web sites going down for a few hours. But in your view, what does the attack on Dyn expose about cybersecurity generally and why are these attacks moving from benign to dangerous?

Mr. Schneier. It is really what I talked about the world moving. The Internet is becoming something that affects the world in a direct physical manner. And the computers are the same. When we are talking about these computers in our phones, in our computers, it is the same computers that are in these cheaper and smaller devices. But while the software is the same, the engineering is the same, there is a fundamental difference between your spreadsheet crashes and you lose your data and your car crashes and you lose your life. The computer is the same, the software is the same, but the effects are night and

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

day different.

And as these computers start -- I live in Minnesota. I have a thermostat I can control from my phone and, you know, if someone hacks it, they can -- well, not this weekend, but in the middle of winter, they can burst my pipes when I am here, and that is real property damage. And that is different than a few Web sites going down. Which I agree, I mean, Dyn was benign. It annoyed some people for a while. It didn't hurt anybody. We are talking about hospitals, we have seen DDoS attacks against 911 services. We are looking at our -- our critical infrastructure, our power grid, our telecommunications network. These are systems that are being controlled by computers.

We had hackers break into a dam a couple of years ago. They didn't do anything, but, you know, next time you might not get lucky. We had Russia attack Ukraine's power grid. These are now -- these are now tools of war and of national aggression. I mean, even the attacks against our election system, which in the scheme of things are pretty benign, might not be next time. I had a piece in the New York Times a couple days ago that talked about, we need to think about this now, because election machines are computers you vote on.

Mr. Pallone. Sure. Well, let me get to -- that kind of leads me to the next question, because you and others have said that the insecurity of devices connected to the Internet stems from market failure, and you even compare the problem to invisible pollution.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Being an environmentalist, I would like to better understand what you mean. Can you expand on the market failure at play here, and how are these insecure devices like traditional environmental pollution?

Mr. Schneier. It is because the insecure effects are often not borne by the buyer and the seller. The person who bought that DVR who is still using it, will use it for the next 5, 10 years, will not bear any of the costs of the insecurity. So the manufacturer and the buyer too reap the benefit. The device was cheaper. It was easier to make because it is insecure. And there is a societal cost that it can be used to attack others, to cause other vulnerabilities, to be used in conjunction to cause other insecurities.

So like pollution, it is something in the environment that neither the buyer nor the seller, when they enter their market agreement to purchase the product, will fix. So I think the solutions are along those lines. We have to think about what is the risk to us as a group; you know, what is the national security risk of this, for example. I mean, there is one, but it is not going to be borne by, you know, the person who bought that. It will be borne by all of us.

So it is incumbent on all of us to secure our critical infrastructure against this risk, and that is -- so I think the solutions are very similar in conception. The tech is very different.

Mr. Pallone. All right. Let me ask you one last question. You seem to believe that regulation of some kind might be part of the

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

solution, but I have heard some at the FCC argue that regulation of devices connected to the Internet will constrain innovation. Would you agree with that?

Mr. Schneier. Yes, it will. I mean, I don't like that, but in the world of dangerous things, we constrain innovation. You cannot just build a plane and fly it, you can't, because it could fall on somebody's house. And you might not care, I mean, it might be a drone, but we societally care. True for medical devices, true for dangerous things. And it might be that the Internet era of fun and games is over, because the Internet is now dangerous.

I mean, we haven't even started talking about actual robots, but, you know, a robot is just a computer with arms and legs that can do stuff. And I personally don't like killer robots. I think they are a mistake and we should regulate them.

So, yes, this is going to constrain innovation. It is not going to be good, I am not going to like it, but this is what we do when innovation can cause catastrophic risk. And it is catastrophic risk here. It is crashing all the cars, it is shutting down all the power plants. I mean, the Internet makes this possible because of the way it scales, and these are real risks.

Mr. Pallone. Thank you.

Thank you, Mr. Chairman.

Mr. Latta. Thank you. The gentleman yields back.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

The chair now recognizes the gentleman from New Jersey for 5 minutes.

Mr. Lance. Thank you. Good morning to the distinguished panel. And I certainly agree with Congresswoman Eshoo that this is one of the more interesting panels that we have had on this extremely important topic.

Professor Fu, of your observations and recommendations, the eight of them you have given to us, I would like to concentrate on three of them.

Number one, you state that security needs to be built into the Internet of things, devices, not bolted on. Could you expand on that as to how you think that might occur, that the security occurs before the device has been manufactured?

Mr. Fu. Right. Thank you. So often when we talk about security problems in the media or the news, you think, oh, this was a poorly implemented product, where, in fact, it was a poorly designed product, and there is a subtle difference. If you don't get security built in to the early design of these IoT devices, it doesn't matter how smart the engineers are, they will never be able to succeed at creating a secure device, and so that is why you really need to build it in.

If you have this residual risk that you then hand off to the consumer, there are -- there are some sweet spots where you can try to mitigate the risk after the fact, but it is extremely rare, extremely

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

hard, and extremely --

Mr. Lance. So how do we do that? How do we build it in initially?

Mr. Fu. Right. There is actually quite a bit of -- this is going to get deep into engineering, but let me just say it in one sentence. It is about hazard analysis. It is all about understanding and enumerating those risks and having the manufacturer choose which risks to accept, which risks to mitigate, which risks to pass on to the consumer.

Mr. Lance. And can that be done through the consumer market or would it require some sort of governmental control? We have mandated, of course, airbags in automobiles, seatbelts in automobiles to be built into the automobile initially and not to be added to the automobile. Is it your recommendation that this will require some sort of governmental mandate or not?

Mr. Fu. I do believe in the long-term, this will likely require some kind of governmental mandate only because, in my experience working with the industry, even though they mean well, even the people who can do it don't have the authority to do the right thing, because they don't have the economic drivers. You often have different constituencies within each company.

And let me just cite an example from the medical world. We didn't think about the safety of over-the-counter drugs until 1982 with the cyanide poisonings in Chicago. Until that day, consumers had quite

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

a bit of faith in those pharmaceuticals. We haven't seen that moment for IoT, but we know that that is there and we know that it can cause harm.

Mr. Lance. Thank you. Moving on, number 4 of your observations for devices already deployed, we should take some comfort that millions of insecure devices are just a small fraction of what the market will resemble in 2020. I suppose you mean by that that this is just at the beginning and there will be many, many more by 2020.

Mr. Fu. That is correct. I would say, on a positive side, it means if we take an action now, we could actually win this, we could actually have a very secure ecosystem. So even though there are terrible, terrible problems today, we can fix it, so we shouldn't give up hope.

Mr. Lance. And can you give us a rough estimate, if we have X number of devices now, how many devices will we have in 2020?

