CYBERSECURITY 2018

Online Security and Safety in Government, Industry and Civil Society

SALUTE TO VETERANS

A Special Report Published by The Washington Times Special Sections Department and Salute to Veterans

Cybersecurity 2018: Online Security and Safety in Government, Industry and Civil Society

The Washington Times
SPECIAL SECTIONS

Cheryl Wetzstein
SPECIAL SECTIONS MANAGER

Advertising Department:
202-636-3062

Larry T. Beasley
PRESIDENT AND CEO

Thomas P. McDevitt
CHAIRMAN

David Dadisman
GENERAL MANAGER

Adam VerCammen
DIRECTOR OF ADVERTISING & SALES

Patrick Crofoot
GRAPHICS SUPERVISOR

Special Sections are multipage tabloid products that run in The Washington Times daily newspaper and are posted online and in PDF form on its website. Sponsors and advertisers collaborate with The Times' advertising and marketing departments to highlight a variety of issues and events, such as The Power of Prayer, North Korea's Nuclear Threat, Gun Rights Policy Conference and Rolling Thunder Memorial Day Tribute to Veterans. Unless otherwise identified, Special Sections are prepared separately and without involvement from the Times' newsroom and editorial staff.

Innovation, modernization key to U.S. cybersecurity leadership

By Sen. Jerry Moran

In recent years, it has become clear that the world of cybersecurity is rapidly changing — cyberattacks are not only growing in volume, but also in complexity. As chairman of the Senate Commerce Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security, I've convened hearings and publicly questioned private corporations to determine what protections and practices they have in place to better protect their customers' personal and financial data.

In 2015, the U.S. Office of Personnel Management (OPM) experienced a breach that exposed the personally identifiable information of tens of millions of Americans. The danger that results from compromising the federal government's data cannot be overstated, and as companies must do all they can to prepare for and prevent hackers from gaining access to their customers' information, the federal government must do the same.

As advancements in information technology (IT) continue to shape our nation's evolving needs related to national security, economic competitiveness, communications, health care and privacy, the federal government must keep pace with these changes through flexible, expeditious and results-driven decision making.

In 2014, Congress enacted the Federal Information Technology Acquisition Reform Act (FITARA), which took the first step toward reforming the way our federal agencies make IT decisions. FITARA makes certain that subject matter experts are part of decision-making processes and enhances covered agency chief information officers' (CIOs) authorities related to agency modernization initiatives in budgeting and planning processes.

Still, a stringent and cumbersome budgeting and acquisition process has tied the hands of agency CIOs in their efforts to modernize their IT systems in an efficient fashion. The U.S. Government Accountability Office's (GAO) 2015 High-Risk Series report highlighted several issues it deemed critical to improving IT acquisition. Specifically, the report stated that about 75 percent of the $80 billion the federal government spends annually on IT investments is spent operating and maintaining outdated and unsupported legacy systems — draining taxpayer dollars and creating major cybersecurity vulnerabilities at home and abroad.

Earlier this Congress, I joined a number of my colleagues in writing to the 24 federal agencies covered by the Chief Financial Officer (CFO) Act, including the Department of Defense and the Department of Homeland Security, requesting updates on the modernization of their mission-critical systems. Unfortunately, the majority of agency responses indicated that they operated numerous insecure legacy systems.

President Trump and his administration have dedicated a plethora of resources to improve in this space through the president's establishment of the White House Office of American Innovation, which has helped guide critical executive orders to update aging systems.

Further, with the support of the administration, I partnered with Senator Tom Udall of New Mexico to introduce the Modernizing Government Technology (MGT) Act last April in the Senate after working together on earlier versions in past Congresses. The MGT Act establishes IT working capital funds at the 24 CFO Act-eligible agencies and allows them to use savings obtained through streamlining IT systems, replacing legacy products and transitioning to cloud computing for further modernization efforts for up to three years. The bill also sets up a separate, centralized modernization fund within the Department of the Treasury for the head of the General Services Administration (GSA) to administer across the federal government in consultation with a federal IT expert board.

It is only fitting that the MGT Act was signed into law last year as part of the National Defense Authorization Act for FY2018, as cybersecurity policy is increasingly interwoven into comprehensive national security discussions. As a member of the Senate Appropriations Subcommittee for Defense, I will continue to prioritize robust resources for cybersecurity programs across all federal agencies in the interest of national security. Additionally, a well-trained cyber workforce capable of upholding and supporting comprehensive, interoperable federal government systems will prove to be critical to this mission, paired with competitive science, technology, engineering and math (STEM) education programs that we must continue to prioritize.

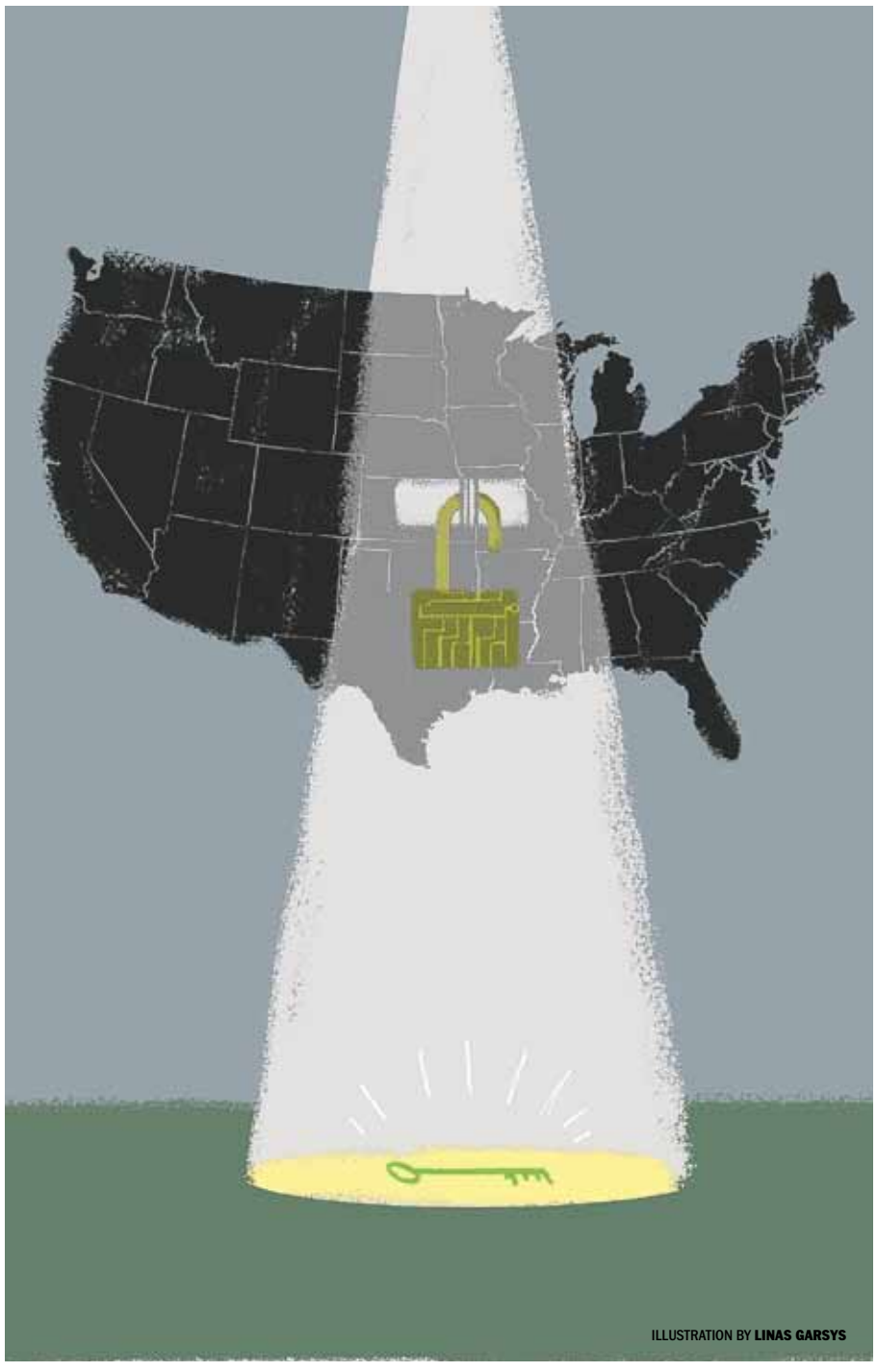


ILLUSTRATION BY **LINAS GARSYS**

My goal is to continue promoting modernization and security in the federal government's IT systems. As we recognize Data Protection Day on January 28, I appreciate the bipartisan, bicameral support the MGT Act received through its enactment and look forward to working with my colleagues and the White House Office of American Innovation on more legislation so America remains the most secure high-tech country in the world. We know the threats are real, and we must continue to innovate to remain the world's leader in cybersecurity defense.

Sen. Jerry Moran, Kansas Republican, is Chairman of the Senate Commerce, Science and Transportation Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security.

New bipartisan law will finally 'retire' outdated U.S. computer systems

By Sen. Tom Udall

The Internal Revenue system is using a nearly 60-year-old computer code to process tax returns and to maintain highly sensitive taxpayer information.

You read that correctly: The IRS relies on a computer system from the 1960s — the days of the Kennedy administration — to get you your tax refund and keep your personal data secure.

The only government building that should have a computer system from the 1960s is the Museum of American History. But across the federal government, agencies continue to depend on grossly outdated information technology (IT) systems to function.

The government's ongoing reliance on out-of-date technology comes at a time when hackers from across the globe are orchestrating ever-more sophisticated cyberattacks to target the American people. If you're one of the millions of Americans whose sensitive information was caught up in the Yahoo!, Equifax or Office of Personnel Management (OPM) breaches, then you know how serious and complex these attacks have become.

Our obsolete federal IT infrastructure is expensive, it's wasteful, and it's dangerous. And fortunately, we're finally taking action to fix it.

Last month, after lots of hard work behind the scenes and across the aisle, Senator Jerry Moran of Kansas and I celebrated the enactment of our landmark, bipartisan Modernizing Government Technology (MGT) Act. This new law will finally bring the federal government's IT systems into the 21st century.

Right now, the federal government spends $80 billion a year on IT — but a whopping 75 percent of that money is being spent to maintain so-called "legacy" systems that are no longer functional or up to the task. And agencies haven't had any incentive to limit waste — or to modernize or innovate the way they work.

The MGT Act will give federal IT managers the flexibility they need to make strategic IT investments and decisions. The law will free agencies to pursue modern IT solutions like cloud computing, which can offer more flexibility, better efficiency and faster processing time than the systems we're currently stuck with.

In addition, the MGT Act creates new flexible funding options for federal agencies to modernize their IT systems — and incentivizes agencies to eliminate waste. The law enables agencies to put the money they save every year into a working capital fund, which can then be used to pay for long-overdue technology improvements and major modernizations. And the MGT Act establishes a centralized fund that agencies can access to pay for major IT overhaul projects.

In total, the MGT Act will save taxpayers up to $20 billion a year. And as it saves taxpayer money, the MGT Act will also give federal agencies the tools they need to tackle dangerous cyber vulnerabilities and better protect Americans' data from cyberattacks.

The bipartisan, commonsense MGT Act will ensure that we're getting better service at a better value for the American people.

And it will help take those outdated, antique computer systems out of government offices — and put them in the history museums where they belong.

Sen. Tom Udall, New Mexico Democrat, serves on the Senate Appropriations Committee; Senate Committee on Commerce, Science and Transportation; Senate Committee on Foreign Relations; Senate Committee on Indian Affairs; and Senate Committee on Rules and Administration.

Stop WannaCry'ing? Step up leadership on cyber hygiene

By Joshua Corman

"Our dependence on connected technology is growing faster than our ability to secure it — in areas affecting public safety and human life." — @iamthecavalry

Through our overdependence on undependable information technology (IT), we have created the conditions such that the actions of any single outlier can have a profound and asymmetric impact on human life, economic and national security.

We need to find political will to lead on cybersecurity affecting public safety. We need to find it now.

As society increasingly depends upon technology, the importance of effective cybersecurity must evolve in kind. In the case of connected cars, connected medicine, Industrial Internet of Things (IoT), oil and gas, smart cities and the like, the consequences of failure will bleed into public safety and human life. We must be at our best.

There is a promise and a peril to connected technologies. Medical innovations are increasing access, reducing costs, improving care and enabling breakthroughs. But if we're cavalier about the perils, a single exotic death could trigger a crisis of confidence in the public or medical professionals to trust these otherwise superior technologies. We must be conscientious and proactive in managing these perils.

I had the privilege to serve on the Congressionally mandated Health Care Industry Cybersecurity Task Force. While we all knew the situation was quite dire, the headline of our summary graphic correctly and candidly stated: "Healthcare Cybersecurity is in Critical Condition." Within weeks of the June 2017 final publication of our findings, the WannaCry ransom worm took out 81 United Kingdom hospitals in a single day — over 40 percent of their national capacity. The U.S. got very, very lucky.

Worse, time is the enemy. There is notoriously slow movement in the relay race of public policy, regulation, research and development, buying cycles and deployment lifespans for safety critical technologies. We cannot wait for such a crisis to initiate necessary hygiene. Moreover, under duress, such reactions are often hurried and more prone to introducing unintended consequences.

We need to be more mature in our posture toward technology and accountability. Much debate over regulating technology sounds a good deal like "fire bad!" Clutching to clichés and talking points is burning valuable time for preparedness and corrective actions.

Over the last 30 years, we have been reluctant to regulate software and IT. There are a number of concerns that have fueled this — some valid, some now less so, and some never were. The chief concern has been a fear that such actions might "stifle innovation and hurt the economy." Malware attacks like Mirai launched from the long tail of low-cost, low-hygiene IoT devices showed us that a failure to regulate IT can "stifle innovation and hurt the economy."

Uncomfortable truths command uncomfortable responses. If we want to see something different, we need to incentivize something different.

We have technical solutions for many of our exposures. What we have lacked is motivation and will. In October, I testified to the House Oversight and Government Reform subcommittee on Information Technology about Virginia Democrat Sen. Mark Warner's IoT cybersecurity bill, which seeks more hygienic IoT for federal use. The House

» see **CORMAN** | C8

Salute to Veterans Series: Inspiring success, insightful discussion, resources, solutions and cybersecurity careers for our 22 million veterans

By Cyrus Zol

The Salute to Veterans Series delves into the top issues that our veterans and troops face daily. The TV series features vibrant discussions and provides advice and solutions from distinguished veterans who are also successful businessmen, community leaders and were accomplished college and/or professional football athletes: Rocky Bleier, Bryce Fisher and Greg Gadson.

Their personal stories of overcoming professional and personal setbacks following military service, while embarking on a fulfilling career path using the tools they learned in the service and on the football field, paints a picture of promise to our nation's veterans. They offer strategic insight and instruction to those troops and vets who will be transitioning into civilian life and facing unemployment or underemployment, seeking educational advancement, changing careers, becoming entrepreneurs and seeking career growth opportunities, namely, in cybersecurity.

This is just one important focus of the Salute to Veterans broadcast, which intentionally airs on military and patriotic holidays when awareness for our troops and vets are raised.

Cybersecurity among government, military, industry and consumers will continue to be a major priority in our lifetime. Cybersecurity career opportunities are growing rapidly in this country and 12 times faster than the overall job market; trained cybersecurity professionals are needed to defend the government and private industry networks. For the most part, veterans already have existing skill sets to transition from defending the country to defending our networks through cybersecurity jobs. With our veterans' highly sought-after traits of a strong work ethic, problem-solving skills, teamwork, situation adaptability and working under pressure to meet deadlines, our nation's heroes are well equipped to step into and excel in cybersecurity roles.

The cybersecurity field is full of opportunity for veterans, with or without degrees, and cybersecurity professionals report an average salary of $116,000 per year — almost triple the average salary nationwide. More resources should be established and maintained to ensure our troops and vets know how to access this information when seeking jobs in these fields. The U.S. is projected to have 500,000 unfilled positions within cybersecurity by 2021, but with our service men and women constantly returning to civilian life, this should not be our forecast.

The timing is crucial for our veterans and military service members to be aware of some of the resources, opportunities and solutions that are available to them within the promising cybersecurity industry. We can all do our part by spreading the word, both in person and in our daily communications, about this exciting opportunity for our nation's well trained and highly capable veterans, to continue protecting our nation through defending our nation's networks.