Mr. Fu. Well, I have heard the number double in the last 62 minutes from 20 billion to 50 billion, so somewhere between 20- to 50 billion, I think, is a reasonable estimate.

Mr. Lance. I see. And then number 7 of your observations, there are tens of thousands of unfilled cybersecurity jobs in this country. Existing approaches are insufficient to train a large number in the workforce for what we need in this area.

Based upon your experience first at MIT and more recently in Ann

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Arbor, what do the great universities need to do in this regard and what do we need to do at the level of community colleges, for example?

Mr. Fu. That is a very good question. I think community colleges play a very important role as we develop the different kinds of skill sets. So actually, in fact, there are 209,000 unfilled cybersecurity positions as of a year ago in the U.S., over a million unfilled positions globally.

The problem is, I think, universities need to shift and adapt to the changing marketplace. Right now we are overrun with students. We cannot teach the number of students who want to take our security courses, and yet we are still not meeting the needs. In Michigan, for instance, we have the automotive companies talking about they have 30 unfilled FTE positions for cybersecurity and they are wondering why no one applies.

Mr. Lance. Well, thank you. My time has expired. I hope to continue the discussion with all on the distinguished panel and particularly with you, Dr. Fu. Thank you very much.

Mr. Latta. Thank you. The gentleman's time has expired. The chair now recognizes the gentleman from California for 5 minutes.

Mr. McNerney. Well, I thank the chair and I thank the panel. This is why I love this subcommittee and this committee. Great stuff happening. I am going to start with Mr. Drew.

In your testimony, you noted that about 2 million of these IoT

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

devices have been affected by this bot, botnet, and only 150,000 were used in the attack. That means there is, what, 1.85 million left. Are they still capable of carrying out new attacks or have they been neutralized in any way?

Mr. Drew. We have taken -- the Internet as a whole has taken steps to try to neuter portions of it, but it is still a 1., you know, 5 or 1.6-million-strong node botnet.

Mr. McNerney. And they can attack not just Dyn servers, but they can attack real physical devices. Is that right?

Mr. Drew. Yeah, correct. I mean, the one fear about a botnet like this or a botnet of this size is that they are capable of doing something called a shaped attack, meaning that the operators of that botnet are able to generate any protocol, any application they want from those machines to be able to direct attacks of very specific nature to their targets.

Mr. McNerney. So we have sort of a Damocles sword hanging over us right now?

Mr. Drew. Yeah. I think the saving grace we have had so far is that no one has been able to afford to rent all 1.7 million nodes. They have been renting them at 80 to 150,000 nodes at a time. Our biggest fear is that another adversary sees the power of this total force and begins to adopt attacks that follow a similar nature.

Mr. McNerney. Mr. Fu, in your testimony, you recommended we

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

should incentivize built-in security. I am kind of following up on Mr. Lance's question. What type of incentives do you believe would be effective to prevent the risks that you have outlined?

Mr. Fu. I think that it all comes down to accountability, whether that be economic accountability or liability. Right now, there just isn't any kind of tangible cost to a manufacturer who deploys something with poor security. Also, there is no benefit if they deploy something with good security.

Mr. McNerney. Well, thank you. This is a question to all witnesses. I want you to answer it with a yes or no.

IoT devices span a wide range of products. Would it be feasible to create one set of security standards for all IoT devices? Starting with Mr. Drew.

Mr. Drew. Yes.

Mr. McNerney. Good.

Mr. Schneier. No.

Mr. McNerney. No?

Mr. Fu. No.

Mr. McNerney. No. Oh. Okay.

In the alternative, the Federal Government could establish minimum security standards for IoT devices and then direct the relevant Federal agencies to provide additional sector-specific requirements. Would that be feasible, yes or no, please?

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Mr. Drew. I am sorry. I missed the question.

Mr. McNerney. Well, since there is a wide range of products, it might be feasible to ask the Federal Government to have the different agencies apply specific standards to those devices. Would that be feasible?

Mr. Drew. Oh, absolutely, because that allows people to apply specific requirements and regulations to the area in which those devices operate.

Mr. Schneier. I think no, because devices do multiple things.

Mr. Fu. I think it depends.

Mr. McNerney. Okay. Good, or not.

Mr. Fu, several things. So many questions, so little time. You said that there is no cost to produce devices with poor security, that is pretty clear, but that IoT security is a solution -- I mean, it should be a solution, not a problem. Could you expand on that a little bit --

Mr. Fu. Right. So my fear is that consumers will not embrace technologies that will improve their quality of life in the future because they don't trust that it will be safe. It won't take too many more horror stories before people start to go back to their analog ways.

So I view security as a solution enabling innovation. In the short term, yes, I would agree with the other witnesses that you may see a short-term problem, because you are going to be interrupting the product development and lifecycle. But in the long-term, we are going

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

to see, I think, this actually producing new innovation, just like what we saw with the car safety regulation many decades ago.

Mr. McNerney. Very good. Now, you also mentioned that devices should incorporate strong crypto security, cryptography. Isn't that asking a lot for these cheap devices to incorporate strong cryptography?

Mr. Fu. Cryp- -- stop leading me, Bruce.

Crypto -- you can implement crypto on these devices. However, there are certain special cases, like medical devices, where it is more challenging. For instance, cryptography does draw more electrical power and it can actually reduce the battery, and so it does cause this sort of risk question. But in the general case, I think it is almost always the right answer to deploy the cryptography.

Mr. McNerney. Well, I have one more important question, but my time has run out, so I yield back.

Mr. Latta. Thank you. The gentleman's time has expired, and the chair now recognizes the gentleman from Kentucky for 5 minutes.

Mr. Guthrie. Thanks. I appreciate you all being here. And thanks, Mr. Chairman.

And this has been really informative to me. Usually when I get memorandums getting ready for a meeting and it uses words like bots and terabytes, it kind of -- my eyes glaze over. But this is important and it is interesting and I have appreciated what you are moving

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

forward.

One thing that -- actually, Mr. Lance asked one of the questions I was going to ask. I was going to let Dr. Fu finish a thought, but one thing that you said earlier, that when we write the regulation or the law, that we are going to have to address this if and when we do, that we can't be too prescriptive, because the sign in blue ink, example you used, and I certainly understand that. And I think a lot of things that we have done in legislating has deferred a lot of that to the agencies and we say, well, everything is going to go in good faith, but we also have to be careful to make sure, as we have seen in a lot of other areas, not necessarily this area, that when an agency gets a little leeway, sometimes they go farther than Congress wants them to go, so that forces us to be more specific as we move forward. So we just have to find the right balance in that.

You were talking about -- I am interested in auto industry, I am interested in computer science technology, and jobs available. And you were talking about the auto industry and 30 full-time equivalents, and then all of a sudden time ran out and you didn't finish your thought. Do you remember that thought, and can you finish, if you can.

Mr. Fu. Sure, sure. So, I mean, Michigan is known as a State with quite a bit of manufacturing, and many of these industries are trying desperately to hire cybersecurity experts. I found one. Many of them have come to me from the automotive industry. They also tend

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

to quit fairly often to go get other jobs. You have got to understand, at the career fair, you will see a line out the door for the Silicon Valley companies, the Googles, the Facebooks of the world. And for these other industries, it is very difficult for them to compete for this talent, not only because of the insufficient number of qualified skilled workers who are trained in appropriate security, but because just the competition is so great.

Mr. Guthrie. So hence, one of the major companies, industrial companies, General Electric's ads about -- so when the kid -- the young man going or woman going to work for General Electric say, I am going to go work for a high tech company, they go, well, you are going to work for General Electric. So maybe that is why they are pursuing that --

Mr. Fu. It is a good marketing strategy.

Mr. Guthrie. -- marketing strategy to try to get people to come work for them, yeah, absolutely, because they are -- exactly proves the point we are saying here. As a matter of fact, they make refrigerators right outside of my district in Louisville, just so that -- and they are very high tech. They are very high tech. As a matter of fact, they were showing me one I couldn't figure out how to operate the refrigerator. It was automatic coffee, pods, and everything in it.

Mr. Fu. My refrigerator tweets.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Mr. Guthrie. Yep. That is what they do there.

So let me ask you, in your testimony, you start with the basic premise that cybersecurity threats -- this is Dr. Fu -- are constantly evolving. This is a truism that we have heard reinforced many times. One of the issues is the identification of vulnerabilities. Can you tell us about how vulnerabilities are shared nowadays and if you have any recommendations moving forward on information sharing?

Mr. Fu. Sure. So there are many different ways to share vulnerabilities. In the consumer world, for instance, there is the US-CERT, which is a coordinating agency, works in concert with DHS, works in concert with Idaho National Labs and other places to collect information from security researchers and then provide it to manufacturers. That is just one pathway.

Other pathways are things like bug bounties rewards directly between the researchers and the companies. And then the third way that is becoming a little more disturbingly popular is just to sort of drop it in the public before there is a chance to deploy any kind of mitigating control or evaluate whether or not the report is true.

Mr. Guthrie. Okay. And you sort of talked about this earlier about that the hackers are going to look at the least secure device and then get into the system through that way, so -- but I was going to ask you this again, what is the general level of security included in consumer grade Internet of things devices, and have the recent

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

attacks prompted any conversations that you are aware of about the security included in those devices with manufacturers?

Mr. Fu. I have seen no good news about any security in any IoT device. Even in my own home, I have seen devices where I could trivially -- anyone on the Internet could just break in and take complete control. This was a device I just picked up in one of those big box stores. I have no good news on the security built in to IoT devices today.

Mr. Guthrie. Well, thank you.

Mr. Chairman, that concludes my questions. I yield back.

Mr. Latta. The gentleman yields back, and the chair now recognizes the gentleman from New Mexico for 5 minutes.

Mr. Lujan. Thank you very much, Mr. Chairman. And thank you for holding this important hearing, to you and to our ranking member.

As we all know, this is an important discussion since the proliferation of cyber attacks represents a serious challenge to both our digital and to our physical space. We saw the proliferation of cyber attacks this year all across the country, including with foreign actors as well being called out by our national security teams.

Pertaining to the development of Internet of things, which will provide a robust and important infrastructure for America, we also know that there is going to be more conflicts and dynamic networks that will result from that.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Dr. Fu, you talked about shadow devices. Currently, Los Alamos National Laboratory is looking at ways to use the data they collect from all devices connected to a network to monitor and protect against malicious attacks. The LANL work addresses the issue of dynamic and ill-defined networks with devices joining and leaving. It constantly monitors these ever-changing networks to detect and respond autonomously to malicious behavior.

Can you talk about the importance of us moving in that direction as well in developing this, maybe looking to national assets like our national laboratories and what we can learn there for tech transfer opportunities, whether it is in a secure space or an open space, to help us with these endeavors?

Mr. Fu. Well, I think what I can do is I can say there is -- NIST has a document that talks about how to do this kind of security well, and I hope LANL is implementing these. And one is you have to know your assets at risk, so you enumerate that, and it sounds like that is what you are referring to. The second is to deploy compensating controls that match those specific risks. And then the third one that we often forget as consumers and industry is to continuously monitor the effectiveness of those controls, and that is where it gets to the shifting threat landscape. You deploy a security product today, might be effective tomorrow, might not work at all.

Now, here is where I am a little skeptical of LANL and other

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

agencies that claim they know all of their networks. I know as a fact that most hospitals refuse to look at the security of their most sensitive networks because they are afraid of tipping over things like linear accelerators, radiation therapy devices, very sensitive machines. They have actually rebooted from very simple security products. So if you are in a facility that has nuclear materials, fissile material, I would be very skeptical of a claim where they have thoroughly vetted the embedded systems to see how well they have survived, unless they have actually tipped something over.

Mr. Lujan. Is there a benefit, though, with working with these national assets to assist us in the private sector?

Mr. Fu. I think there can be a benefit for safety-critical issues for places like LANL. I think there is quite a bit of expertise in what is called embedded security at many of the national labs. However, this is a very interdisciplinary problem, and I have seen this come up already in my vulnerability reports to different agencies. They will often tell me, I am sorry, we don't have an in-house expert on that particular subject of this healthcare situation, let me try to help you, and they usually have a difficult time finding a partner.

Mr. Lujan. Mr. Schneier, as more and more of our critical health, energy, and finance infrastructure is brought online, the things connected to the networks will need to be secured from inception to delivery. Are you able to speak specifically to what we can do with

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

securing the technology foundations and supply chains through the Internet of things, whether it be through semiconductor chips, secure IoT device operating systems, secure communication protocols, or secure device access management?

Mr. Schneier. So this is actually, I think, you know, part of the big problem. Security has to go all the way down. So someone there, I think, who left talked about that phone that surreptitiously, unbeknownst to the consumer, would send copies of your text messages to China. Now, on the plus side, it was cheaper, but you are not going to know, and that could be the software. We are worried about switching equipment that we use in our country that comes from China, because we worry about the hardware, that there might be some hardware switch that will eavesdrop or turn off in the face of hostilities. And these are very complicated questions. And any place in the stack, we can cause an insecurity that affects the others. Lots of people are working on this, there is a lot of tech here, but this is, I think, an extreme worrisome issue when we deal with global manufacturing.