The internationally broadcast Salute to Veterans TV program for 2018 is hosted by PBS NewsHour anchor Lisa Dejardins and is just one of many available channels of information available to our troops and vets. Here are a few others:

- The Department of Homeland Security (DHS) is offering several free resources to veterans looking to expand their education and knowledge within the growing field of cybersecurity, with free on-demand video training, scholarship opportunities and a free, downloadable guide entitled "Veterans Cybersecurity Training and Education Guide."
- Veterans are able to log onto DHS's free cybersecurity training through the Federal Virtual Training Environment (FedVTE) and review some of the academic programs offered through the National Centers of Academic Excellence (CAE).
- The Forever GI Bill's expanded tuition assistance will further advance veteran opportunities within the lucrative cybersecurity field through removing the time limit to utilize benefits and increasing tuition assistance access among National Guard, Reservists and Purple Heart recipients.
- Veterans can seek cybersecurity degrees that are becoming increasingly offered at universities, colleges, community colleges and online educational institutions nationwide. Since 2009, more than 350,000 veterans have earned postsecondary certificates and degrees through the GI Bill.
- The SANS Institute is the largest source for information security training and security certification in the world. The SANS Institute provides training for defending systems and networks. The training can be administered in a class with SANS-certified instructors through online education or in mentored settings, reaching more than 30,000 people in the U.S. and internationally. In 2015, SANS launched its first VetSuccess Academy, giving veterans the opportunity to receive advanced technical training, GIAC certifications, and employment opportunities among leading companies offering exciting cybersecurity careers.

(From left to right), PBS NewsHour Anchor Lisa Desjardins, Rocky Bleier U.S. Army Veteran, 4-time Champion with Pittsburgh , Greg Gadson U.S. Army Veteran, Honorary Captain & 2-time Champion with New York and Bryce Fisher U.S. Air Force Veteran, 1-time Champion Runner Up with Seattle

Veteran employment has greatly improved nationally; however, hundreds of thousands of transitioning service men and women will continue to enter the workforce over the next few years, many of whom are qualified to fill these many open positions. A recent report from ISACA found that 55 percent of organizations reported that open cyber positions take at least three months to fill while 32 percent said they take six months or more. And 27 percent of U.S. companies said they are unable to fill cybersecurity positions at all.

Overall, veterans have an understanding of technology and IT through their training and military experience. With the cybersecurity unemployment rate at 0 percent, the timing is ideal for veterans to enter the cybersecurity job market.

Legendary businessman and philanthropist Warren Buffett warned last year that cyberattacks are a top priority that needed to be addressed worldwide and that "I don't know that much about cyber, but I do think that's the number one problem with mankind."

The U.S. veteran population can position themselves for success, given their mission-critical military experience and knowledge of security procedures, into this ever-growing field.

Now is the time.

SALUTE TO VETERANS

Cyrus Zol is creator of the Salute to Veterans Series, a televised series covering the top issues that our veterans and troops face daily, including veteran employment and cybersecurity opportunities among our nation's 3.3 million U.S. active-duty service members, reservists, and 22 million veterans. The veterans' series spotlights veteran success stories, discussion and solutions for important veteran issues and advocacy in advancing the interests of our nation's veterans. The TV program is hosted by PBS NewsHour anchor Lisa Dejardins and airs during the military and patriotic holidays nationwide and internationally to our troops and their families serving in 174 countries and U.S. Navy ships at sea. Visit www.salutetoveterans.org for more information.

Reducing security risk by protecting enterprise applications

By Justin Somaini

Relentless threats from increasingly sophisticated attackers. Organized crime and rogue nation-states. Hacktivism and new mechanisms of compromise. Many years ago, the prospect of these security challenges seemed like something out of James Bond. Now I defend organizations from these threats every minute of every day.

Cybersecurity is an endless journey for organizations, including government agencies at the federal, state, city, and county levels. Facing an ever-changing threat landscape, public administrations know they need to protect IT systems and critical infrastructure. Less understood, however, is the need to secure enterprise software applications and solutions.

The data and transactions processed by these applications represent the operational center of many agencies, entities, and organizations. This is especially true in oil and gas, aerospace, defense, public sector, and utilities. Ensuring deep security at the application layer — where data resides and transactions radiate to networks and the endpoints beyond — is a fundamental requirement.

But the vast majority of software companies fail to implement security as an integral component of their applications. Most software offers only the most basic security protections for data and transactions, enabling organized groups and individual actors to easily exploit security weaknesses. In many products, protection is applied as an afterthought — a Band-Aid intended to compensate for a lack of security at the application layer.

Government and business leaders typically are surprised by this. They believe that their collection of security tools will protect their organization from the bad guys and that applications placed behind their firewalls are safe. Nothing could be further from the truth.

The solution to this problem is double-sided. Enterprise software vendors need to employ more mature cybersecurity technologies. And decision makers need to make security a higher priority when choosing and deploying enterprise software.

Because SAP solutions handle the most sensitive data and transactions of more than 300,000 of the world's largest companies and institutions, we consider security one of our highest priorities. Our focus is on incorporating advanced, threat-based security features in all of our applications.

This approach differs from that of other software vendors whose security features are designed to meet the minimum requirements needed to attain compliance certification. For government and industry regulators, compliance mandates are the only way to raise the bar when it comes to protection. But public sector executives must realize that regulatory compliance is the lowest bar — one that cannot and will not address all of their security concerns.

Instead, IT departments must build out a security strategy, using software that offers enhanced protection out of the box. To stay one step ahead of hackers and bad actors, it's important to choose vendors that are committed to continuously improving and updating their products.

To help organizations become secure and protected, we aim for the highest bar: targeting the actual threat. Organizations that want to reach beyond compliance should look for enterprise software that includes advanced security features, such as:

- Sophisticated 360-degree correlation analytics across the network, endpoints, applications, and data.
- Real-time incident response and forensics to accelerate detection, limiting the impact of threats.
- Next-generation context- and application-aware firewalls to enhance both protection and performance.
- Deep, machine learning-powered cybersecurity analytics that respond to threats in an adaptive manner.

Focusing on securing critical infrastructures helps ensure they can be defended against both physical and digital threats. In doing so, organizations can protect everything from logistics and operational management to HR systems and vendor interactions.

Protection should also extend to the burgeoning network of Internet of Things (IoT) sensors and devices. In the last few years, we've seen customers use IoT security features to keep trains running in Italy, cranes operating in Dubai, and city streets well-lit and safe in Germany.

To stay ahead of the increasing number and variety of threats, we continue incorporating new technology into our solutions. Today we're exploring new ways to use artificial intelligence and machine learning to identify new or previously unseen attacks. Our upcoming generations of software should be able to identify and prevent attacks from within the application, store data in the cloud, protect it from outside control, and minimize vulnerability across the IT landscape.

As public sector organizations consider transforming their cybersecurity strategies, there are several key steps they should consider.

Take care of the basics. Breaches are more likely when there is a consistent lack of patch management, configuration management, and log analysis.

Implement mechanisms that enhance visibility. Networks are more complex than ever before, with digitalized businesses connected throughout the value chain and executing as one. Security solutions that increase cross-enterprise visibility can help organizations identify and stop malicious activity.

Prioritize ease of use. Traditional security solutions often created hurdles that compromised the protectiveness of the technology. With powerful security features embedded in their applications, organizations can expedite and streamline protection.

Finally, get started identifying the most sensitive data and transactions in your network and know where they reside. By combining enhanced security knowledge with enterprise software that offers security at the application layer, you can better defend your organization against today's — and tomorrow's — most difficult threats.

We're all in this together. And we don't need James Bond to figure it out. By joining forces to tackle cybersecurity challenges, software vendors and public sector organizations can enable secure IT environments that support your timeless mission of protecting the community, providing services, and helping the economy prosper.

For more information on how you can ensure deep security at the application layer, visit https://www.sap.com/corporate/en/company/security.html

Justin Somaini heads the SAP Global Security (SGS) team. With more than 20 years of information security experience, he is responsible for SAP's overall security strategy, ensuring that SAP and our customers have a consistent and convenient security experience and establishing SAP as a recognized and trusted leader in the industry. In his role Justin is accountable for three core domains — Physical Security, Product Security, and Enterprise Security — for all of SAP.

Preparing now for safe, secure self-driving cars and other innovative technologies

By Rep. Bob Latta

There really isn't anything quite like American innovation. What makes U.S. innovation so different is that it's not just one field or sector; it's an ethos that inspires business across the country. Whether it's due to Americans' work ethic, an entrepreneurial spirit or a framework that allows innovators to succeed, the United States is second to none when it comes to creating technology that improves our daily lives.

With that in mind, the U.S. Constitution empowers Congress with an important duty — included in the Commerce Clause — to provide oversight of interstate and foreign commerce. This constitutional power is central to the work of the 223-year-old Energy and Commerce Committee, the oldest continuously standing committee in the House of Representatives. While none of the members of the Committee have been around since its inception, it's fair to say much has changed over time — from horse-drawn carriages to the Ford Model T to the potential of fully self-driving vehicles — but the committee has always provided stewardship over American innovation, promotion of commerce and protecting consumers.

Not only are we examining present-day issues involving consumer safety and technology, we are looking ahead to the future of innovation — what is coming five or 10 years down the road. With the promise of new innovations and technological capabilities coming our way, the landscape is ever-changing.

The number of connected devices is on the rise, and our digital economy continues to grow. American consumers have come to expect the speed, choice and convenience of online shopping, digital commerce, on-demand credit, mobile payments and much more. While most Americans feel that technology positively affects society and our everyday lives, polls show they are skeptical about how personal information is used and protected online.

Recent data breaches from Equifax, Uber and other companies raise the specter about the protection of consumers in a data-driven economy. Breaches involving sensitive personal and financial information are a serious threat to the well-being of American consumers and our economy. Last fall, the Subcommittee on Digital Commerce and Consumer Protection — which I chair — made solid progress in examining data breach and cybersecurity issues. Through a number of public hearings, including testimony running the gamut from the former CEO of Equifax to renowned cybersecurity experts, we learned about the challenges to protecting consumer information while ensuring access to the services they want.

These issues remain at the top of my agenda in 2018. The subcommittee has already begun working with a wide range of stakeholders on potential proposals and recommendations that can incentivize security and help prevent breaches of personal and financial data.

Another consumer protection issue that continues to be on our radar is self-driving cars. We need to make sure these vehicles are safe for consumers and at the same time promote innovation in this space. That's why we passed the SELF DRIVE Act — a first-of-its-kind piece of legislation — to do just that. It passed the Energy and Commerce Committee in a bipartisan 54-0 vote and then received unanimous approval in the House.

This bill helps ensure that self-driving cars are safe by focusing on both structural features and cybersecurity. In fact, the legislation makes clear that auto manufacturers cannot sell or introduce into commerce a self-driving car unless a cybersecurity plan has been developed. This legislation is also important for our senior citizens and for individuals with disabilities as autonomous vehicles would increase mobility.

As this technology is already underway and further development continues, the SELF DRIVE Act provides a clear, consistent framework under which innovation can thrive. We remain committed to working with our Senate colleagues and getting self-driving car legislation to the president's desk. This is an important step for consumer safety and innovation as more and more of this incredible technology reaches America's roads.

We're also looking at the challenges and implications that come with the Internet of Things (IoT). IoT is the name for the network of connected devices, services and objects that collect and exchange information. IoT applications, like smart home devices and wearable technologies, can offer significant benefits to consumers by providing quick responsive services, convenience and enhanced user experiences.

However, cybersecurity remains an ever-present concern for any internet-connected device. Constant vigilance and improved coordination are necessary to help prevent bad actors from taking advantage of weaknesses. With so many of these items now in homes and businesses across the country, our committee continues to examine the privacy and security concerns associated with IoT.

As a result of advancements like the Internet of Things, self-driving cars and digital commerce, the American people are more connected to information and opportunity than ever before. My goal on the Digital Commerce and Consumer Protection Subcommittee has always been to act in the best interest of the consumer and the American people. In any policy decision, we must anticipate what's coming next in the fast-paced environment of innovation. The tremendous benefits of our internet-enabled, data-driven economy need not be at the expense of safeguarding consumers' personal information.

Rep. Bob Latta, Ohio Republican, is Chairman of the House Energy and Commerce Subcommittee on Digital Commerce and Consumer Protection.

CORMAN

From page **C4**

Energy & Commerce Committee asked the Health and Human Services Department to enact one of our Health Care Task Force recommendations: create a software "bill of materials" (or ingredients list) for medical technologies. Two Members of Congress, Rep. Will Hurd, Texas Republican, and Rep. James Langevin, Rhode Island Democrat, joined me at DEF CON®, the world's largest hacker conference in August. Earlier that summer, the Cyber Med Summit in Phoenix saw the first hospital hacking simulations with medical stakeholders. I am hopeful these discussions take root.

From a policy perspective, Mirai disrupted the "prior prevailing hopes" with regards to lighter touch regulation/policy. There was the belief that adding transparency, security "nutrition labels" and a software bill of materials would enable consumers and purchasers to better discern "more secure products" from "less secure products." The bulk of discussion was about enabling free market choice. Mirai revealed the externalities challenges and "tragedy of the commons" aspects of our interdependence. Yes, transparency can enable informed and conscientious individuals to buy a safer product, but choices made by others can still hurt us — severely.

At current hygiene levels, the stunning growth rate of IoT and connected technologies represents a public health issue. Hackable — but unpatchable technologies — cannot remain the norm. If you add software to something, you make it hackable. If you connect something, you make it exposed. While this was bad enough when it was $100 internet cameras taking out the Internet for an afternoon, we will surely regret it when a similar attack is comprised of life-and-limb medical equipment and patient care and actual lives are impacted.

Mirai, WannaCry, NotPetya and attacks on the grid and critical infrastructure are increasing. If we are overdependent on undependable things, we have choices: Muster the will to ensure these things are more dependable or depend upon them less. We are prone. We are prey. Predators have taken notice. Our relative obscurity is over. What will we do about it?

Joshua Corman, a nationally recognized security expert, is Chief Security Officer and Senior Vice President at PTC. He is Founder of I Am The Cavalry (iamthecavalry.org), a global, grassroots organization that focuses on issues — such as medical devices, automobiles, home electronics and public infrastructure — where computer security intersects public safety and human life. @joshcorman.

Time's up for poor cyber hygiene

By Rep. Anna G. Eshoo

On Jan. 30, President Trump will deliver his first State of the Union address to Congress. The purpose of this constitutionally sanctioned speech is to reflect on the challenges facing our country and policies to address them. One challenge that must not be ignored is the ongoing threat of cyberattacks to our personal security.

Last year was one of the worst years for cyberattacks in U.S. history. In May, the WannaCry ransomware attack affected hundreds of thousands of computers in more than 150 countries, including the U.S., and held computers hostage until ransoms were paid by owners to restore access. This new type of ransomware, which we later learned was launched by the North Korean regime, exploited known vulnerabilities in computers that failed to install basic software patches.

The WannaCry attack was soon dwarfed in comparison by the Equifax data breach, which compromised the personal information of nearly 146 million Americans including names, Social Security numbers, birth dates, addresses and driver's license numbers. Appearing before the House Energy and Commerce Committee, Equifax's now-former CEO announced that the breach was reportedly caused by the failure of a single Equifax employee to install basic software updates in a timely manner. Altogether, the personal information of hundreds of millions of consumers was exposed to malicious hackers last year, and it's likely yours was too.

Despite the severity of these attacks and the pronouncements of outrage by Members of Congress, no sensible legislation has been advanced to prevent a similar attack from happening in the future.

If we're actually serious about protecting ourselves from data breaches and cybercrime that increasingly threaten our daily lives and personal security, we have to address the twin pillars of network security: cyber hygiene and security management.

Cyber hygiene is the responsibility of all Internet users to take basic and proactive steps to secure networks and devices. Installing software updates to patch known vulnerabilities; using strong, secure passwords; and utilizing modern firewall and security techniques are some of the hallmarks of good cyber hygiene. As an entire network can be compromised by a single individual's neglect of cybersecurity, as in the Equifax case, maintaining good cyber hygiene is imperative.

The other essential pillar of cybersecurity is security management. It is the responsibility of organizations to maintain secure networks. Businesses and government agencies can greatly reduce the incidence of cybercrime within their networks by implementing security controls, classifying sensitive data, and creating and practicing attack response plans. Vigilant security management, coupled with good cyber hygiene, is a recipe for keeping our digital systems secure.