So this is an American device made, I believe, in China. And many of our devices are made in countries that might not be as friendly to us at all times as we would like. And while we have tech that will hopefully detect these things, it is an arms race, and right now there is an edge on the attacker. It is easier to hide a vulnerability in something like this than it is to detect it.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Now, we also use that, right? I mean, the NSA uses that to spy on our enemies, so there is some good here too, but I think by and large it is dangerous for us.

Mr. Lujan. And, Mr. Chairman, as my time runs out, I think, Dr. Schneier, I will maybe submit a question to you pertaining to maybe expanded use of trusted foundries pertaining to hardware, and then we can have an expanded conversation in that space.

Mr. Schneier. I would be happy to.

Mr. Lujan. Thank you, Mr. Chairman.

Mr. Latta. Well, thank you. The gentleman's time has expired, and the chair now recognizes the gentleman from Texas for 5 minutes.

Mr. Olson. I thank the chair.

And welcome, Mr. Drew, Mr. Schneier, and Dr. Fu. I have to admit, last night I lost a little sleep preparing for this hearing all because we focused on September 21st of this year when a Mirai botnet launched a DDoS strike on the KrebsOnSecurity. Over 600 gigabits per second swarmed them. And then a month later, October 21st, the same bad actor went after Dyn.

I lost sleep because after 9 years in our Navy as a naval aviator, 8 years working with the Senate side as a senior staffer for two Texas senators, and four terms in the House, I know the biggest threat to our security and our prosperity is not bombs, it is not missiles; it is cyber attacks and cybersecurity, ones and zeroes.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

What bothers me most about what happened earlier this year is that the attacks -- the execution was exactly what Coach McHugh told me when I was 9 years old on the football field. He got his little -- drew a play in the sand: Here are the defenders, there are two over there. We will swarm them with four offensive people, score a touchdown. That is exactly what these guys did, nothing hard, nothing new, and yet they had the success of having 600 gigabits per second swarm KrebsOnSecurity.

And so in this environment, we can't be reactive. We have to be proactive. Our government has to be proactive. Now, I said the word "government" and said "proactive." Looking around the room here, some people shook their heads and smiled. They know those words don't go together, but somehow we have to come together to address this problem.

And, Dr. Fu, I love your term about we have to have it built in, not bolted on. I know Mr. Lance asked questions about that, but I want to further elaborate on it. Say you went crazy, you ran for Congress, you won, you are a member of this committee. How would you ask -- what do you think we should do to help out our American economy to make sure we control these attacks and be proactive instead of reactive? What is our role here in D.C.?

Mr. Fu. All right. Thank you. Let me first correct the build it in, not bolted on is actually a phrase my community has been using for many years, including Mr. Schneier is behind that quite a bit.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

But I would say to really get out in front of this problem and be proactive, we haven't even done what I would consider -- if I were talking with my students, I would say, you have to do your prelab first before you do the real work. And the prelab is actually going out and actually getting firsthand information from some of these constituents. I am doing that and that is where I am getting my firsthand information, from the executives themselves, from the engineers, and I am just picking up horror story after horror story. I can't relay that to you in this manner, because you haven't seen the people I have talked to. I think that needs to happen. I think there needs to be some congressional visits to these sites. I think they need to go to the universities, I think they need to see where the struggles are happening, what are the barriers.

I believe that likely after you see the same problems that I am seeing, you are probably going to start thinking about, we need to have incentive systems built in economically. I don't know what these are going to resemble. Could they be regulations? Maybe. Could they be more financial incentives or financial penalties? Maybe. Is it more about corporate liability? Perhaps. I don't know the answer on the mechanism, but I know that we need to get more people doing congressional visits to these sites to understand where the problems are borne.

Mr. Olson. Thank you.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Congressman Drew, your concerns about that how as we get involved in D.C., how laws -- if you could write laws, how would you write the laws to help your organization overcome this incredible challenge we have with these cyber attacks?

Mr. Drew. I believe -- I agree entirely with regards to us having the right incentives to make sure that, whether I am a business buying technology or whether I am a consumer buying technology, that we have the right incentives, whether they are economic, liability, or regulation. I completely agree with that mind-set.

And I do think that there are a significant number of existing frameworks with regards to each of those ideals around health, safety, convenience, and use with regards to these threats, as well as with regards to these technologies.

Mr. Olson. And very quickly, Congressman Schneier, your comments about how would you approach this from a Federal Government role.

Mr. Schneier. So I think you have a serious problem here, and I think we have in a lot of areas, that we are now at the point where the speed of technology exceeds the speed of law. And that has probably changed in the past decade or so. It used to be laws could lead technology and now it has reversed. And so we need to figure out a regulatory structure, an incentive structure, liability structure that is technologically invariant; that we can't focus on technology and

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

rely on them, but focus on people and incentives, because that is what is invariant. Technology will change.

And you are right, these DDoS attacks are kindergarten stuff. It is basic, it is not sophisticated, and yet highly effective. The sophisticated stuff is worse.

Mr. Olson. Thank you. I yield back the balance of my time.

Mr. Latta. Thank you very much. The gentleman yields back, and the chair now recognizes for 5 minutes the gentleman from Ohio.

Mr. Johnson. Thank you, Mr. Chairman. And thank you, gentlemen, for joining us today.

I -- you know, having spent nearly 30 years of my professional career in information technology, I want to get a little bit more into the technical aspects of some of the things we are talking about this morning, particularly traditional DDoS attacks versus these connected device DDoS attacks.

Mr. Drew, as I understand it, these DDoS attacks have been around almost as long as the Internet itself has. They have certainly gotten worse over the last few years, but at least for traditional DDoS attacks, we know that -- we know how to defend them against -- using techniques like IP address blacklisting or white listing and IP packet inspection, among other techniques. Can you tell us a bit more about those defensive techniques, why they have been successful in defending against traditional DDoS attacks?

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Mr. Drew. I would say about every 3 years or so we encounter an evolution of capability with regards to DoS attacks. Every 3 years or so, we have somewhat of a backbone impairment event on the global Internet that is resulting of adversaries developing new capability based on either new weaknesses or new technology and then directing that capability to the backbone. And so I would say that the community at large has been fairly proactive as well as reactive in investigating what those bad guys are doing, the techniques that they are evolving and shaping, and making sure that our capability to respond is built into the platform, or in some cases, bolted onto the platform by redirecting traffic and scrubbing it.

So what I would say is what scares us about IoT attacks is just the enormous potential scale, whereas, you know, the typical botnet that is involved in these attacks over the past handful of years to up to a decade has been in the tens of thousands. We now have the potential of devices in the millions. And network capability for filtering and scrubbing has not scaled at that sort of a factor. So it is something that we are taking with great notice and great pause to make sure that we can invest in our capability and technology to prepare for that.