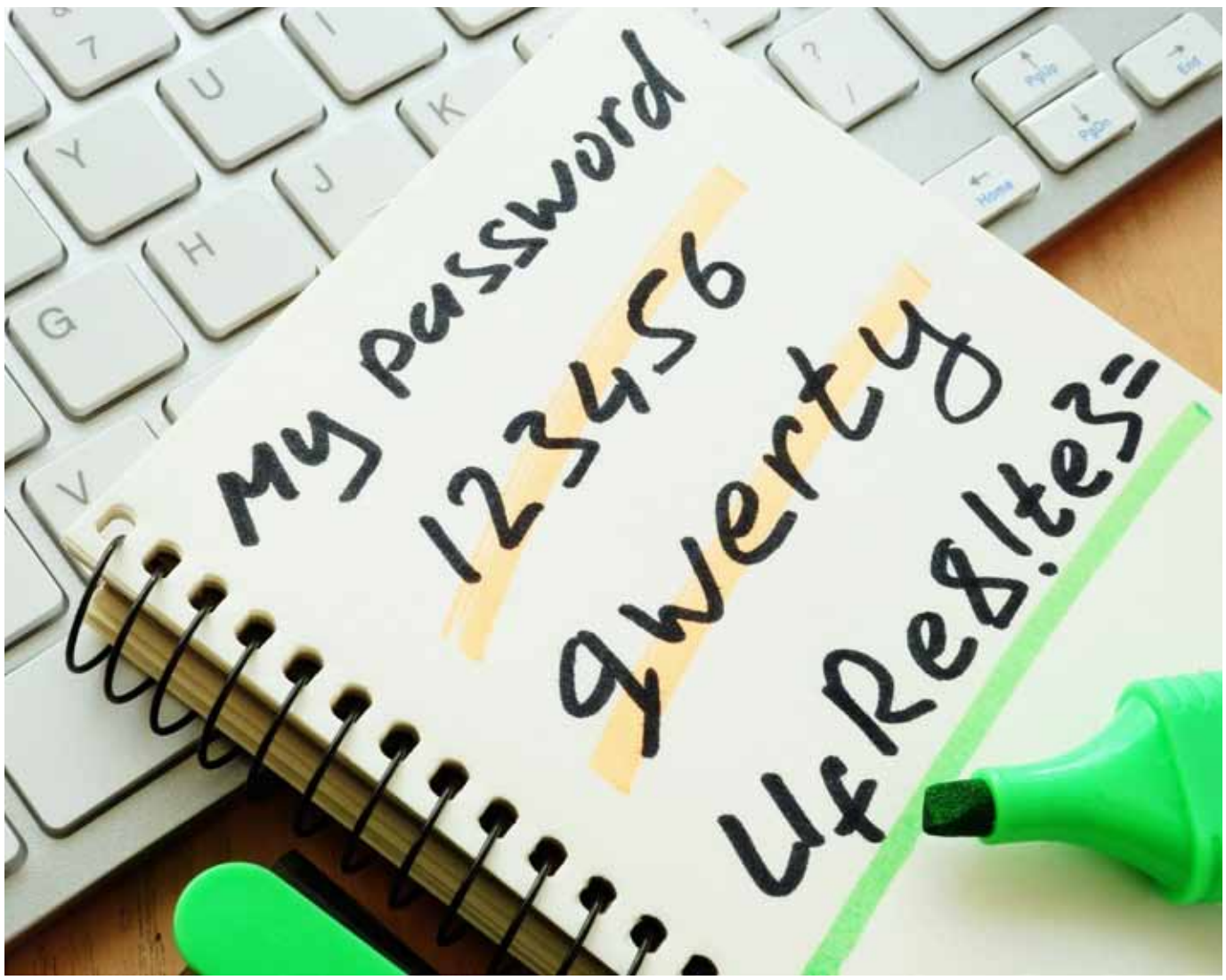
In the wake of last year's attacks, I introduced the bipartisan Promoting Good Cyber Hygiene Act to strengthen both pillars of American cybersecurity. The bill promotes cyber hygiene by instructing the National Institute of Standards and Technology (NIST) to maintain a user-friendly list of cybersecurity best practices that is easily accessible to the American people. As security protocol is constantly evolving, this list of up-to-date best practices will be prized by anyone seeking to improve their cyber hygiene.

This bill also strengthens cybersecurity management within the federal government by mandating that the Department of Homeland Security regularly assess cybersecurity threats and work with agencies to address them. As the federal government curates the most sensitive and vast collection of data on Earth, it is central to our national interest to keep that data secure.

In today's ever-increasing digital world, the American people need to trust the Internet with their most sensitive and intimate information. From online bank accounts to medical records, the information we store and transmit online must be protected. For the state of our union to be strong, it is imperative that Congress act this year to improve our nation's cybersecurity. The digital systems that sustain our way of life are vulnerable to attack, and we must act to protect whatever the American people deem as private and whatever our government deems as essential to our national security.

If we're actually serious about protecting ourselves from data breaches and cybercrime ... we have to address the twin pillars of network security: cyber hygiene and security management.

Democrat Rep. Anna G. Eshoo represents the 18th Congressional District of California. She is a senior member of the Energy and Commerce Committee.



The 3 prongs of a sound cybersecurity strategy

By Rep. Robin Kelly

ILLUSTRATION BY GREG GROESCH

In 2018, our security can no longer exclusively be defined in terms of tanks, airplanes and weapon systems.

As government, private industry and American families have adopted technology into nearly every aspect of our lives, the need for cybersecurity has grown exponentially. Unfortunately, our response to this threat has been piecemeal at best.

In order to combat this real and growing threat, we need a three-pronged approach that involves everyone from Washington D.C., to Chicago to Silicon Valley and everywhere in between.

Prong One — Washington, D.C.: On too many issues, business as usual is either broken or ineffective within the Beltway. Thankfully, one area where we are making strides through bipartisanship is in cybersecurity.

I'm privileged to serve as the Ranking Member of the House Oversight and Government Reform Subcommittee on Information Technology with Chairman Will Hurd, Texas Republican. It would be difficult to find someone in Congress, or frankly anywhere else, who has more experience and understanding on these critical issues.

Together, we have been able to craft legislation in an open, process-driven way that will revolutionize government IT acquisition, increase cybersecurity and save taxpayer dollars. This legislation, called the Modernizing Government Technology (MGT) Act and signed into law in December, is an important first step. Still, more work remains to ensure that all government data is protected from today's and tomorrow's cyberthreats.

Right now, I'm working on pieces of legislation to ensure baked-in security measures for internet-connected devices like webcams and to help agencies better manage their IT inventory. Additionally, Chairman Hurd has proposed the idea of a Cyber National Guard to increase cybersecurity talent within government; I support this commonsense proposal.

While these are good ideas, they achieve nothing if they are trapped in our subcommittee. When we worked on the MGT Act, we held field hearings and hearings in Washington, we allowed amendments, and we worked across the aisle to craft the best possible plan. Congress needs to do more of this. We need to work on legislation together, not in party-driven ideological silos. Let's actually allow the space for the best ideas to come forward. When it comes to cybersecurity, we cannot afford to let good policy sit on the shelf because of whose name is on the sponsor line.

Prong Two — Every Community: When it comes to combating cyberthreats, we need everyone from every community involved. According to the Level Playing Field Institute, there will be 1.4 million new tech jobs by 2020 and 70 percent will be unfilled. Many of these jobs will be devoted to cybersecurity or play a critical role in cyber defense. We clearly cannot allow the vast majority of these jobs to remain open; we need to redouble our efforts to train new workers, retrain mature workers and inspire students to pursue STEM careers.

In order to meet the bourgeoning demand for new cybersecurity and tech professionals that our economy needs, we need to reach into every community: suburban, veteran, working class and communities of color. With this great need, we cannot allow someone's ZIP code or background to lock them out of these opportunities.

One real challenge we face is that just 22 percent of schools with AP programs offer computer science coursework and nationwide nearly 30 percent of schools do not offer any AP coursework. This means that thousands, if not millions, of American students are blocked from learning critical skills that could open the door to a career as a cyber professional. The first step toward addressing this crisis is to get more computer science teachers into the classroom. My Today's American Dream Act includes a provision that would incentivize people to teach computer science by helping to pay off some of their student loan debt.

Prong Three — On Every Computer: Combatting cybersecurity is not someone else's responsibility. It is everyone's responsibility. In October 2016, household kitchen items were used to knock out Internet access to users on the East Coast. It should not be that easy for cybercriminals to exploit these vulnerabilities, and families can take simple steps to prevent it.

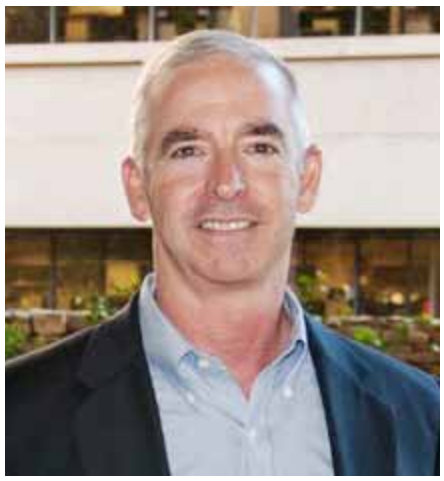
As new cyberthreats continue to grow and evolve, every person needs to take these issues seriously and be proactive in stopping them. There are simple, everyday things that every person can do, even with limited technical expertise, to make themselves, their data and the entire system safer.

These include simple things like multifactor identification (when you receive a text with a code to confirm a login) and using only trusted Wi-Fi networks and passwords that are secure (please stop using Password123). Trust me, you want to do these things before your data is compromised or your bank account is drained, and it will help make everyone and the system safer.

We still have a lot of work to do to bolster cybersecurity. We are starting to make the right steps and now is the time to go from small steps toward giant leaps. Technology and hackers will not wait.

Democrat Rep. Robin Kelly represents Illinois' 2nd Congressional District. She serves as the Ranking Member of the House Oversight and Government Reform Subcommittee on Information Technology.

Fighting cybercrime: A shared responsibility for the nation, home and workplace



By Gary McAlum

Cybercrime is an unfortunate reality in our world today. It is something that has become common language, and many Americans have become fatigued and numb to the continuous cyberthreats.

This is why Data Privacy Day is important to me and my team. It is an opportunity to reinforce to consumers the importance of always being vigilant and allows us to continue the conversation of what we can do to better protect ourselves from cyberthreats.

Throughout my military career of 25 years with the Air Force, I had the opportunity to work in a variety of IT and technology roles, but the positions involving cybersecurity were the most challenging. The scope and magnitude of cyber issues facing our nation became crystal clear to me, and I realized I wanted to continue to work in this important area for a company like USAA after retiring from the military.

At USAA, my team is responsible for protecting our more than 12 million members from cybercrime. It is an honor to serve our military, veterans and their families and help stop more than 9 million cyberattacks and prevent $8.7 million fraud loss daily. This data point makes me proud of our team, but it also reinforces the important fact: Threat is real and never-ending.

Oftentimes, consumers think that they are immune or safe from cybercrime. However, as a veteran, I have been the victim of many data breaches and, most recently, was a victim of the Office of Personnel Management (OPM) breach. In this case, I knew what type of information was compromised from the sensitive information I provided for my security clearance.

The data compromised wasn't just my information; my family was impacted as well — and received letters from OPM directly. Knowing that my family members were now victims of identity theft for the rest of their lives made me angry. I understand firsthand the frustration of being a victim of identity theft, and I carry it with me every day in protecting our members at USAA. They depend on us, and I know how they would feel if it happened to them on my watch.

I've also experienced a wide range of cyberattacks directly, ranging from phishing emails to fraudsters attempting to impersonate me or even call me pretending to be a company I trust. At USAA, we reinforce that fighting fraud is a shared responsibility and try to reiterate some of the key ways to protect yourself from cyber threats:

Multifactor authentication (MFA): The reality is our personal information is already known or easily available. The most effective thing we can do to protect our online accounts is to use strong authentication. If your online account offers options beyond passwords and security questions, please consider them. I use a combination of the random code option — a one-time security code that is texted to me — and biometric options when available, including fingerprint, voice or facial recognition.

Better passwords: When you don't have access to MFA options, it's critical to use a strong password that includes a mixture of symbols and letters. The key is to change it up — don't use the same password for all accounts.

Stay vigilant: Phishing is a common tactic to gain your personal information, and fraudsters prey on individuals hoping the user clicks a link or takes actions without acknowledging red flags. Fraudsters will often call you directly impersonating a credible company. Bottom line, follow your senses. If in doubt, pause to confirm you really want to proceed.

Monitor your info (and your children's accounts): We tend to focus on steps to avoid identity theft for ourselves but may not think about our children. This is a growing trend and can be difficult to detect and resolve. Make sure to review your information and respond to any security or fraud alerts.

Many individuals may feel online security seems like a lost cause. The reality is that it's a risk management situation, and we have the ability to minimize some risks by the actions we take, or don't take. As consumers, we can take control by embracing these tips into our daily lives. Fraud will always exist — the key is to make it as difficult as possible so the fraudster will prey elsewhere.

As the chief security officer at USAA, my team stands strong to protect our members' information. This commitment requires a 24/7 mindset and offers no room for failure. We have the best talent on our team, and a solid percentage are veterans or military spouses. While we were honored to receive the "Best in Class" award in Javelin's 2017 Account Safety in Banking Scorecard, we embrace one of the Navy SEALs' mottos as a top security priority: The only easy day was yesterday. There is no place for complacency when you work in cybersecurity.

Gary McAlum is Chief Security Officer at USAA. His responsibilities include Information Security & Privacy, Fraud and Financial Crimes Management & Investigations, and Physical Security services. Prior to joining the USAA team in February 2010, he completed 25 years of service in the U.S. Air Force, which included years within the information technology career field.

USAA®

Effective national policy needed to protect the cyber domain

By Rep. Doug Lamborn

Our world is increasingly reliant on the cyber domain and the connections that it creates. We live in a world where the "internet of things" includes the smartphones and computers we use every day and also seemingly benign objects such as factory robots and appliances in our homes. This digital connection to the world around us brings great convenience, efficiency and prosperity, but vulnerability accompanies it.

Early this month, the discovery of two critical flaws in the design of processing chips found in most of our devices reaffirmed this fact.

Until recently, we were not paying enough attention to security in the cyber domain. Hardware, software and network designers often prioritized performance over security. However, our adversaries were paying attention, and the risk of cyberattack and data breaches is increasing.

Cyberspace is a borderless domain that leaves loopholes for our enemies. As stated in the National Security Strategy (NSS), cyberspace provides "opportunities to seriously damage or disrupt critical infrastructure, cripple American businesses, weaken our Federal networks, and attack the tools and devices Americans use every day." In short, a cyberattack could threaten any of us, and originate from anywhere, at any time. Cybersecurity is not just a domestic policy issue; it is a national defense issue.

The recently released National Defense Strategy unequivocally identifies cyberspace as a warfighting domain and promises further investment to ensure our continued relevance in cyberspace. Congress is heeding the call. The recently passed National Defense Authorization Act takes steps ensuring the security of our acquisition programs by limiting influence of foreign-made technology. It also calls on the president and secretary of defense to develop a national cyber policy that ensures we integrate our considerable cyber capabilities across the government.

National defense is more than just military policy. That's why we also enhanced cybersecurity education programs by authorizing $10 million this fiscal year for scholarships and grants to help colleges train students in cyber education, and $8 million for education of military reserve and National Guard members. We added additional support to promote educator recruitment in cybersecurity and improve teaching methods and computer science curriculums for kindergarten through grade 12.

Good national policy starts at the state and local level. I'm proud Colorado's 5th Congressional District leads the way in this arena. The Colorado Springs community is home to more than 80 cybersecurity employers, including five designated as workforce training organizations.

Strong partnerships between employers, government and academia — fueled in part by federal workforce and small-business development efforts — is bridging critical skills gaps between training and hiring. Continued development of our highly skilled cyber workforce is a minimum requirement if our country is to lead the way.

The recently established National Cybersecurity Center (NCC) provides public officials and employers nationwide with training and leadership to collaborate, respond and recover from cyberattacks. The NCC demonstrates the critical importance of addressing cybersecurity holistically as a national goal rather than segmenting between public, private and defense sectors.

Our local military partners understand this well. In 2016, the Air Force stood up its CyberWorx venture at the U.S. Air Force Academy. CyberWorx is a joint public-private effort to foster ingenuity and resolve problems requiring timely, innovative solutions. With assistance of the Catalyst Campus' Center for Technology, Research and Commercialization, CyberWorx teamed with nearly 50 industry and academic organizations its first year alone, and the Air Force has directed further expansion. Catalyst Campus itself is a "collaboratory" where innovative small businesses actively collaborate with government to discover, develop and rapidly prototype solutions to military space and cyber problems.