Mr. Johnson. Is it safe to say that the majority of these defensive techniques have worked because they target the way that traditional DDoS attacks use spoofing and amplification?

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Mr. Drew. I would say that with regards to what the traffic looks like itself, meaning how that traffic is executed upon the victim, there have been slight evolutions in the way that that traffic looks, but for the most part, that the definition that has an upper and lower control in it, that is fairly well understood. And so the technology is geared to be able to operate within that sort of control parameter. It is really -- the big issue is the scale in which that the devices are coming at that victim and being able to launch those sorts of attacks.

Mr. Johnson. Okay. So to get kind of to the heart of the matter of why we are here today, because from what we have been told, this Mirai botnet doesn't use spoofing or amplification. Is that accurate?

Mr. Drew. That is correct. It uses what is called a shaped attack where it can send any protocol or any packet that it wants to.

Mr. Johnson. Okay. Instead, the botnet is built out of these individual connected devices, and you would say now there are potentially millions of them out there that are so numerous that spoofing and amplification aren't even necessary. It is the total -- it is just a deluge of traffic from those connected devices, correct?

Mr. Drew. That is correct. If you wanted to send a large amount of traffic in the past, you would use an amplification attack.

Mr. Johnson. Okay.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Mr. Drew. Now with devices like this, you don't need that.

Mr. Johnson. Well, you know, I think we need to dig into this a little more then, because when we were talking about defensive techniques before, most of those defensive techniques seem to rely on DDoS attacks that use spoofing and amplification. If a DDoS attack doesn't use spoofing or amplification, and you began to allude to it a little bit, how do techniques like IP address blacklisting or white listing or IP packet inspection work and how effective are they?

Mr. Drew. I would say, in fact, they are probably more effective on nonspoofed traffic. And so the overall capability to inspect and mitigate is more capable when the traffic is not spoofed. Again, I am going to go back to the scale issue, is that a lot of that technology is built for the, you know, hundreds of thousands of inspections at the same time as opposed to the millions of inspections at the same time.

Mr. Johnson. My time has expired, but I guess it is safe to say we have got a lot of work to do and we have got to stay on this because we have got to develop new techniques to handle this new threat. Correct?

Mr. Drew. Absolutely.

Mr. Johnson. Okay. Thank you, gentlemen.

Mr. Chairman, I yield back.

Mr. Burgess. The chair thanks the gentleman. The gentleman

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

yields back.

The chair recognizes the gentleman from Missouri, Mr. Long. Five minutes for questions, please.

Mr. Long. Thank you, Mr. Chairman.

And, Mr. Drew, I understand that newer brand name devices are generally safer and less vulnerable to cyber attacks, but how much blame would you put on low end manufacturers cutting corners on security with the type of attack that happened in October?

Mr. Drew. Well, with specific regards to the type of attack that happened in October, a vast majority of the devices were those low end manufacturers from other countries. We spoke to a vast majority of those vendors. Those vendors had not really contemplated the idea that their devices could be used in that sort of fashion. Some were mortified and were trying to wrap their head around how they could deploy cybersecurity. And, frankly, other manufacturers had no interest in deploying because they had every belief that their consumers would continue to purchase their product.

Mr. Long. Okay. This is directed to all of you. I guess we will start with Dr. Drew since he is T'd up there, but what are some ways hardware and software manufacturers can band together to prevent a cyber attack like the recent one?

Mr. Fu. So I would say --

Mr. Long. Maybe we won't start with Dr. Drew.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Mr. Fu. Oh.

Mr. Long. No. That is fine. I was just --

Mr. Fu. Okay. Were you referring to me? I am sorry.

Mr. Drew. He is Dr. Fu, I am Mr. Drew.

Mr. Long. Oh, okay. I am sorry.

Mr. Fu. But together we are interdisciplinary, and I would say the key point here is interdisciplinarianism for the hardware and the software.

There is a good -- function follows form. And if you look at the educational system, you will see that the people trained on hardware and the people trained on software don't actually have sort of the closest cultures in terms of education. I think it is going to be very important to educate people in a way that brings hardware and software together, because otherwise you are not going to have the workforce that is going to be skilled and trained to be able to solve these problems. So that is certainly something I am trying to do personally, is when I train students, I train them in both hardware and software, because you just can't abstract it away anymore.

Mr. Long. So, Dr. Schneier.

Mr. Schneier. So I think this is a particular challenge --

Mr. Long. Mr. I am sorry. I have got too many -- I can't see this angle with my glasses. I need new glasses or a different angle, I guess. There you go.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Mr. Schneier. I think it is a particular challenge, because engineering operates in silos. The companies that made those DVRs got a chip with software on it. They didn't inspect it, because it is a blob, and they put it in their device. They sold that device to some other company that put their name on it, and sold it to the consumer. And you have this chain which is very opaque, and companies will hand off to each other. So banding together, I think, is going to be very difficult. And the way we can do that is to incent it. If I have liabilities that go up the chain, if I have regulations that will affect each other, then I am giving the companies reason to not just say, yep, this works, I am going to put it in my device and I am going to sell it cheaply. This is -- it is hard, and I don't have a good, crisp answer. Hopefully Mr. Drew does.

Mr. Long. That is why we put him last.

Mr. Drew. Yeah. I would say that I agree with regards to cheap IoT. I think with regards to cheap IoT, the focus primarily is on the specific set of application that they are looking to develop. They get a -- they get hardware from another manufacturer, they get the baseline operating system from somebody else, and they just develop their application and don't really know how it all interconnects together as a global ecosystem.

I would say on more emerging IoT that is a bit more integrated and a bit more capable of being interconnected to other IoT devices,

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

we are seeing a lot more sort of discipline and knowledge with regards to marrying both hardware and software disciplines together, as well as being able to achieve higher security standards as they interact with each other from device ecosystems. So a long way to go, but a lot of growth in that particular area.

Mr. Long. Let me ask you something else. Could the recent cyber attacks have been avoided if the targeted sites registered with more than one company that provided the same services that D-Y-N provides?

Mr. Drew. Presumably, yes. What we did see, though, on the Dyn attack is that a number of the domains that were targeted, they fell back to another authoritative server, and the bad guy detected that and then launched an attack against that other authoritative server. So, you know, in this case, the bad guy was following specific victims and reacting to them as they mitigated and moved.

Mr. Long. Okay. Yeah. I heard you say that earlier in the opening. I think -- Dr. Fu, how's that? Is that okay? Dr. Fu, to what extent did default passwords play a role in these recent cyber attacks we have been discussing today?

Mr. Fu. So default passwords played a key role because it was the entry point to take over this army of unwitting agents to attack Dyn.

Default passwords are everywhere. In my testimony, I provided a graphic of default passwords for medical devices. There is nothing

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

stopping the same attack from happening to another industry, other IoT products. Default passwords are a big problem. The fact that we are even relying on passwords at all is a big problem.

Mr. Long. Okay. Thank you all.

My time has expired and I yield back.

Mr. Burgess. The gentleman yields back. The chair thanks the gentleman.

The chair recognizes the gentleman from Florida, Mr. Bilirakis. Five minutes for questions, please.

Mr. Bilirakis. Thank you, Mr. Chairman. I appreciate it very much.

On October 21st, the attack is unprecedented in size, and thought unforeseeable. On January 2015, the FCC staff reported the outlined security risks -- thank you -- Internet of things devices present, including potential attacks on other systems.

Dr. Fu, it appears that one of the reoccurring problems identified in your testimony is the use of insecure operating systems, which are actually easier to infect a target for distributed denial of service attacks. Have you seen industry react to these issues and move forward more stable operating systems, and are there impediments to making such a switch?

Mr. Fu. I have seen industry move to better operating systems, but like most communities, there is a wide distribution. There is a

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

leader, there is maybe not the leader.

I still see Windows XP, which is a decades-old operating system, in critical systems. There is a photograph of one Windows XP system in a water treatment facility in Michigan in my testimony controlling water pumps for the city.

Windows XP is susceptible to the last decade of already released malware. It doesn't take anyone, more than a kid in their basement, to be able to cause a problem. It hasn't happened, because no one's wanted it to happen.

It is all about the economics. Certainly on the high-end devices, like linear accelerators, for example, or radiation therapy devices, you are talking multimillion-dollar machines. Certainly when a hospital buys a new device, they are more likely to get a new operating system because it just comes with the new system. However, most hospitals have capital equipment costs. And they don't want to have to buy a new MRI or whatnot every 10 years. You know, it should last 20 or 30. This is why you will still see Windows 95 machines, you will see Windows 98 machines -- the year is important -- in hospitals, because when they go to the manufacturers saying, hey, we really want to have an operating system that we can keep secure, they will say, oh, sure, just why don't you buy a whole new machine.

And so there was this unwritten assumption that the software would be maintained. It may not have been written into the agreement, but

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

the healthcare community felt that it should have been kept secure, kept maintained, but from the manufacturing standpoint, it was, we have provided you this device.

Mr. Bilirakis. Thank you. Reports show that many devices used in the October attack were situated overseas. While some seek to regulate devices in our own country, how do we protect ourselves from devices that are outside the U.S.?

Dr. Fu, and then if someone wants to chime in, that is okay too.

Mr. Fu. Sure. Let me just comment briefly, and I will let my fellow witnesses opine.

I think the important thing about computer security is not to be able to put yourselves in a secure environment, but you need to be able to tolerate an insecure environment. We are never going to be able to make networks, you know, blissful places full of rainbows. The networks are always going to be hostile. So we need to make sure that whatever we put on there is going to be able to tolerate malicious traffic. DDoS attacks, however, are extremely hard to defend against because they cut at the core of where we are least prepared, and that is high availability.

Mr. Bilirakis. Anyone else want to comment on that?

Mr. Schneier. So it is two things. I think that U.S. regulation, especially if it is U.S. and Europe and some more major markets, can cause a new environment, which raises the tide for

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

everybody, because companies are not going to make two devices. They are just going to make one device and sell it. So we can make a difference with us and like-minded countries, like we can in so many other industries.

But Dr. Fu is correct that we can't assume ever a benign environment; that it is going to be a combination of making the devices that we can touch more secure, which means the integrated devices are more a minority, and then building infrastructure controls to secure against this malicious minority. And it will always be that.

Mr. Bilirakis. Thank you.

Mr. Drew, do you want to comment quickly, because I have one more question?

Mr. Drew. I was just going to say that we have a fundamental belief of ensuring that we can try to route packets on the backbone that are based on reputation. So the more that businesses and backbones can collaborate together on data and route traffic based on reputation, I think the better prepared we are going to be.

Mr. Bilirakis. Thank you.

One of the biggest concerns -- for Dr. Fu. One of the biggest concerns of the future distributed denial of service attacks is the potential impact on hospitals and their patients. We already know that hospitals are targets in other areas, such as ransomware hacks. Question for Dr. Fu: How can hospitals best protect themselves from

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

these threats and their current technology, and should industry prioritize the healthcare sector in preventing current cyber threats?

Mr. Fu. Right. Well, in the short term, hospitals are in a sticky place. There is not a whole lot of mitigating solutions. So the best medicine I can recommend for hospitals right now is to really know their inventory of medical devices. I saw some discussion yesterday in a DHS report about a bill of materials of software. Hospitals don't even know what software is running on the inside of their facility because the manufacturers don't know themselves what are on those medical devices. If we only knew what was on the medical devices, we could better understand what risks we are taking.

Mr. Bilirakis. Thank you very much.

I yield back, Mr. Chairman. I appreciate it.

Mr. Burgess. The chair thanks the gentleman. The gentleman yields back.

The chair recognizes the gentlelady from Indiana, Mrs. Brooks. Five minutes for your questions.

Mrs. Brooks. Thank you. I am going to follow up, Dr. Fu, and if you would explain a bit more about what -- your concern is is that the devices that are being used actually in the hospitals, the hospitals are not aware of what is on those devices. And so what kind of mechanisms should we have so that hospital systems are fully aware of what is in their hospital?

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Mr. Fu. Right. So let me just frame the context. So hospitals want to make sure that they have continuity of operations of their clinical work flow so they don't have to shut down, like the MedStar system shut down in this area for several days. And so the problem is when you don't know what your assets are, how are you going to protect that, if you don't know what ports are open? The manufacturers, they are not, I would say, willfully causing harm, as far as I know, but they are simply not providing enough information so that the hospital staff can do their jobs to assure the continuity of their clinical facilities.

So providing a bill of materials of what software comes on a device when it enters the hospital, it won't completely solve the problem, but it is going to really help, because you can't do step two until you do step one. You have to know your assets, you have to know your inventory before you can effectively control security mitigation controls.

Mrs. Brooks. And so while that has obviously lifesaving or life-ending implications, what other sectors are you most concerned about -- and this is for the panel -- that -- you know, that the sector integration, so to speak, of devices within maybe the system is not known?

Mr. Fu. I will just say public utilities, water, gas, electric. It surprises me how people just sort of laugh about, oh, we don't have

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

security, hahaha. And, you know, we are not going to be laughing when the lights go out.