As stated in the NSS, "Protection from persistent cyberattacks is needed to support America's future growth." Colorado's 5th Congressional District leads the way on public-private partnerships to accomplish just that.

We can do more. The lack of a stable budget for our military prevents their advances in cyberspace, and Congress owes it to the nation to pass a budget and fully fund our defense. Furthermore, Congress should continue to invest in cybersecurity through strong national policy to promote effective public-private cybersecurity partnerships, limit unnecessary regulation and further protect national interests in cyberspace. Strong cybersecurity protects all Americans. We must do everything we can to ensure access, reliability and protection in this domain.

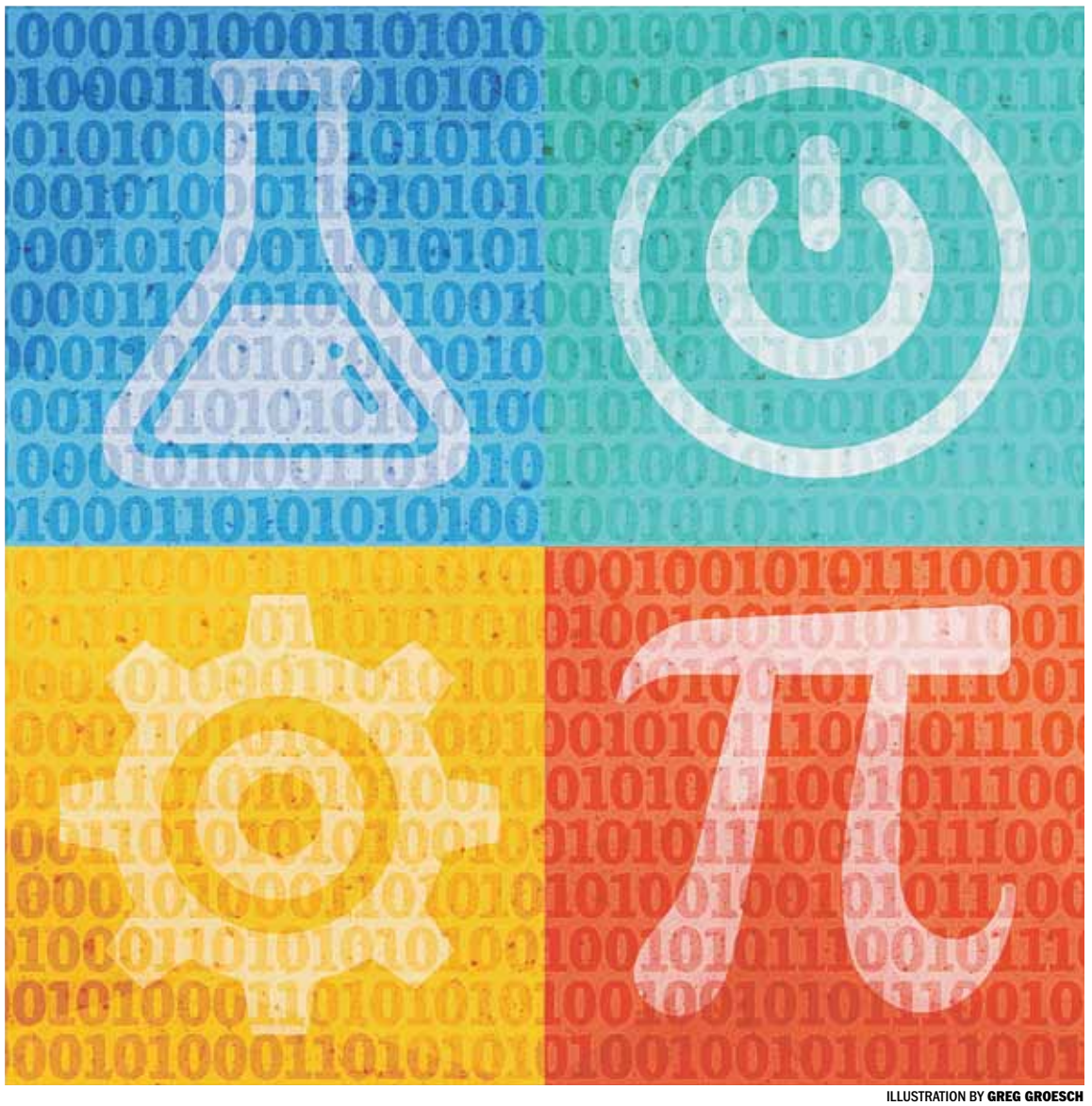


ILLUSTRATION BY **GREG GROESCH**

Rep. Doug Lamborn, Colorado Republican, serves on the House Armed Services Committee and the House Natural Resources Committee, where he is Chairman of the Subcommittee on Water, Power and Oceans.

How tech can address the greatest security challenges of our time

By Gary Shapiro

After Hurricane Harvey struck southeast Texas in August, a network of Good Samaritans who call themselves the Cajun Navy took to social media to help organize relief efforts. Airbnb's Homes program connected hosts with people in need of emergency shelter. And Lyft added the American Red Cross to its Round Up & Donate feature, letting riders contribute to relief efforts.

Following the mass shooting at a Las Vegas music festival in October, Facebook activated its safety check feature, the city's police department took to Twitter to help families locate missing loved ones, and a GoFundMe account created by Clark County Commission Chair Steve Sisolak raised more than $11 million for victims and their families.

In the wake of disasters, natural or manmade, technology has the power to make things better. Americans recognize and appreciate the value these tech tools present. In fact, most Americans like social media services and credit technology with improving lives. And according to a recent Pew study, Americans say technology will be the most important factor in improving their lives in the decades to come.

There's good reason for their enthusiasm. The American tech industry — the crown jewel of our economy — is one of the strongest in the world. Not only does its combined direct, indirect and induced economic activity account for ten percent of our GDP and more than 15 million U.S. jobs, it is a source of many remarkable international partnerships.

Every year at CES®, the world's largest tech event, which took place earlier this month in Las Vegas, I meet international executives keen to partner with or emulate U.S. companies. I also meet innovators from around the world who travel to CES to pitch their ideas, share their strategies and forge business partnerships. To bash the tech industry is to bash a major economic driver and source of cooperation and diplomacy.

Government leaders and the tech industry should work together to strengthen personal cybersecurity challenges and national security, solve consumer problems, improve our world and fend off bad actors. Technology needs flexibility to innovate — and government shouldn't impose burdensome rules that stifle industry.

The answer is not to stomp out the tech that fights terrorists and criminals — it's to develop savvier tech to outsmart these bad actors. America's greatest strengths are its freedoms — freedoms that draw innovators from around the world to our shores for study, for business and for CES.

To defend these freedoms, startups are offering the next technologies to help combat terrorism. For example, Israeli tech startup Beyond Verbal developed an app that can hear a voice and recognize emotions. This and other technologies could be used to identify deception in our airports and at our borders. More, innovations in biometrics — such as advanced facial recognition and fingerprinting software — can play a huge role in counterterrorism efforts, thwarting future attacks and securing our borders. And predictive analytics technologies harness the power of big data to help law enforcement infer when and where criminals strike.

If we want to preserve our freedoms, we have to strike a difficult balance. On the one hand, we must defend ourselves from those who use innovation and technology to destroy our freedoms and hold accountable bad actors who abuse that innovation and technology for selfish and sinister reasons. On the other, we need to ensure that in defending our own freedoms we don't wind up compromising them.

Only by working together — across sectors, industries and parties — can we protect our birthright and uphold our beliefs on the global stage.

Gary Shapiro is president and CEO of the Consumer Technology Association (CTA)™, the U.S. trade association representing more than 2,200 consumer technology companies, and owner and producer of CES®, the world's largest tech event. Shapiro is author of the New York Times best-selling books, "Ninja Innovation: The Ten Killer Strategies of the World's Most Successful Businesses" and "The Comeback: How Innovation Will Restore the American Dream." His views are his own. Connect with him on Twitter: @GaryShapiro.

Safeguarding Americans' data in federal agencies

By Rep. John Ratcliffe

In today's digital age, nearly every service imaginable is available through a couple of quick clicks on an app or a website. We can order food or groceries right to our doorsteps, we can call a ride to the airport, or we can pay for a parking spot — all within seconds. But this convenience comes with inherent risk — living one's life in the digital age means trusting your sensitive information with outside applications, organizations and vendors.

Given the possibility that information hosted digitally could end up in the wrong hands, people are rightfully cautious when deciding which companies and products they trust. To generate consumer confidence, companies understandably tout the quality or reliability of the security tools used to safeguard information they collect from their customers. Similarly, the federal government, which possesses every American's sensitive personal information, must prove — to an even greater extent — that it is worthy of protecting troves of their most sensitive information.

In the past few years, major breaches at the U.S. Office of Personnel Management and IRS have unfortunately eroded the public's faith in this important government function. In the wake of these incidents that placed millions of people's data at risk, I urged officials at the Department of Homeland Security (DHS) to swiftly address this troubling problem, and I'm encouraged they are moving in the right direction.

We all know the challenge we face in our federal government's cybersecurity isn't a lack of available technology. The private sector has been innovating and coming up with the kinds of sensors and dashboards necessary to find and visualize this data. The challenge lies in equipping agencies to utilize these tools and capabilities and ensuring the procurement process is agile enough to meet the evolving cybersecurity needs.

A critical component of this effort involves overseeing and improving the tools we've granted DHS to leverage in accomplishing this important responsibility. And beyond this, ensuring we deploy continuous strategies that are nimble and dynamic enough to be valuable cybersecurity tools for years to come through an emphasis on cloud, mobile and Internet of Things (IoT).

Right now, one of the biggest assets at DHS' disposal to prevent future breaches is the Continuous Diagnostics and Mitigation (CDM) program. CDM ensures strong cybersecurity hygiene by allowing the federal enterprise to monitor and assess the vulnerabilities and threats to its networks and systems in real time — or as close to real time as possible — by allowing data defenders to see what is happening in their digital ecosystem. After all, you can't protect what you can't see.

In 2012, DHS launched the rollout of a continuous four-phase process that will allow CDM to eventually provide the American people the kind of federal cybersecurity that they deserve. This will be accomplished by granting the ongoing ability to buy and implement security technologies that will provide visibility and real-time risk assessments, which will allow security experts to coordinate their defenses.

Right now, DHS is overseeing the process of identifying what and who is on federal networks before shifting into the final phase, which will focus on the security of the data itself. From the perimeter down to the data, CDM will provide a dynamic means of providing cybersecurity awareness to empower network defenders to do their job.

Before we can move forward, however, it's critical that we learn what we are doing right and what we could be doing better. That's why we invited key stakeholders from Splunk, RSA Archer, CGI Federal and Information Technology Alliance for Public Sector to testify at our cybersecurity subcommittee hearing just this month.

In our discussion, we confirmed that full deployment of the CDM program should be viewed as a journey rather than a destination. This means the subcommittee must be sure to examine a longer-term approach for the program — not just a focus on the low-hanging fruit. We in Congress must keep the pressure on DHS to provide a continuously rolling and adaptive CDM program to keep pace with the ever-evolving threats our federal agencies and departments face.

Before the age of the Internet, agencies weren't generally considered part of the national security conversation, but we must realize that every agency that maintains personally identifiable information is on the front line of keeping this country safe. Moving forward, we will continue focusing on the CDM program and DHS' overarching cybersecurity mission to ensure that federal agencies have the right tools to protect the data of every American and prevent the massive data breaches that erode public trust.

Rep. John Ratcliffe, Texas Republican, is Chairman of the House Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection.

America's Air Force: Defenders of air, space and cyberspace

By Maj. Gen. Robert J. Skinner

In this daily deluge of information that shapes our American way of life, we continue to see headline after headline of cyberattacks affecting our trusted government agencies, commercial corporations — large and small — and in some cases, our very own personal data.

In fact, in 2017 alone, the Center for Strategic and International Studies lists dozens of examples of such cyberattacks, including a Russian operation to send malicious spear-phishing messages to more than 10,000 Twitter users in our Defense Department; a ransomware campaign that spread to 99 countries; denial-of-service attacks widely attributed to North Korea that targeted media, financial, aerospace and critical infrastructure organizations; and the Equifax data breach that revealed the Social Security numbers and other personally identifiable information of more than 143 million Americans.

In 1984, I enlisted in the United States military and have had the privilege to wear the uniform ever since. After completing my bachelor's degree in computer science, I've spent most of my 33-year career in positions that have allowed me to witness firsthand the advances of the digital age and the wholesale evolution of cyberspace. And I can say they've completely transformed our American way of warfare and our American way of life. From my first technical assignment as a software programmer in 1990 to my current position as deputy commander of Air Force Space Command, a 36,000-person organization responsible for providing mission-ready space and cyberspace forces for the nation, I've seen the exponential growth of our dependence on cyberspace and the way cyberspace can improve military lethality.

Today, relentless cyberattacks continue to demonstrate how cyberspace has truly become a warfighting domain. And since we, as a nation, have become so reliant on cyberspace, it is absolutely critical that we defend this domain just like we defend the air, land, sea and space.

From my vantage point, we (your nation's Air Force) must also be relentless and continually ask the question: How do we outpace our adversaries and increase the lethality and readiness of our Airmen to protect our networks and critical infrastructure, which are absolutely fundamental to defending our nation, our allies and our interests around the globe?

To tackle this challenge, our Air Force recently implemented numerous efforts to defend our Department of Defense (DoD) networks, which ultimately enable our joint warfighters on the battlefield. At the enterprise level, we have hardened our cyberspace perimeter, collapsed hundreds of networks into one defendable Air Force network and built defensive maneuver forces able to quickly posture against emerging threats.

In our Air Force cyber squadrons, we are completely shifting our focus to a warfighting perspective, changing our culture one Airman at a time with the support and leadership of our commanders at all levels. Prior to this change, our cyber Airmen spent most of their workday operating and maintaining information technology (IT) infrastructure. Today, we are ensuring our cyber warriors are not only trained

» see SKINNER | C15

Preparing our nation for 21st century challenges in the digital age

By Rep. Elise Stefanik

In early December of 2017, world technology leaders assembled in Wuzhen, China, for the 4th Annual World Internet Conference. It was a widely attended event and included the chief executive officers of Apple and Google. The theme of the conference was "developing a digital economy of openness and shared benefits."

As Chairwoman of the subcommittee that provides oversight of DARPA, whose technological breakthroughs created the Internet itself, I found myself concerned that such an event wasn't being held in the United States, already home of a digital economy of openness and shared benefits.

The House Armed Services Committee, and my subcommittee on Emerging Threats and Capabilities in particular, has for the past several years reviewed in detail China's advances in technology, including their cyber and information warfare capabilities and advanced weapons systems such as hypersonics and directed energy. Just a few weeks ago, we held an open hearing focused on many of the newer technologies that China is investing in to support their national objectives, including artificial intelligence, high-performance and quantum computing, and genomic engineering.

What we learned was alarming. China continues to increase their research and development investments at an alarming pace and is rapidly closing many of their technology gaps. More and more, they use only domestic Chinese firms while creating high market-access barriers to support domestic capacity. The effect is to replace any and all dependency on foreign companies, investments and technologies.

Aside from the obvious economic benefit of China being able to create millions of exclusive, high-paying, high-skill jobs for its workers, there are also obvious national security implications should they corner the market on advanced technologies critical to national security.

China is also aggressively moving to acquire enabling commodities such as data; current trajectories have China on track to have roughly 30 percent of the world's data by 2030. China's vision for dominating technology and the Internet is based more on control than on the democratic values our country was founded, including free, open markets and capitalism. But in a digital economy, data is the new currency, and we are learning the hard way that China is about to strike it rich.

Many of China's published national-level plans — such as achieving dominance in artificial intelligence by 2030 — indicate a top-down, government-driven agenda that provides a road map for strategic collaboration between industry, academia and their civil society. These plans, when combined with resourcing, effort and patience, may propel China to leap ahead in many of the technology sectors the United States currently dominates. Most notably, China's leadership appears to recognize the connection between the development of many of these advanced technologies and economic growth. This is something we should remind ourselves of as we continue to examine this important topic; perhaps it is a lesson we need to relearn amidst our debates on Sequestration and Continuing Resolutions.

Despite these trends and concerns, I firmly believe that China's dominance in technology is not a foregone conclusion. And we are wise to remember that in the end, this is not about China. Rather, it is about what the United States can and must do to improve and maintain our technological edge for this information-enabled 21st century economy.

In the coming weeks, I intend to take what my subcommittee has learned and translate this into action, to inform and reform our government in support of national-level efforts so that the United States remains home to the world's leading experts, researchers and technological breakthroughs.

Fortunately, we have momentum to build upon. Previous defense bills have reformed outdated and cumbersome laws, energized the defense industrial base and stimulated innovation by authorizing initiatives such as the Defense Innovation Unit-Experimental (DIUx) and the Defense Digital Service. Still, much work remains — and includes modernizing our defense labs, improving critical infrastructure and ensuring our ability to operate in an information- and cyber-degraded environment, and stimulating small businesses and private-public partnerships.

Our recent hearings have also highlighted the need for us to develop and consider national-level strategies for other emerging technologies such as machine learning and artificial intelligence, genomics, and high-performance and advance computing. And I intend to ensure the Pentagon considers these technologies for our use while also monitoring and mitigating adversarial use as well.

I firmly believe that we can and should drive a national-level dialogue to advance innovation across the government, to maintain a battlefield advantage, and to energize our domestic industrial base and provide technology jobs and opportunities across many sectors here in the United States.

These actions will ensure policy keeps pace with technology as we develop an information economy for the 21st century.

Rep. Elise Stefanik, New York Republican, is Chairwoman of the House Armed Services Subcommittee on Emerging Threats and Capabilities.

SKINNER

From page **C14**

and equipped to defend our networks, but that they are providing our commanders with critical information regarding potential threats, indications or warnings their missions may face as well as operational options in the cyberspace domain. Our Airmen are now thinking like warfighters and working to ensure we are ready to fight and win against any threat.

We are also collaborating with our industry partners to leverage their vast expertise and experience to use the latest technology and applications to strengthen our networks. These partnerships enable our cyber Airmen to move away from IT service delivery and instead hone their warfighting focus on active cyberspace mission defense and assurance.

Last year, we teamed with information security specialists from around the world through our "Hack the Air Force" programs. These programs are designed to better secure our internet presence by capitalizing on the skills of private sector, independent and government experts to assess our vulnerabilities, find ways to fix them and strengthen our networks against potential adversaries.

In addition, many of our cyberspace Airmen are directly supporting U.S. Cyber Command as part of the 133 Cyber Mission Force teams. These teams, which began forming in 2013, are scheduled to be fully operational by the end of June 2018. They support a number of critical missions, including blocking adversary attacks and maneuvering to defeat them, protecting DoD information networks and priority missions, and preparing cyber forces for combat.

These key initiatives — the Cyber Mission Force teams, partnerships with industry and our refocus to a warfighting mindset — are just some of our ongoing efforts in the Air Force. We will continue to innovate and develop ways to strengthen our cyberspace defenses, such as reporting our progress through the DoD Cybersecurity Scorecard and providing the most highly trained, lethal forces on the battlefield.

As our nation's livelihood and national defense continue to expand and exploit the cyberspace domain, rest assured — your Airmen are serving 24/7 around the globe to defend the air, space and cyberspace domains and, ultimately, our American way of life. Your Air Force will continue to answer the Nation's call.

Maj. Gen. Robert J. Skinner is Deputy Commander of Air Force Space Command at Peterson Air Force Base in Colorado. Prior to his current position, he held several positions at Fort Meade, Maryland, including Deputy Commander of the Joint Force Headquarters Department of Defense Information Networks.

The 5th domain: Cyber defense needed in the 21st century

By Rep. Adam Kinzinger

In today's world, we have all been to cyberspace and enjoyed the many conveniences this global domain has added to our lives. But did you know that cyberspace has been declared the fifth domain of warfare? Just like it does in our own lives, cyberspace provides interconnectivity and communications between the other four domains of war — air, land, sea and space. Therefore, an enemy doesn't need extensive ground troops or nuclear weapons to take on the United States. All that's needed are a few inexpensive tools, some knowledge and skill, and access to our networks where the cost of entry is almost nonexistent.

The U.S. faces millions of cyberattacks each day in both the public and private sectors; in some cases, hackers can easily find points of vulnerability in our systems. Typical cybercriminals will look for bank routing numbers, medical records and other sensitive personal information. Cyber actors working on behalf of nation-states or terrorist organizations seek access to corporate and copyrighted information, critical infrastructure and state secrets.

Yet, the United States continues to lack a coherent, comprehensive strategy to address these threats.

Last year, the Pentagon reported the cyber capabilities of other nations exceed the United States' ability to defend its networks, meaning the likes of China and Russia are able to hack our networks and potentially wreak havoc.

Our adversaries have already shown they can and will exploit our vulnerabilities. In 2011, Iran hacked major financial institutions and then seized control of a New York City dam during a 2013 operation. In 2014, North Korea used their cyber skills to attack Sony Pictures in what most people viewed as a retaliation against a comedy film about an assassination attempt on Kim Jong Un. China's massive intrusion into the security-clearance files at the U.S. Office of Personnel Management led to a data breach of over 23.9 million federal workers between 2014 and 2015.

Most recently, we dealt with Russian interference in the 2016 elections, and there are no signs of Russia stopping their attacks on our democracy or on others around the world.

These are just a few of the major cyberattacks we have endured over the years, and sadly, we will continue to face these threats unless we take action. Across the United States, it's likely that we have all been victims of data breaches. So what will it take for us to change course and do something about these cyberattacks? We cannot sit back and wait for a catastrophic event, such as a major power grid getting hacked and taking us offline. Something of that magnitude would create panic and chaos, upending our daily lives like never before. Now that would be apocalyptic!

There is no cure-all to fix the state of our cyber defenses. But there are actions that can and should be taken to vastly improve our standing with our own cybersecurity.

First, we must build healthy partnerships between the public and private sectors in terms of deterring, detecting, defending, rapidly responding to, and recovering from cyber invasions. After the enactment of the Cybersecurity Act of 2015, we made some progress in this area, but we must be more effective in facilitating information-sharing in real time to better respond to quickly evolving cyberattacks.

Second, we must address the lack of cybersecurity professionals in both the public and private sectors here in the U.S. These professionals man the front lines, develop programming and fortify our networks. As a nation, we must expand and improve our future cyber workforce by bolstering education in science, technology, engineering and mathematics (STEM) with a particular focus on computer sciences. This is an area we can and must improve upon, and that starts with encouraging our future generations to get involved and become educated in these fields.

Third, the public and private sectors must establish appropriate ways to notify and communicate these threats to the general public. For our own consumer protection, the public must be notified as soon as possible about breaches and be provided guidance on how best to prevent identity theft.

Fourth, we must finally construct a comprehensive national cybersecurity strategy. This country can no longer afford to sustain these cyberattacks, lick our wounds and ultimately fail to change course. We must make clear, for instance, that a cyberattack would be met with a superior cyber reaction, or in extreme cases, using our military to deter these foes. Frankly, the American people deserve better from their institutions, and our institutions can do better for the safety and security of the American people.

Lastly, and perhaps most importantly, in order to be effective in preventing attacks, we need greater public and private financial investments in cyber defense. Although federal investment in cybersecurity has increased over the years, it's failing to meet the challenges of the complex, ever-changing threat environment we face. Our enemies see opportunity in our vulnerabilities in cyberspace, and they are investing heavily to exploit them. We must rise to the occasion.

Taken together, these actions will put us on sound footing to meet or exceed the investments — and corresponding capabilities — of our adversaries.

To be clear, we can take some comfort in recent progress with our cybersecurity. In August, President Trump elevated U.S. Cyber Command to a Unified Combatant Command, which recognizes that the threats we face are far more dangerous than ever. In December, the administration announced a new "whole-of-government" national security approach, focusing on how cyberspace relates to all other aspects of our national security. But even with these efforts from the Trump administration, we do not have a fully comprehensive or coherent strategy for cybersecurity.

On Jan. 30, President Trump will give his State of the Union Address. Here, he has an opportunity to further recognize the challenges we face in cyberspace, assure the American people that a strategy is forthcoming, and then make good on his word. I hope he seizes this moment and gives us reason to see past our differences and work together towards a stronger, more cybersecure America.

Rep. Adam Kinzinger, Illinois Republican, serves on the House Committee on Foreign Affairs and the House Committee on Energy and Commerce.

Global cooperation of 'utmost importance' for a stable cyberspace

By Ambassador Marina Kaljurand

I come from Estonia, a country that is known for Skype and the NATO Cooperative Cyber Defense Center of Excellence, as well as for being the first country in the world to introduce e-government, e-taxation, e-voting and a thousand other e-services. These are all part of what we call our e-lifestyle.

In 2007, Estonia was also the first sovereign state in the world to be subjected to politically motivated cyberattacks supported by another state. We learned that our e-lifestyle also entails e-challenges and e-responsibilities. We knew then — and know even better now — that no services are completely secure, whether online or offline. But we can, and must, face these challenges by taking appropriate steps to minimize risks.

Over the past decade, cyber incidents have grown in severity and number. Distributed Denial of Service (DDoS) attacks have become increasingly commonplace while new threats have emerged. 2017 was replete with cyber-related headlines, many of which spoke to different facets of an increasingly complex challenge. The WannaCry and NotPetya malware worms were at the forefront of a new wave of ransomware attacks. The growth of the Internet of Things (IoT) helped fuel a nearly twofold rise in the number of DDoS attacks in 2017 compared with 2016, while a frightening number of botnets now lie dormant, waiting for an unknown purpose. Meanwhile, incidents of "hacking democracy" continue.

Even as the nature of the cyberthreat has grown and evolved, the need to enhance international cooperation and adopt a multistakeholder approach has not changed; in fact, these have to be accepted as the foundation of an effective global approach to ensuring cybersecurity. Why?

Firstly, while the cyber domain has become accepted as an integral element of any approach to national security, it is not one that states can effectively manage alone. Given that the cyber realm does not have borders, international cooperation is of utmost importance.

Unfortunately, attempts to foster such cooperation at an intergovernmental level seem to have reached an impasse. The failure of governmental expert discussions (UN GGE — United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security) and stalemates in other diplomatic fora show that the ideological divide on the use of information and communications technologies (ICTs) is too deep, and governments do not have enough political will to reach agreement in the near future.

ILLUSTRATION BY **GREG GROESCH**

While regrettable, this does not mean that discussions will — or should — come to an end. Talks have to continue under the auspices of the U.N. as well as in other frameworks. Hopefully, all states will find the courage and determination to return to constructive negotiations — ideally, sooner than later.

Secondly, despite states' traditional dominance over all questions related to international peace and security, their role within the overall ecosystem of cyberspace is central but limited. Governments alone simply cannot dictate all aspects of a domain in which civil society writes much of the key code, the private sector owns nearly all the digital and physical assets, academia analyzes the complex issues of applicability of international law to cyberspace, and the IT community has the best technical expertise. Given this complex landscape, it is clear that a multistakeholder approach to cybersecurity is the only effective way forward — one in which all stakeholders have a unique role, including developing norms of responsible behavior.

Cyberspace is not a jungle and should not be governed by the laws of the jungle. A predictable and stable cyberspace needs clear laws and rules that minimize "gray zones" in which it is unclear which norms apply — and what the consequences are if they are broken.

The members of the United Nations agreed as early as 2013 that international law applies to cyberspace. Now we need concrete answers from governments as to how it applies. Otherwise, some states will continue to exploit gray zones where the applicability of international law is not certain, e.g., about sovereignty in the case of the Democratic National Committee hacks or about protecting critical voting infrastructure in the case of other attempts at interfering in elections.

In addition to legally binding norms of international law that can be adopted and applied by states, there are also nonbinding voluntary (political) norms. Non-state actors should also play an important role in developing the latter. Here are just a few examples.

As the Chair of the Global Commission on the Stability of Cyberspace (GCSC) (https://cyberstability.org), I am proud to introduce a norm that was launched in November 2017 — the Call to Protect the Public Core of the Internet. It is an appeal for a new global norm to apply to both state and non-state actors to refrain from activity that intentionally and substantially damages the general accessibility or integrity of the Internet itself. The Carnegie Endowment has proposed a norm to protect financial stability against cyberthreats, while Microsoft is working on a technical accord — a proposal by the technology sector to protect people in cyberspace. States should review and seriously consider these proposals while engaging constructively with other stakeholders. Public-private partnership should not only be a political concept, but a standard operating practice adopted by governments and the private sector. These could be very clear and substantial steps on the road to cyber stability.

It is time for states and non-state actors who share democratic values and who believe in an open and secure cyber future to come together and to act together — globally, decisively and boldly — to protect a free, safe, stable, accessible and available Internet while fostering the continued growth and development of the use of ICTs.

Ambassador Marina Kaljurand is Chair of the Global Commission on the Stability of Cyberspace. She has served as Estonia's Foreign Minister and represented Estonia in six nations, as well as at the U.N. Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.

Painful cyberattacks driving demand for security

By Lenore Hawkins and Chris Versace

The right to defend yourself and your property applies in today's increasingly connected world, just as it did more than 200 years ago. While the Second Amendment protects the right to keep and bear arms, the threats we face today are changing, just as the way we interact with people, data and content are changing. As individuals, companies and countries, we must be increasingly on guard and behaviors need to shift away from reactionary defense towards an always prepared and secure posture, much the way we've seen with homeland security and traditional national defense.

In 2015, for example, two researchers at the Black Hat conference hacked a 2014 Jeep Cherokee over the internet and paralyzed it on I-64, forcing Chrysler to recall 1.4 million vehicles. Hackers have found security flaws in smart home connectors that are used to turn up the thermostat, turn on your lights or access your Wi-Fi network through your smart fridge.

Cyber is global. In 2017, the WannaCry and Petya attacks reminded many of the growing threat of worldwide cyberattacks. We believe cybersecurity is an extraordinary growth market as individuals, companies and other institutions look to shore up their existing cyber defenses, assess attack and intrusion vulnerabilities and ward off future attacks.

CyberSecurity Ventures and other forecasters projected cybersecurity spending to balloon to $120 billion in 2017, up from $3.5 billion in 2004 — an increase of 35 times in 13 years. By 2021, CyberSecurity says worldwide spending on cybersecurity software, services and hardware services could "eclipse $1 trillion." As one might expect, one of the fastest-growing segments of corporate consulting is cybersecurity advice, reaching $7.1 billion in 2016.

Key areas to watch in 2018:

■ **Cyber is only one aspect of security.** As crucial as cybersecurity will be, it is still just one aspect of the far larger Safety & Security spending that occurs each and every year. Total global cybersecurity spending represented roughly 23 percent of the $522 billion 2017 U.S. defense budget. Candidate Trump pledged to rebuild the U.S. military and President Trump is looking to boost defense spending to $575 billion in 2018, a 10 percent increase from the last full-year budget in fiscal 2016 and about 9.5 percent more than the budget Congress approved for 2017. Aside from big-ticket items like military aircraft, ships and other marine vessels, the budget includes national security spending, weapons procurement as well as research and procurement.

■ **Outside the U.S.** Rising global tensions have led to increasing demand for defense and military products in the Middle East, Eastern Europe, North Korea, the Far East and South China Seas. This is instigating increased defense spending globally, especially in the United Arab Emirates (UAE), Saudi Arabia, South Korea, Japan, India, China and Russia. For example, the Middle Eastern Homeland Security market is slated to grow at a CAGR of 15.5 percent to achieve $17.05 billion by 2021, up from $7.19 billion in 2015, driven by government initiatives to create a smart and secure environment amidst high terrorist activities in the region.

ILLUSTRATION BY **LINAS GARSYS**

■ **Home security**. With the media's emphasis on cybersecurity (just Google "security" and see what comes up), attention is lost on other aspects of individual or personal security. The global home security solutions market — which includes video surveillance, electronic locks, alarms, access control, sensors, detectors and corresponding services — is predicted to reach $30.3 billion by 2022, up from $8.3 billion in 2014.

The increasing acceptance of video surveillance systems is expected to propel not only the video surveillance subsector, but also the data storage sector as the demand for IP-based video surveillance will increase due to its improved video-capturing quality. This growth is not just U.S.-based as the number of monitored alarm systems in Europe is forecasted to grow from 8.7 million in 2016 to reach 10.6 million in 2021, according to research by Berg Insight. In North America, the number of monitored alarm systems is forecasted to grow from 32.1 million at the end of 2016 to 37.1 million at the end of 2021.

■ **New threats, new solutions**. Our Safety & Security investment theme is not only demand-driven as people, corporations and other entities spend on protecting and securing themselves, but is also ripe for change as industries evolve. The M&A activity in the defense contracting sector to purchase cyber firms as the "battlefield" increasingly expands into the digital world illustrates this rapid need for change. Another catalyst is the Internet of Things (IoT) and the increasing reality that even our own personal devices could be rendered useless or even dangerous through a cyberattack unleashed by a foreign government or other nefarious entity.