Mr. Schneier. So I think looking at it in sectors is almost self-defeating. So what we are worried about is interactions. And, you know, if you asked somebody a month and a half ago whether a vulnerability in a Web camera can affect Twitter, you know, people would say no. And in a lot of ways, we barely know how the Internet works. I mean, Mr. Drew's answer of whether this particular defense would have mitigated this particular attack, and the answer was we are not really sure. And it is the emergent properties of interconnecting everything that causes the vulnerabilities.

We focus on a sector, we risk missing the big picture. And they are all computers, whether they have wheels or propellers or in your body, and they affect each other, they are on the same Internet. So I urge you to think holistically and not -- I mean, there are sectors that are more vulnerable, more critical, that is obvious, but the cause of the vulnerability could come from nowhere.

Mrs. Brooks. Mr. Drew, a question whether or not -- what your thoughts are as to whether or not hacking back or some other form of active defense should be permissible. Thoughts on that?

Mr. Drew. I know that this has been a fairly large debate within my industry. It has been a fairly large debate within the U.S. We have these conversations on a regular basis about green -- you know,

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

green viruses where if we know a particular exposure exists and we know that we can write software to go out and patch this system on the user's behalf to get the malware off the system, then we would be better protecting both the consumer as well as the Internet as a whole. And I think that that is a fairly dark road to go down. I think that it is an excuse for us not fixing the ecosystem and providing the right incentives in the right locations, and potentially has impacts that, you know, the author writing that software isn't necessarily aware of, as he is touching a pretty broad set of devices out on the ecosystem. So I would say I fear more of the consequences of that than I do pushing the right incentives in the right layers.

Mrs. Brooks. And going back to the question about whether or not we have the appropriate safeguards in place, we have 209,000 job openings right now, according to Dr. Fu, and what are the programs, degree programs or other types of certification programs, that should be offered that we are not offering enough in our higher ed institutions or training programs? And, you know, are degrees necessary or do we need to have different types of certifications short of degrees?

Mr. Fu. I think we need all of the above, especially it is a little known discipline called embedded cybersecurity, but this is very related to IoT, bridging the hardware and the software. I think we need both at the community college level, I think we need both at the four-year college, both in the graduate studies, also especially in

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

advanced master's programs for already skilled workers who are perhaps experts at building cars or designing cars but need to know how do you build security into that thinking. There aren't enough opportunities for those workers to come back to get that training.

And a final comment is the pipeline. I think in the engineering, in some of the sciences, we have difficulty, I think, attracting, tapping new resources, different demographics. I think we need to be much more -- doing much more outreach to high schools and some of the kids who are coming up to encourage them to go into these fields, and especially women and minorities.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

RPTR BRYANT

EDTR ZAMORA

[12:05 p.m.]

Mrs. Brooks. Thank you all for your work. I yield back.

Mr. Burgess. [Presiding.] The chair thanks the gentlelady. The gentlelady yields back.

And the chair recognizes the gentleman from Illinois, Mr. Kinzinger. Five minutes for questions.

Mr. Kinzinger. Thank you, Mr. Chairman.

Thank you all for being here, taking the time and elaborating on these issues.

Mr. Drew, for you, is it accurate to categorize the recent DDoS attacks as an international issue?

Mr. Drew. It absolutely is an international issue. The device manufacturers were foreign. The majority of the locations where the devices were located was foreign. You know, most of what we are talking about here today, from a regulation perspective, wouldn't have a direct significant impact on at least the adversaries that were involved in the October 21 attacks.

Mr. Kinzinger. Do you know, are there any other countries, international groups, et cetera, focused on these security issues right

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

now?

Mr. Drew. I mean, yes. I mean, there are a number of countries that are focused on very progressive cybersecurity controls. In Great Britain, as an example, there is a significant amount of cybersecurity work with regards to integrating that into the telecommunications sector, so -- meaning that if you are going to be offering telecommunication services or if the government is going to be purchasing services, you have to be certified at a certain cybersecurity level.

Mr. Kinzinger. So are you seeing, through these groups and countries, any kind of a consensus on how to move forward? And, I guess, what recommendations would you give to Congress to, in essence, marry up to that or work together on those issues, to help the conversation?

Mr. Drew. You know, I am going to go back to one of my original points, which is I do believe that we are missing, you know, defined standards in this space, that we can get some adoption around, that we can get some pressure focused on, and we can change buying and investment patterns.

I think that by setting those standards and by setting them by both domestic and international groups, whether it is NIST or ISO, you know, setting these standards so that you can force buying behaviors in both consumers as well as businesses I think is going to be a major

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

step forward.

Mr. Kinzinger. A lot of reports are indicating, as we have discussed, a staggering increase in the number of connected devices over the next few years. It is a number we heard today anywhere between 20 and 50 billion devices, which is unreal. What do you think policymakers and stakeholders should think about, in general, regarding cybersecurity and interconnection moving forward? What would be kind of the takeaway you would want us to leave with?

Mr. Drew. I think innovation is progressing faster than discipline. And, you know, what tends to happen is we go on a biorhythm of a lack of discipline causing significant unintended and unforeseen consequences. Our ability to adapt and respond to those is the thing that is going to keep that infrastructure protected and as well as continue to evolve it.

So I think that, you know, the average CSO has to manage 75 separate security vendors, and that is to bolt on security controls for products and services that they are purchasing. And when we get one of those dials wrong, there are some significant consequences as a result. And so focusing on making sure that premarket controls are placed in that infrastructure is going to be a significant adaptable win for us.

Mr. Kinzinger. Dr. Fu, Congressman Long brought up the issue of default passwords, and you stated that we should get away from passwords

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

all together. Can you elaborate on that?

Mr. Fu. I mean, so passwords are just intrinsically insecure. You know, we are human. We write them down. We choose poorly. So pretty much any password system is going to encourage unwise security behavior. There are some technologies out there. There is one company in Ann Arbor, for instance, Duo, that does something called two-factor authentication where you have, for instance, a mobile phone in addition to a password.

But at the heart of it, we need to figure out other ways. And I am going to defer to the other witnesses for suggestions on that. But I just feel we really need to retire passwords. We need to kill those off, because these are going to be bringing down our most sensitive systems.

Mr. Kinzinger. Do any of you want to elaborate on that at all?

Mr. Schneier. So I largely agree. I mean, there will always be a role for passwords. There will be low-security devices, applications, low amounts of latent time, times when you generally need security for a short amount of time. But, in general, passwords have outlived their usefulness, and there are other technologies. You can secure your Gmail account now with a code that comes to your phone as a second factor. I can sure this with my fingerprint.