Lenore Hawkins is Tematica's Chief Macro Strategist of Tematica Research and Chris Versace is the firm's Chief Investment Officer. Tematica Research develops proprietary thematic investment strategies and delivers related content across custom indices, published research and model portfolios to both self-directed investors and institutional clients. The company's Safety & Security investment theme taps into evolving needs across individual, cyber, corporate and homeland security, targeting companies that offer products and services ranging from corporate security and monitoring solutions, to firearms arms and home-security, to cybersecurity and national defense. Find us at https://www.tematicaresearch.com.

Cybersecurity and elections: Are we ready for November?

By Rep. Yvette Clarke and Rep. Terri A. Sewell

At first, "Cozy-Bear," "Fancy-Bear" and "Gucifer 2.0" may sound like characters out of a science fiction thriller. But on June 15, 2016, we learned that these were the names associated with Russian groups who hacked into campaign committee computer networks. The following week, Wikileaks published 20,000 emails from the hack, which exposed the cybersecurity vulnerabilities of our democratic institutions for all Americans to witness.

It has now been a full year since the intelligence community released its declassified report on the cyber breach, confirming both that Russia executed the attacks and that Russian hackers will be back to exploit vulnerabilities in future elections. But after one year, after more than 800 votes in the House and the Senate, and nearly 365 days into the Trump administration, federal lawmakers have yet to pass a single bill to protect our elections from another attack.

With campaigns already gearing up for the 2018 elections, it's open season on our democracy.

To be clear, no evidence suggests that Russian cyberattacks compromised any election equipment, or that they were able to tamper with voting ballots. But we know that they "cased the joint," and there is a consensus among the intelligence community and cybersecurity experts that Russia will strike again in future elections. Defending our democracy against another attack will require action now. Not next month, not next year, but starting today.

Unfortunately, this sense of urgency is not shared by everyone. We have been disappointed in the lack of leadership by the White House on this important issue. Instead of unifying the country following Russia's cyberattacks, this administration established a now-defunct sham election commission in order to support President Trump's foregone and unfounded conclusion of voter fraud.

The good news is that the decentralized nature of our election system makes it difficult for hackers to infiltrate our system using only one entry point. But difficult does not mean impossible. If a malicious actor is strategic enough, and focuses on unsecured voting equipment in a few counties in key battleground states, this intruder could successfully manipulate the outcome of an election. Given the recent revelations on how Russia exploited social media platforms to strategically disseminate divisive and narrowly tailored ads in key states, we now have proof that our adversaries have studied our vulnerabilities and intend to find ways to exploit them.

ILLUSTRATION BY **GREG GROESCH**

The bad news is that a decentralized election system is more difficult to update and secure in a comprehensive manner, and any infrastructure that is improperly secured could easily become the potential doorway to sabotage and data breaches.

But in some corners of Washington, officials and lawmakers are working quietly to address the issue of cybersecurity in our elections. Last year, former Department of Homeland Security (DHS) Secretary Jeh Johnson designated election equipment as critical infrastructure. Former DHS Secretary John Kelly upheld this decision, underlining the importance of protecting this nation's voting systems. This designation ensures that voting equipment receives the same vigilant protection as other national security systems. More importantly, it gives election officials direct access to DHS resources and support services to be better equipped to deter cyberattacks.

And here in Congress, we've joined forces to introduce the SHIELD Act, a critical piece of legislation that would establish an Election Security Board of Advisors. As members of the Congressional Voting Rights Caucus, we are leading the fight for unfettered access to the ballot box by all eligible citizens. This includes equal access to up-to-date and certified voting systems that protect the sanctity of each person's determined vote and increases their confidence in the democratic process.

Additionally, we believe that Congress plays a vital role in partnering with states to protect this critical infrastructure. Much of the election equipment used by states are nearing the end of their shelf lives and are sometimes incompatible with new software updates. By making voluntary technological grants to states an annual appropriations line item, Congress could assist states in being able to keep pace with the rapid technological developments.

We therefore call upon all those who work to protect our democracy to remain persistent in safeguarding our election infrastructure from cyberattacks. Every vulnerability must be strengthened and every precinct equipped with the means to protect against cyberattacks. We urge our colleagues to support and pass legislative measures that adequately protect this critical infrastructure for all communities. We also strongly urge the administration to refocus its efforts toward protecting against malicious actors, foreign and domestic, rather than advancing a false narrative of voter fraud aimed at disenfranchising millions of voters across the country.

Rep. Yvette D. Clarke, New York Democrat, represents New York's 9th District. She sits on the Energy and Commerce, Small Business, and Ethic Committees. Rep. Clarke is the Member-at-Large of the Congressional Black Caucus, Co-Chair of the Caucus on Black Women and Girls, and the Co-Chair of the Multicultural Media Caucus. She is also a member of the newly formed Voting Rights Caucus. Rep. Terri A. Sewell, Alabama Democrat, is serving her fourth term representing Alabama's 7th District. She sits on the House Permanent Select Committee on Intelligence and on the House Ways and Means Committee. Rep. Sewell is a member of the Congressional Black Caucus and is Vice Chair of the New Democrat Coalition. She is also Co-Chair of the newly formed Voting Rights Caucus.

West Point's Army Cyber Institute: Developing the cyber leadership model

By Col. Andrew O. Hall, Ph.D. and Lt. Col. Terence M. Kelley

Speaking at CyCon U.S., General Mark Milley challenged the audience's younger members to take up the mantle of cyber leadership. "That rock is going to go in your rucksack, and we are counting on you for the future." The need for innovative programs to train our future cyber leaders is apparent to the U.S. Army chief of staff and many national-level leaders. The problem is not limited to the military: In a borderless domain, cyberthreats don't distinguish between military and civilian networks. Nor is the problem solely technological: The Army chief also pointed out the moral, legal and ethical concerns brought on by advances in artificial intelligence and autonomous battlefield systems.

These challenges are not unique to the U.S. Army nor even the U.S. military. The nation's need for adaptive cyber leaders spans the military's ranks, industry's labs and trading floors, and the halls of our universities. Yet, the cyber training shortfall narrative is so ubiquitous it hardly needs to be cited. Academia, industry and the military are all innovating to prepare our future cyber leaders, and the Army Cyber Institute (ACI) at West Point is working to bridge all three efforts as we build a model to develop cyber leaders.

Inspiring young people to serve and motivating them to a career of service by necessity goes beyond the classroom. That's why, in addition to researching and developing pre-commissioning training and curriculum for our future Army officers, we developed the Cyber Leader Development Program to incorporate external opportunities. Developed at West Point, the Cyber Leader Development Program has expanded to include ROTC. Based at our nation's civilian universities, ROTC programs are an Army touchpoint to the research being done in the larger academic community.

Although the Cyber Leader Development Program is an Army program, the principles transcend an officer's service and career path; all of the military's junior leaders will be leading through multidomain competition and conflict, and must understand operations on land, air, and sea — and now cyberspace. The nation's senior military colleges are a key partner. The immersive 24/7 military experience offered by these institutions is ideal for identifying and developing future cyber leaders. It connects us to the research being done at the senior military colleges, including beyond their military programs. As the senior military colleges commission into all services, we are better able to develop the joint force's cyber leader development model. Even those students who complete the program but do not join the military will be better prepared to serve in other capacities. The program's result: a more formidable U.S. workforce, in and out of uniform.

Col. Andrew O. Hall with Google's Vinton G. Cerf, co-designer of the TCP/IP protocols and the architecture of the Internet, a keynote speaker at CyCon U.S. in November 2017. U.S. Army photo by Clare Blackmon.

Developing tomorrow's cyber leaders must be a multidisciplinary effort. We cannot separate the math and engineering students exploring cyberspace in their labs from the strategic, legal and ethical discussions social science students debate in their seminar rooms. We need work across disciplines to ensure each of our students leverages the diversity offered at their colleges and universities.

We have also begun a summer internship program at West Point for ROTC students: Cadets from across the country and from various disciplines immerse themselves in multidisciplinary cyber research under the supervision of the ACI's researchers. The program develops cadets' creative thinking skills as they seek innovative solutions to real-world problems. It is an opportunity to advance their technical knowledge and skills, develop leadership abilities and contribute to real-world research benefiting the U.S. Army. We're proud to announce that we are now accepting applications for this summer's Army Cyber Institute Internship Program.

Competitions are a great way to get students excited about cyber defense, testing their problem-solving skills both as individuals and teammates. A great example is the NSA's annual Cyber Exercise, in which the world's top network specialists challenge student teams with state-of-the-art hacker techniques. The students design, build and configure their own networks — safely removed from real-world networks — and then defend them against determined intruders. Each gains a sense of the dangers posed by a hostile network environment and learn realistic defense strategies. West Point has won as many times as all other teams combined, and this spring our cadets will strive to retake the trophy.

These competitions don't even require attendance at a military academy or university. To challenge all our soldiers, we developed and host the annual All Army Cyber Stakes competition. Regardless of where they may be stationed, contestants compete against each other, testing their skills in forensics, cryptography, binary exploitation, reverse engineering and web-based attacks. The result is a good-natured frenzy of competition, with reach round of results generating March Madness-like excitement, but the real outcome is increased readiness within our cyber ranks. Organizations and universities should consider developing their own cyber competition to hone their employee and student skills.

We have created a venue for our students, leaders and academics to present their research and learn from world-class practitioners. That's why we developed scholarships to bring service academy and ROTC students to CyCon U.S., our annual symposium exploring cyber conflict in a globally connected world and to Tallinn, Estonia, for the CyCon conference hosted by the NATO Cooperative Cyber Defence Centre of Excellence. Despite their youth and inexperience, they're often our most enthusiastic audience members and routinely pose challenging questions to generals, corporate executives and policymakers alike.

Many challenges remain: creating a dynamic cyberspace career alongside the military's traditional stringent career path, a lack of flexibility compensation for government civilian and military professionals, and a perceived gap with private-sector opportunities. The continuing work spearheaded by the Army will ensure our nation has a more ready cyber force.

Col. Andrew O. Hall, Ph.D., is the director of the Army Cyber Institute at West Point. Lt. Col. Terence M. Kelley is a U.S. Army public affairs officer. The views expressed are those of the authors and do not represent the official policy of the Department of Defense, the U.S. Army, nor the U.S. Military Academy at West Point. ROTC Cadets interested in the ACI Cyber Internship Program may request more information from contact.cyber@usma.edu.

‘Zero Trust’ computer policy: A timely solution

By Howard P. “Buck” McKeon

Challenges posed by cybercrime are one of the most frightening threats our country faces today.

In recent years, we have had a reactive approach to cybersecurity. We hear about it when an organization has been hacked or sensitive information has been released. Organizations, companies and our government agencies should not simply be reacting when a cybercrime has taken place, but instead need to be proactive.

In order to be proactive, however, the main challenge from which all other cybersecurity issues stem needs to be identified. The United States, along with the entire world, is seeing a global cyber catastrophe that is causing us to reconsider how to establish a network defense. Now more than ever, cybercriminals have access to advanced technologies that put people at risk. That means our government agencies need to establish better defenses.

We have heard of retailers, financial institutions and health care organizations experiencing major hacks, which is why it was disheartening to see that in the 2017 U.S. State and Federal Government Cybersecurity Report, government institutions were listed among the “bottom performers,” scoring lower than retail, health care and information services. I believe that is due to a misidentification of the underlying cybersecurity problem.

The real problem stems from an outdated “computer architecture” that was developed without knowing how today’s cyber connection would look and operate. This obsolete foundation is essentially why cybersecurity attacks take place.

Our defenses are no match for these security breaches. Our computer architecture has reached its ceiling. There was no way the developers and engineers who designed it 40 years ago could have envisioned how the internet and the impact of global connection would have facilitated such cyberthreats. The demand for an increase in computing capabilities and programs overshadowed the computer architecture with the development of the internet.

I have had the opportunity to work alongside experts within the cybersecurity industry who also believe the computer architecture is the main issue at hand. Ed Brinskele, the CEO of Vir2us, has said that IT professionals are dependent on what the “experts” determine are the best practices or defenses for cybersecurity.

“The difficulty is that there has been a significant failure on the part of solutions providers to recognize that a keeping-*the-bad-guys-out* approach reveals a failure to correctly identify the problem,” Mr. Brinskele said. “Once the checkpoints in these solutions are bypassed, they provide virtually no security. This is known as an outside-in and top-down approach and is a fundamentally flawed strategy. As a result, these solutions only address the symptoms of a much more fundamental design problem.”

To address these newfound security challenges, antivirus and firewalls were created to provide somewhat of a Band-Aid. These solutions are not good enough to combat the technology that is available to cybercriminals.

Our outdated architecture is a sinking ship. There are a number of holes in the boat, and we keep trying to patch it up instead of rebuilding it so we can float. These patches include heuristic algorithms and whitelisting, but even these solutions continue to fail. They simply cannot withstand the constant and ever-changing threats.

Additionally, it is virtually impossible to attempt to pinpoint threats from a list-based strategy. Every day, these lists evolve and develop. There is no way to stay current on possible threats or attacks.

“Antivirus and firewalls are list-based solutions and can only deal with known threats. In today’s world of morphing viruses and malware, these solutions are less than 27 percent effective,” Mr. Brinskele continued. “[A leading consumer cybersecurity firm] recently said that their average time to identify threats and update lists is more than nine months. In a challenge that is moving at the speed of light this is problematic. While combating challenges moving at the speed of light, that solution is unacceptable.”

Not only do these outdated solutions consistently fail, they are also extremely inefficient. It has been reported that these “legacy solutions” can consume up to 80 percent of network bandwidth capacity and computer processing power. These inefficiencies negatively impact revenue and productivity. According to the U.S. Government, global business and institutions lose over $1 trillion to fending off cybercrimes and attacks annually.

Rather than trying to fend off possible attacks, implementing a “Zero Trust” policy or architecture would be significantly more practical and successful than fighting to stay current on a list of emerging threats. With a Zero Trust architecture, the “Known” list is manageable and can be maintained.

As cyberthreats continue to unfold, we need to take a hard look and consider improving our computer architecture. A new approach and a radical change within the cybersecurity industry needs to take place in order to provide dynamic security.

Howard P. “Buck” McKeon represented the people of the 25th District of California in the U.S. House of Representatives for 22 years and served as both the Chairman of the House Armed Services Committee and Chairman of the House Education and the Workforce Committee. Today, he is the CEO of McKeon Group, a consulting firm that provides strategic analysis, public relations, advocacy and comprehensive government relations for their clients.

Federal cyber leadership should be bipartisan

By Rep. Gerry Connolly

Imagine: @realDonaldTrump has been hacked and the latest missive from the president's Twitter account announces imminent airstrikes on Genovia. Foreign militaries scramble, and the potential for an accidental escalation of conflict is suddenly very real.

This has not happened, and hopefully it never will, but it does demonstrate the precarious position seemingly innocuous technology occupies in our national security infrastructure.

Many federal information technology (IT) systems are similarly on the hook for the safety and security of 320 million Americans, and, unfortunately, we are not doing everything we can to secure these systems. However, there are simple steps we can take to ensure cybersecurity does not remain the soft underbelly of U.S. national security.

The first step is to reverse a dangerous lack of investment in federal information technology systems. The second is to fill leadership positions in the form of presidentially nominated and Senate-confirmed appointees who have the vision to address cybersecurity threats. And the third is to ensure we have a qualified and dedicated workforce to help upgrade outdated federal information technology infrastructure, help protect critical infrastructure and thwart cyberattacks that could lead to the theft of personal information and intellectual property.

The security of federal networks also depends on these people — and this administration and Congress must cease immediately their attacks on federal employees, which only makes it harder to recruit, hire and retain the cybersecurity talent our country needs.

To understand what is at stake, consider two cybersecurity vignettes — the first regarding national security and the second hinting at the potential economic harm that can result from a cyberattack on federal IT systems.

Nearly everyone, save for President Trump, recognizes that the Russian government directed a sustained and coordinated attack on our electoral system during the 2016 election. It is hard to imagine a more fundamental threat to the security of our Republic than foreign adversaries undermining and potentially upending the public's faith in our most basic democratic exercise — free and fair elections. Every day, bad actors attempt to breach the federal networks that hold sensitive information. U.S. Food and Drug Administration (FDA) servers contain at any point in time some portion of the proprietary information that spurs $333 billion in pharmaceutical sales in the U.S. each year — a potential bonanza for hackers lies just beyond a government firewall.

ILLUSTRATION BY **HUNTER**

While federal agencies and their employees do their best to thwart cyber intrusions, they are hampered by old information technology systems that make their jobs harder and the job of cybercriminals easier. Legacy IT systems, some dating back to the Johnson administration, make protecting federal networks difficult because they are hard to encrypt and are expensive to maintain. At the Internal Revenue Service (IRS), which has the sensitive information of every taxpaying individual and company, the systems that are critical to collecting more than $3 trillion in taxes are some of the federal government's oldest systems. Because of this, the IRS spends about 70 percent of its $2.7 billion annual IT budget on its operational or legacy systems. Yet, the IRS is unable to upgrade its IT systems in part because of the severe and drastic budget cuts that have been enacted since 2010. The current IRS budget is almost 20 percent less than the FY2010 funding level when adjusted for inflation, and the IRS continues to face additional proposed cuts amid heightened demand for its services and additional unfunded mandates such as enacting provisions of the recently passed tax bill.

The issues facing the IRS are not unique to the agency. Across the government, departments like Veterans Affairs and Department of Defense face the same problems. Congress has done its part to help agencies with this problem by passing the Federal Information Technology Acquisition and Reform Act (FITARA) and the Modernizing Government Technology (MGT) Act to provide agencies with the foundation to make better IT acquisition investments and the money to upgrade their IT infrastructure.

The challenges agencies face to modernize their IT infrastructure and take a 21st century approach to cybersecurity are compounded by a lack of focus from this administration. Although the administration issued a cybersecurity executive order in May and recently released a National Security Strategy, there have been little-to-no specifics on what actions this administration will take to address cybersecurity threats.

This is a crisis that demands more than just white papers. It requires sustained leadership and attention, which is sorely lacking throughout the government. Over a year into this administration, the president still has not named a Federal Chief Information Officer to guide agencies in upgrading outdated information technology infrastructure, which leaves federal networks vulnerable to attacks. The Federal Chief Information Security Officer (CISO) position has also been left vacant, filled in an acting capacity by the Deputy CISO who has taken on a third role as a senior director for cybersecurity for the National Security Council.

Governmentwide, positions that are critical to implementing any cybersecurity strategy are going unfilled. The president has not nominated a candidate for Undersecretary for the Department of Homeland Security's National Protection and Programs Directorate, which is charged with coordinating efforts to protect the country's critical infrastructure and enhancing the security of our cyber and communications infrastructure. The Department of Veterans Affairs, where the IT systems have been designated by the VA inspector general as a material weakness for 18 years, is also waiting for a nominee to fill the position of Assistant Secretary for Information Technology. Critical positions at the Department of Defense, including the Principal Deputy Undersecretary for Acquisition, Technology, and Logistics, and the Chief Information Officer, are filled with acting officials while they wait for the president to name permanent leaders.

At the same time, this administration and the majority in Congress are taking actions that make it difficult to compete with the private sector in recruiting and retaining skilled cybersecurity and IT professionals. In his first budget proposal, the president took a meat cleaver to federal employees' retirement benefits. In Congress, the House of Representatives passed legislation to increase the probationary period for federal employees from one year to two years. Many seeking to enter public service understand that the government cannot pay as much as the private sector, but reducing retirement benefits while increasing trial periods for a highly sought-after workforce is counterproductive and only makes the federal government more vulnerable to malicious cyber-enabled activities.

The good news is that there is a road map, and it can be bipartisan. In Congress, we have found incredible success putting aside partisan differences, rolling up our sleeves and delivering solutions to the most vexing challenges facing federal IT. If this administration gets serious, it can join the fight and ensure the men and women on the front line fending off cyberattacks have the skills and resources they need to safeguard our national security.

Rep. Gerry Connolly, Virginia Democrat, is the Ranking Member of the House Oversight and Government Reform Subcommittee on Government Operations.

Our nation's counties, cybersecurity and ransomware

By Dr. Alan R. Shark

America's counties employ 3.6 million employees who serve some 308 million county residents. Counties play a significant role in every aspect of our lives — including hospitals and clinics, roads, bridges, airports and other infrastructure, public safety and courts — and are largely responsible for local and federal elections administration. Counties provide vital services to all Americans, from issuing birth certificates and marriage licenses, to operating 911 call centers. While balancing numerous administrative responsibilities, counties deliver essential services to ensure healthy, vibrant and safe communities across the United States.

Given this vast scope of responsibilities, county governments have become increasingly attractive to cybercriminals who view counties as vulnerable targets.

The National Association of Counties and the Public Technology Institute recently completed a survey on information technology (IT) professionals' top concerns. It was no surprise that cybersecurity ranked No. 1. Indeed, cybersecurity has been ranked as the top concern over the past five years.

Cybersecurity breaches have grown some 26 percent over last year with ransomware, in particular, continuing to rise.

Imagine waking up to find that all your government files and applications are frozen. You receive a message requesting $23,000 in Bitcoins (basically dollars converted to untraceable cryptocurrency) as the price to regain control of critical files and operations. This is exactly what happened to Mecklenburg County, North Carolina, in early December 2017.

Until recently, ransomware has become highly profitable for the "bad guys." Ransomware demands are often paid because of the relatively small amount asked coupled with what it might cost to completely reconstruct a system — let alone the perceived comfort of immediate relief.

In the case of Mecklenburg County, they spent many hours agonizing over the pros and cons of "giving in." It would have been far cheaper to pay the bad guys off, but what if they reneged, or asked for more, or attacked again?

In the end, Mecklenburg County took the advice of most major security experts; they decided not to pay and, instead, went through a labor-intensive and time-consuming exercise in rebuilding their systems from previous backups. It was more than money that was at stake.

As long as ransomware demands are met, more such attacks will continue. But according to cyber experts, if more counties followed the latest best practices, much can be done toward prevention.

County IT professionals are fighting back and adapting to an ever-challenging environment. Just a few years ago, the focus was on purchasing better firewalls as the main defense. Today, IT professionals are moving away from relying on perimeter-based protection systems and toward active monitoring systems that constantly scan for intrusions and system anomalies throughout the enterprise. Savvy IT managers know to have to-the-minute accurate backups, as well as system mirror-image application systems that allow restoration of a system to its pre-infected state. Another major development has been the introduction of software that reviews incoming messages and automatically isolates suspicious files before causing damage.

Imagine waking up to find that all your government files and applications are frozen. You receive a message requesting $23,000 in Bitcoins (basically dollars converted to untraceable cryptocurrency) as the price to regain control of critical files and operations. This is exactly what happened to Mecklenburg County, North Carolina, in early December 2017.

Today, county leaders realize that cybersecurity defense is an all-hands endeavor. All county employees should undergo continuous cybersecurity awareness training to keep up with the latest threats. IT professionals should undergo continuous training to keep apace with the latest technologies and mitigation strategies. IT professionals should take the lead in establishing and enforcing new policies regarding mobile device usage and storage in county government.

Finally, regardless of all the new technologies, the human element holds major opportunities for counties in cybersecurity awareness as well as leadership training. Counties must be willing to share their experiences with others so that when something bad happens, others can learn and adjust. Here, Mecklenburg County is but one good example.

Dr. Alan R. Shark writes for the National Association of Counties (NACo) serving as a senior advisor for technology leadership. Dr. Shark also serves as Executive Director and CEO for the Public Technology Institute, and is an associate professor at the Schar School of Policy & Government, George Mason University.

Too small to get hacked? Think again ...

By Maria Roat

I worked for two small businesses in the early 2000s. I was responsible for managing a Network and Security Operations Center that monitored and managed several federal agencies' networks and systems — an environment that was much different than it is today. We focused on changes to the operating environment — internal threats. However, we operated in an environment where more than 50 percent of American households had internet access. The sophistication of the security tools at that time was limited, so threats like the Sapphire worm were able to infect hundreds of thousands of computers in less than three hours.

Fast-forward to today where at the U.S. Small Business Administration (SBA), I am responsible for securing and protecting the data of millions of entrepreneurs and small businesses across the country. Nearly 30 million small businesses employ approximately 50 percent of the nation's workforce, and these small businesses are also responsible for protecting their own data.

Small businesses are targets, and many are unprepared for cybersecurity challenges including ever-changing and increasing threats from malware, viruses and ransomware against intellectual property and company data. Nor are they adequately prepared to recognize or respond to an internal or external incident.

Business owners depend on information technology to protect not only their own data, but their client's data as well. Further, intellectual property must be protected. Cloud technologies make it easy to buy technology applications such as human resources and financial applications — no hardware or software capital expenses required. It's all about the data, and data is an asset that has significant financial value.

It is important for small-business owners to understand the protections afforded by their cloud-based technology service providers. Is the data stored in the United States? Is it backed up, and where? What is the recovery or restoration time? How do I know I can trust my provider to protect my data? What happens if there is a security breach? What are the liabilities in case of a security breach, and who is responsible?

Small businesses constantly face this paradox – either focus on growing their business or divert their attention to cybersecurity. This is where the Small Business Administration plays a vital role with small businesses.

Small businesses have public records such as business licenses, DUNS records and articles of incorporation. Even registering for a web domain can expose business owners to cyberattacks if their profile is public. Each of these pieces of public information in aggregate can be compiled by cyberattackers, making business owners and their employees vulnerable to identity theft.

A small-business owner must understand his or her data exposure when employees are connecting to a public network such as the local coffee shop. Not only is it about protecting the data, but securing the connection to the data. And, it is critical to train employees on basic security awareness to address phishing and spam attacks from social media, social engineering, messaging services, and other technology or human interactions.

A small-business owner cannot be naïve and assume that insider threat is not a factor. Insider threats include personnel, facilities, information, equipment, networks and computer systems. Research indicates that insider threat is a major factor for all organizations.

Navigating the many resources available is a challenge and can be confusing, especially if business owners do not understand what they need, what they must protect, and what their responsibilities are.

There are 46 identified cybersecurity programs, projects and activities available to small businesses across the federal government alone. Additionally, cybersecurity resources for small businesses can be found in a myriad of other venues, including state and local web sites, online courses, and workshops from groups such as the National Cyber Security Alliance and local chambers of commerce.

Business owners can learn how to detect a breach; be safer online; and identify key assets and ransomware and phishing attacks, to name a few. Some worthwhile investments business owners should consider is cyber insurance and subscribing to alerts from United States Computer Emergency Readiness Team (US-CERT). US-CERT is simple, free and provides valuable and timely information on cyberthreats and vulnerabilities.

The SBA, in partnership with the Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST), are responding to Congress' instructions to develop a Cyber Strategy for Small Business Development Centers (SBDC). The SBDCs must advance their capabilities to provide cybersecurity support to small businesses.

The SBA is uniquely positioned to provide the outreach and cyber-advising expertise that is responsive to small business concerns. SBDCs leverage existing partnerships and develop new ones with federal, state and local governments; educational institutions; and other private companies. In partnership with the SBA, DHS has a critical role leading the development of cybersecurity guides and promoting cybersecurity resources.

It is often stated that a breach in security is not "if" it will happen, but "when" it will happen. Organizations of all sizes have dealt with security breaches, and in the last few years, the number of cyber incidents has increased substantially. It is imperative for small businesses to be adequately informed and prepared. Small businesses constantly face this paradox— either focus on growing their business or divert their attention to cybersecurity.

This is where SBA plays a vital role with small businesses: The SBA provides the assistance small businesses need, so they can focus their energy on business growth. As small businesses grow, so too does our nation's economy.

Maria Roat is Chief Information Officer at the U.S. Small Business Administration.

Veterans wanted! Cyber career opportunities abound for veterans

By Karen S. Evans

Cybersecurity jobs are grounded in patriotism. Every single day, businesses and government entities across the nation are being targeted and breached by opportunists (with varying motives) who identify vulnerabilities and take advantage of those vulnerabilities, leaving a wake of victims in their path.

All industries are now targets, with millions of citizens being victimized in our country. Therefore, the mission to provide defenses, reduce vulnerabilities and protect citizens is a priority both in the public and private sectors. The difficulty, though, has been to identify enough talent to fill the significant cybersecurity workforce gap — one estimate put it at 1.8 million workers by 2022 — we see today. This is where the importance of veterans comes into play.

Today, many veterans are trying to find a promising career path following their tenure in the service. Whether they have a technological background or not, veterans should strongly consider the field of cybersecurity as a potential path. With a history of serving the nation and securing the homeland, veterans already have the mental attitude and protective instincts needed to be successful new cybersecurity hires. Veterans also have extensive experience in high-stress, high-stakes situations mirroring cybersecurity breach response and the strategies needed to defend assets.

Today, there is a wealth of training opportunities to help veterans break into the field without investing significant time and money. All that's necessary is a desire and natural interest to pursue a cybersecurity career and the initiative to take the first steps. Although employers appreciate degrees, having a four-year degree in computer science with a cybersecurity focus is not required. Barriers to entry have thus been reduced. Employers realize that with technology constantly changing, they need to hire talent that is naturally interested and curious in information security and independently exploring and developing their skills. Employers want to know potential hires can do the job beginning on Day One, and a diploma doesn't guarantee this capability. Instead, employers recognize there are other skills-set qualifiers — specifically, competitions.

Cybersecurity competitions are a method of validating skill levels, whether the individual learned these skills in a formal education environment or not, and successful performance in competitions holds significant weight on an individual's resume. Veterans have the opportunity to participate in such competitions and build their resume**s** in such a way that will make them attractive for a cybersecurity-focused position.

U.S. Cyber Challenge (USCC) was created as one of the methods to identify, train and validate skills and performance while providing networking opportunities with potential employers.

As an educational program, USCC first identifies talent through an annual online competition called Cyber Quests. Top performers in the online competition are then invited to one of the week-long boot camps throughout the country to receive high-caliber training with our nation's leading experts in the fields. The competitor's performance determines the fees associated with the boot camp.

In addition to technical training, USCC camps also offer ethics training, resume workshops and job fairs. This holistic approach to cybersecurity training helps direct a career path for aspiring talent.

A substantial list of cybersecurity competitions is provided on the CyberCompEx.org website. CyberCompEx.org was developed as an online social community for those interested in deepening their knowledge of cybersecurity and networking in the community for potential opportunities. CyberCompEx offers an updated list of cybersecurity competitions offered across the country, which are mapped to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. The NICE Framework was developed by National Institute for Standards and Technology (NIST) as a "resource that categorizes and describes cybersecurity work." By applying the NICE Framework to competitions, individuals can strategically choose the competitions best fitting their career aspirations for specific cybersecurity positions. The NICE Framework also helps employers identify gaps in their workforce and accurately describe the positions available for prospective employees.

The need for cybersecurity professionals is great, and veterans can help us close the workforce gap. To get started, veterans can join the CyberCompEx.org community to understand what opportunities for competition involvement are available to them and next steps in their pursuit of a career in cybersecurity.

U.S. Cyber Challenge participants competed in a "Capture-the-Flag" competition as part of a weeklong boot camp training program with experts. Photo credit: San Jose State University.

Karen S. Evans is National Director of U.S. Cyber Challenge. The USCC is a program supported by the Department of Homeland Security Science and Technology Directorate through a contract with the Center for Internet Security, a 501(c)3 organization. It has the mission to significantly reduce the shortage in the cyber workforce by serving as the premier program to identify, attract, recruit and place the next generation of cybersecurity professionals. USCC's goal is to find 10,000 of America's best and brightest to fill the ranks of cybersecurity professionals in jobs where their skills can be of the greatest value to the nation. Visit us online: www.uscyberchallenge.org. Network with others in cybersecurity: www.cybercompex.org.

Cyber deterrence remains a missing piece of U.S. cybersecurity

By Leo Taddeo

While we wait for Robert Mueller to wrap up his investigation into President Trump's pre-election dealings with Russians, let's remember how we got here. The Russian Government compromised the emails of U.S. political organizations and used the information to damage the Clinton campaign. Punishing any potential violations of U.S. law that enabled this effort is important, so why is the Trump administration doing so little to beef up our nation's ability to investigate and apprehend cybercriminals?

Cybercriminals, including nation-state hackers, are — for the most part — rational beings. Before attacking the U.S., they conduct a risk-reward analysis. Is the risk of getting caught and being held responsible greater than the reward of disrupting services, damaging U.S. infrastructure, or even interfering in our democratic processes? The answer, so far, has been a resounding no. And despite Mr. Trump's promises to shore up the nation's cybersecurity, the risk-reward analysis remains in the attacker's favor. We must change this equation by adding resources to cyber law enforcement.