There are many other systems that give us more robust authentication, and I think that would go a long way in a lot of our

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

systems to help secure them. Because we are talking about two different ways to break into things. We are talking about vulnerabilities, which are exploited; we are talking about bad user practice, which is also exploited. And if I can get rid of one of them or at least reduce it, I am going to go a long way to making things better.

Mr. Kinzinger. Okay. Great. Well, I am out of time, and thank you all for your time.

And I will yield back.

Mr. Burgess. The chair thanks the gentleman. The gentleman yields back.

The chair would recognize Mr. McNerney for the purposes of followup questions.

Mr. McNerney. I want to thank the chair for an opportunity to ask another question. This one is a little philosophical, so I hope you don't mind.

Mr. Schneier, you mentioned that the attacks are easier than defense on this complex system and making more complexity opens up new vulnerabilities. But biological systems work in the other way. They build complexity in order to defend themselves. Is there some kind of parallel we can learn from on this?

Mr. Schneier. So in the past decade or so, there has been a lot of research on sort of moving the biological metaphors of security into

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

IT, and there are some lessons and there are some things that don't work. Biological systems tend to sacrifice the individual to save the species, which is kind of not something we want to think about in IT or even, you know, in our society.

But, yes, there are ways of thinking about a security-immune system, but the complexity of a biological system is complexity that is constrained. So, for example, you know, we all have a different genome, and that gives us a resistance, our species, against a disease. And you might be able to do that with an operating system, but it is not going to be two or three, it is going to be billions of different operating systems, which is suddenly much more expensive by, you know, orders and orders of magnitude.

So a lot of the lessons don't apply. Some do, and the researchers are trying to learn from them. And that is kind of the new cool way of thinking, and I think there is a lot of value there. But still, complexity, unintended consequences, interconnections, the attack surface, the enormous attack surface we are talking about, makes it so that in at least the foreseeable future, attack will have the advantage. My guess is there will be some fundamental advances in security which will give us, maybe not in our lifetimes but eventually, a defensive advantage, but no time soon.

Mr. McNerney. All right. Thank you.

Mr. Chairman, I yield back.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Mr. Burgess. Thank you.

Mr. Schneier -- just recognize myself for a followup question. You had mentioned along this line and then you had mentioned in, I think, response to an earlier question about the autonomous vehicles. And, yes, yesterday in our Commerce, Manufacturing, and Trade Subcommittee, we did have a hearing on autonomous vehicles. So particular vulnerabilities or places where the focus should be as autonomous vehicles, self-driving vehicles develop as a separate entity.

Mr. Schneier. So I think it is a really interesting test bed for what we are thinking about. And I don't know how much detail you went into on the vulnerabilities. What we learn is the vulnerabilities are surprising. There is one attack that used the DVD player as a way to inject malware into the car that controlled the engine. Now, that shouldn't be possible, but surprise. And similarly, I am worried about the USB port on the airplane seat potentially controlling the avionics. The airline companies will say that is impossible, but those in computer security don't believe it.

So, again, the more holistic we can be, the better. There are always going to be surprises. So to get back to the immune system model, how do we build resilience into the system? How do we ensure that it fails safely and fails securely? How do we ensure or at least make it more likely that a vulnerability here doesn't migrate to another vulnerability there causing something more catastrophic? So the more

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

we can look at the big picture, the less we focus on this or that, because it is the connections. And so if you think about it, it is exponential.

I mean, I have five things, that is 25 connections. I have 100 things, that 10,000 connections. It goes up by a factor of square. I just did some math -- so sorry -- here, but -- now, that is the vulnerability, and that is why this is so -- that is why complexity is such a problem.

Mr. Burgess. Well, I mean, I had posed the question earlier, and, really, this is for any of the three of you who wish to answer, you know, the question of thinking like a criminal. But, you know, really, we are still playing checkers and they are playing three-dimensional chess or perhaps a multifactorial level of three-dimensional chess. So, I mean, what are the things that keep you all up at night? What are the things that you have wondered about?

Mr. Drew. I would say the best advancement in the security space for us, as an example, is behavior analytics. It is being able to monitor the network, monitor the enterprise, monitor our infrastructure, and look for behavior that we have never seen before to determine whether or not that is unauthorized traffic or not.

But no matter what, that technology is based on a compromise already having occurred, a bad guy already being in the network. And so our ability to be more proactive, our ability to get ahead of that attack and predict those attacks before they occur and change the

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

technology before they can be exploited, that is where we need to migrate.

Mr. Burgess. Mr. Schneier.

Mr. Schneier. I worry about catastrophic risk. You know, the Dyn attack is interesting. It was one person had the expertise to figure out how to do it. He encapsulated his expertise in software, and now anybody can do it. So it is unlike my home where I only have to worry about the burglars whom driving to my home is worth the bother. And there is some bell curve of burglar quality, and the average burglar is what I care about. On the Internet, it is the most sophisticated attacker I care about, anywhere in the world, because of the way computers encapsulate expertise into software.

Mr. Burgess. Dr. Fu.

Mr. Fu. I worry about something a little more human, and that is sort of bureaucracies. I worry about the inability to change. I worry about being stuck saying, well, we have never done it that way before. I worry about saying things like, you know, well, that is unprecedented. Well, the Internet of things is unprecedented and so there are going to have to be some changes. So I do worry that we won't have the strength and resolve to do it. It will take some guts, I think, but this is foresight.

In the safety world, we saw this with handwashing. In the 1840s, handwashing was not even a thought that crossed your mind until after

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Ignaz Semmelweis. It took 165 years to get to the point where handwashing is common. It is going to take some time for security, but the time is ripe to do something now and to do something wise.

Mr. Burgess. And I would just note for the record, I think Dr. Semmelweis did end up dying of a strep infection from not handwashing. So it --

Mr. Fu. He also messed up his experiments. He didn't write them up well.

Mr. Burgess. Well, wonderful. This has been a very informative hearing.

Seeing no further members wishing to ask questions, I do want to thank our witnesses for being here today.

Before we conclude, I would like to include the following documents to be submitted for the record by unanimous consent: A letter from the Online Trust Alliance; a letter from the National Electrical Manufacturers Association; a letter from the College of Healthcare Information Management Executives; a letter from AdvaMed, the Advanced Medical Technology Association; and a letter from CTA.

[The information follows:]

******** COMMITTEE INSERT ********

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Mr. Burgess. Pursuant to committee rules, I remind members they have 10 business days to submit additional questions for the record. I ask the witnesses to submit their response within 10 business days upon receipt of the questions.

I didn't say it, but, without objection, so ordered that all those things are inserted into the record.

And, without objection, the subcommittee is adjourned.

[Whereupon, at 12:17 p.m., the subcommittee was adjourned.]