Throughout the 2016 presidential campaign, then President-elect Trump expressed concern over the state of the nation's cybersecurity. "We have to get very tough on cyber and cyberwarfare. It is a huge problem," Mr. Trump said. "The security aspect of cyber is very, very tough and maybe it's ... it's hardly doable."

Mr. Trump also criticized the cybersecurity efforts of the Obama administration and made a number of promises to beef up the U.S. response to cyber threats. "We have no defense. We're run by people that don't know what they're doing," he said.

The Obama administration's efforts did indeed come up short in doing enough to stop attacks and reduce exposure. That administration was too cautious in its steps to create a real deterrent and put too much focus on information sharing as a countermeasure.

Mr. Trump promised to turn things around, starting with a 90-day cybersecurity review. "We have some of the greatest computer minds anywhere in the world that we've assembled," he said. "We're going to put those minds together and we're going to form a defense."

But all that talk appears to be just that. In the early part of the Trump administration, we saw some of the president's thinking in a draft cybersecurity policy. This included a leading role for the U.S. military and a new approach to confronting cyberthreats. Under the order, the Department of Defense would have 60 days to review national security systems for vulnerabilities, and the Department of Homeland Security would have 60 days to review the protection of critical infrastructure.

More notable, however, is what was left out of the draft: This is no mention of the FBI. That was one thing the Obama administration addressed early on. The FBI played an important role in cybersecurity.

After much criticism, Mr. Trump's early draft policy gave way to a watered-down version issued in the form of an executive order in May of 2017. Unfortunately, the executive order wasn't much better than the draft policy, and it sounded very familiar. The Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure is largely based on the policies and procedures established under the Obama administration.

At the time of the signing, Ben Flatgard, former National Security Council Director for Cybersecurity Policy, told Ars Technica, "[The order] is directionally sound in many regards. It gives you incremental improvements and progress and some consolidation of stuff we've already put in place."

But he added: "[F]or a new administration, this doesn't represent big, ambitious plans to really leap forward in terms of how we address cyber threats."

The people best positioned to advise Mr. Trump on cybersecurity appeared to agree. In August 2017, the administration lost a number of cybersecurity advisors, as a quarter of the members of the National Infrastructure Advisory Council resigned from their posts, citing in their resignation letter, "specific shortfalls in the administration's approach to cybersecurity," among other things.

What the administration failed to do in the executive order must be addressed. The U.S. needs:

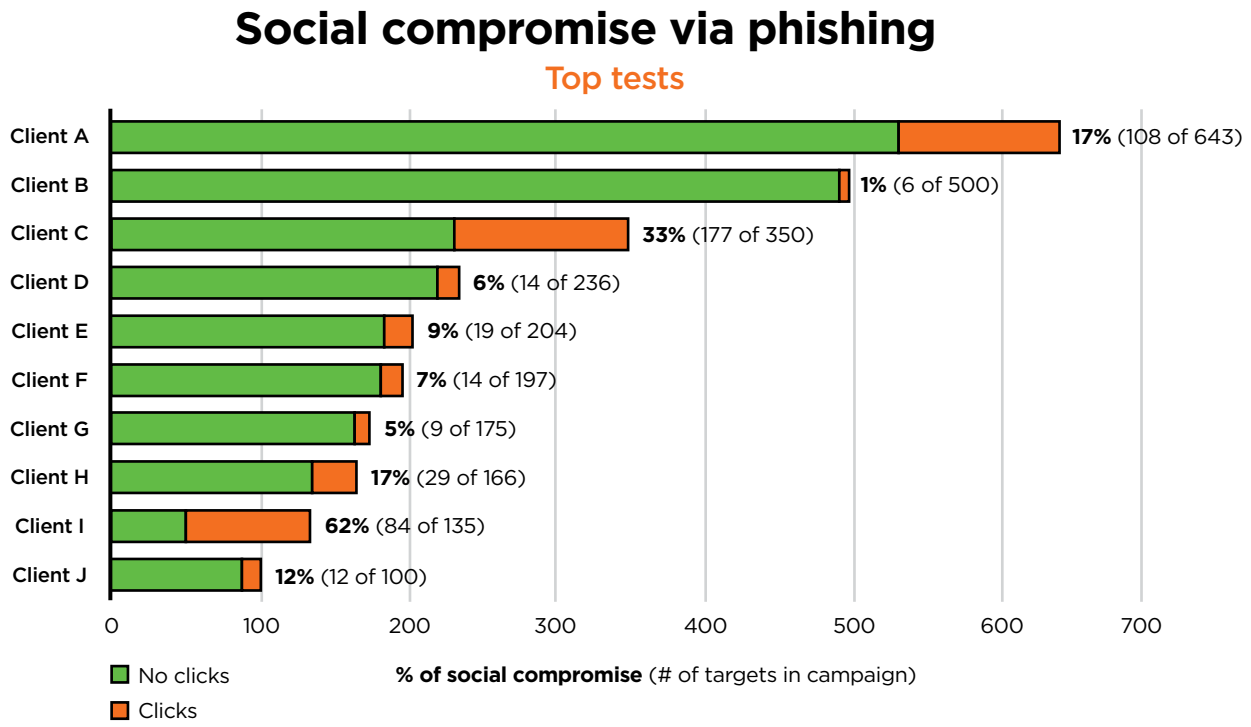
- Legislation to streamline information-sharing and cooperation with friendly foreign governments.
- More resources for the FBI and other federal law enforcement agencies to go after cyber spies and cybercriminals.
- A consolidated central repository for both state and federal law enforcement on cyber crime.

Until the administration addresses the need for law enforcement resources to improve cyber deterrence, our country remains in a precarious position. Nation-state cyberattackers know that there is little or no risk involved in attacking the U.S., and until that changes the U.S. will continue to have a big target looming over it.

Leo Taddeo is Chief Information Security Office at Cyxtera, where he is responsible for oversight of Cyxtera's global security operations, investigations and intelligence programs, crisis management, and business continuity processes. He provides deep domain insight into the techniques, tactics and procedures used by cybercriminals to help Cyxtera continue to develop disruptive solutions that enable customers to defend against advanced threats and breaches. Mr. Taddeo, a decorated Gulf War Marine veteran, is also former Special Agent in Charge of the Special Operations/Cyber Division of the FBI's New York Office.

Human phish-bait: Why people are the weakest link in our cyber defense

By Tom McAndrew



Over the past century there have been tremendous improvements in our ability to use and defend cyber systems. Technology itself has changed drastically from our heavy vacuum tube computers in the 1950s to the world we see today, teeming with mobile devices, the Internet of Things, Cloud computing — and the next big idea.

However, in every piece of technology we have created, there has been a single vulnerability, a common issue that plagues every engineer and programmer: the human element.

Until the 1990s, humans primarily caused issues through inadvertent mistakes: fat fingering the wrong code, entering data in a way that no one considered, forgetting an important task or process. But over time, we have seen other humans — those with malicious intent — exploit these weakness in new and innovating ways. So much emphasis is put on cutting-edge technologies that defend and fight our networks, but very little is written about the greater risks posed by the fallibility of people that move our businesses forward on a daily basis.

So, where are the greatest points of risk? While there is no one answer for every enterprise, every person that is a part of the business ecosystem can contribute to "the insider threat": authorized users that impact the security of the systems they use, intentionally or unintentionally. This includes employees in every department, vendors, partners, even customers. People have an innate desire to make things easier and accept risk by compromising security, usually without realizing it. Use a four-digit PIN instead of a password — sold. Use the same PIN across my ATM and all my systems — done. Make my shopping experience easier by doing one-click with no authentication — sign me up.

In our hectic, busy lives, people often unknowingly accept risk in the name of simplifying chaos without fully understanding the impact, and cybersecurity professionals are constantly trying to work around and respond to our bad habits.

We cannot accept the risk when we are unaware of the threats and their impact.

The majority of cybersecurity breaches introduce malware by simply sending a malicious email to targets and hoping they fall for the bait. Whether it's an email attachment such as a funny photo, video, spreadsheet or Word document, or a link to a malicious website, it is just as easy for an attacker to get someone to fall for their tricks today as it was 20 years ago. In fact, many believe it is even easier today because the attack tools are automated and free for purchase. No IT savvy is needed.

Coalfire conducted cybersecurity engagements for more than 2,500 clients in the past two years and analyzed the data from our phishing attacks. Companies hire us to test their defenses to see how well they work and what their susceptibility is to an attacker.

The data is sobering — during nearly 100 percent of our phishing campaigns, we can get people to do things they shouldn't. And usually we can lure in about 10 percent of the population. You may think a 90-percent defense rate is an "A," but in cyber warfare it means the bad guys have the upper hand. (Imagine if the food you ate was safe for consumption 90 percent of the time?)

The accompanying chart, drawn from a Coalfire report to be released in early 2018, shows our penetration testers' rate of success in phishing campaigns conducted on a representative set of 10 customers. No customer was left unscathed: The most successful company saw a 1 percent click rate; most of our customers saw 5 percent-plus; and one as high as 33 percent. These customers invested considerable time, training and money into defending themselves — and yet, one in three people still did the wrong thing.

So, what does a bad guy do with a phishing scam? Ransomware, which freezes data assets by encrypting them until payment is received (usually via cryptocurrency), is one potential result.

Ransomware has exploded from a nearly nonexistent form of crime three years ago into a $2 billion-plus market. This blight on the cyber domain has interrupted operations of critical organizations such as hospitals — and is frequently enabled by phishing. According to most reports, phishing has been the primary ransomware introduction method in a steadily growing number of incidents, a trend that is likely to continue to grow. Infected websites are another significant method of delivery, and many of these websites attract visitors through, you guessed it, phishing attacks.

So, what is the solution to the human vulnerability conundrum? The answer is both simple and complicated: training and technology.

Companies that have good cybersecurity training and awareness are less susceptible to phishing. They will think twice before clicking that link or downloading that file. They will also react quicker and get help if they know what to do. Additionally, it's essential to leverage information technology systems to identify likely scams, remove or quarantine the emails, and learn from one mistake and apply it to others.

In order to stop phishing, we also have to remove humans from the loop to the greatest practical extent and leverage technology.

We are, and always will be, the unknown parameter in an increasing digital world. Don't fight it, embrace it — it's this unknown, unpredictable aspect that makes us human. But if we hope to win in the war against cyberthreats, we must limit the consequences of our actions through better training and technology.

Tom McAndrew is Chief Operating Officer at Coalfire, an independent cybersecurity advisory that provides independent assessments, technical testing, cyber engineering, and cyber risk management services to private and public sector companies. A graduate of the U.S. Naval Academy, Tom is one of the leading experts in cybersecurity, with expertise in Cloud ecosystems, cfinancial services, retail and government security strategies. He is a member of the National Association of Corporate Directors, serving on several boards, and was recognized as one of the top influencers in the Federal Government (FCW Federal 100 Award).

U.S. ingenuity created the Internet; can it keep it safe and secure?

By Rep. Mike Gallagher

On March 23, 2016, Su Bin, a Chinese national, pled guilty to a criminal conspiracy involving hacking into the networks of key American defense contractors, stealing critical military data and then sending that information back to China. The data he stole involved programs such as the C-17 strategic airlifter as well as advanced American fighter jets. This operation was just one in a series of recent high-profile, cyber espionage campaigns against U.S. military targets.

Chinese cyber warfare, however, targets much more than the American military. As the U.S.-China Economic and Security Review Commission describes, "China has laid out an ambitious whole-of-government plan to achieve dominance in advanced technology." To this end, Chinese doctrine blurs military and economic power and leverages cyberattacks and vulnerabilities to further its interests in both domains. A landmark 2013 study on intellectual property theft found that China is responsible for 96 percent of cyber espionage attacks. Even if this figure is high, Chinese intellectual-property theft alone costs the United States more than $100 billion in annual sales and 2.1 million jobs. All told, roughly $300 billion in American intellectual property is stolen over networks each year.

This past summer, U.S. Immigration and Customs Enforcement released a memo cautioning that DJI — a Chinese company that owns about half of the entire commercial drone market across North America — was transmitting key information on American infrastructure and law enforcement to the Chinese government. As the memo describes, DJI targets American customers based on their "ability to disrupt critical infrastructure," amassing customers that include "some of the biggest utility and transportation companies in the United States." Concerns about data security led the Army to ban soldiers from using DJI devices last fall.

And last year, the FBI arrested a Chinese national linked to the catastrophic 2015 breach of the Official of Personnel Management, which resulted in the compromise of highly sensitive information of over 21 million Americans. Intelligence officials are also concerned about the recent Chinese purchase of Grindr, a gay dating application, as it potentially gives the Chinese government access to a large pool of extremely personal data.

The threat extends into all our communities. A few hours from my hometown of Green Bay, Wisconsin, Chinese actors hacked the back office computer of Cate Machine & Welding, a local family-owned business. After taking control of Cate's relatively unprotected server, the hackers used it to launch subsequent attacks against businesses, law firms and universities across the globe — from Silicon Valley to New York to Thailand.

This integrated Chinese approach to cyber, economic and military power demands that we come up with a creative and strategic response of our own. The United States cannot and should not mirror China's centralized model. China is an autocratic society in which the government can centrally plan and implement a unified approach. In contrast, our free and open system, while less directed, fosters innovation and creativity. This is a feature, not a bug. This is one reason why almost 330,000 Chinese nationals came to America in 2016 to study in our world-class universities.

So we must find a way to reinforce the strengths of our open system — a system in which citizens should jealously guard their privacy and intellectual property — while also fostering closer collaboration between government and the private sector. As one group of cyber experts recently argued, "the U.S. public and private sectors [must] learn how to train, exercise, and operate cooperatively in cyberspace."

After all, success in cyber ultimately depends on human capital and creativity. Here too, we face challenges. China has built-in numeric advantages when it comes to its labor force, and it is moving rapidly to develop specialized cyber warriors — with four to six dedicated cybersecurity schools planned over the next 10 years. In contrast, the United States is struggling to meet the increasing demand for cyber, with over 285,000 cyber-related job openings (http://cyberseek.org/heatmap.html). We must work diligently to develop new educational and workforce-development pathways to stay ahead of our competitors.

One idea we should explore is creating a cyber service academy, not unlike West Point or the Naval Academy, where we could train the next generation of cyber warriors to serve in and out of uniform. The private sector has already recognized the importance of starting cyber education well before college, and leading companies are already working with schools and organizations at the K-12 level to teach basic cyber skills. The government needs to catch up and complement this effort.

The United States cannot afford to fall further behind in this increasingly central domain of geopolitical competition or suffer additional cyberattacks that increase our vulnerabilities across all levels of society. We need a national wake-up call that acknowledges our long-term competition with China, especially in the cyber domain, and recognizes that in order to win, we all have to participate. After all, American ingenuity invented the internet, thereby unleashing opportunities for human advancement and prosperity that would have seemed impossible just a few decades ago. Now it is our responsibility to secure these blessings to ourselves and our posterity.

Rep. Mike Gallagher, Wisconsin Republican, serves on the House Armed Services Committee and House Homeland Security Committee.

Chinese information warfare: 'The Panda That Eats, Shoots, and Leaves'

By Bill Gertz

The following is an excerpt from "iWar: War and Peace in the Information Age."

No other nation today poses a greater danger to American national security than China, a state engaged in an unprecedented campaign of information warfare using both massive cyberattacks and influence operations aimed at diminishing what Beijing regards as its most important strategic enemy. Yet American leaders remain lost in a Cold War political gambit that once saw China as covert ally against the Soviet Union. Today the Soviet Union is gone but China remains a nuclear-armed communist dictatorship on the march.

From an information warfare stance, China today has emerged as one of the most powerful and capable threats facing the United States. By May 2016 American intelligence agencies had made a startling discovery: Chinese cyber-intelligence services had developed technology and network penetration skills allowing them to control the results of Internet searches conducted on Google's world-famous search engine. By controlling one of the most significant Information Age technologies used in refining and searching the massive ocean of data on the Internet, the Chinese are now able to control and influence what millions of users in China see when they search using Google. Thus a search for the name Tiananmen — the main square in Beijing, where Chinese troops murdered unarmed pro-democracy protesters in June 1989 — can be spoofed by Chinese information warriors into returning results in which the first several pages make no reference to the massacre. The breakthrough is

» see **GERTZ** | C29

GERTZ

From page **C28**

similar to the kind of totalitarian control outlined in George Orwell's novel Nineteen Eighty-Four with the creation of a fictional language called Newspeak, which was used to serve the total dominance of the state.

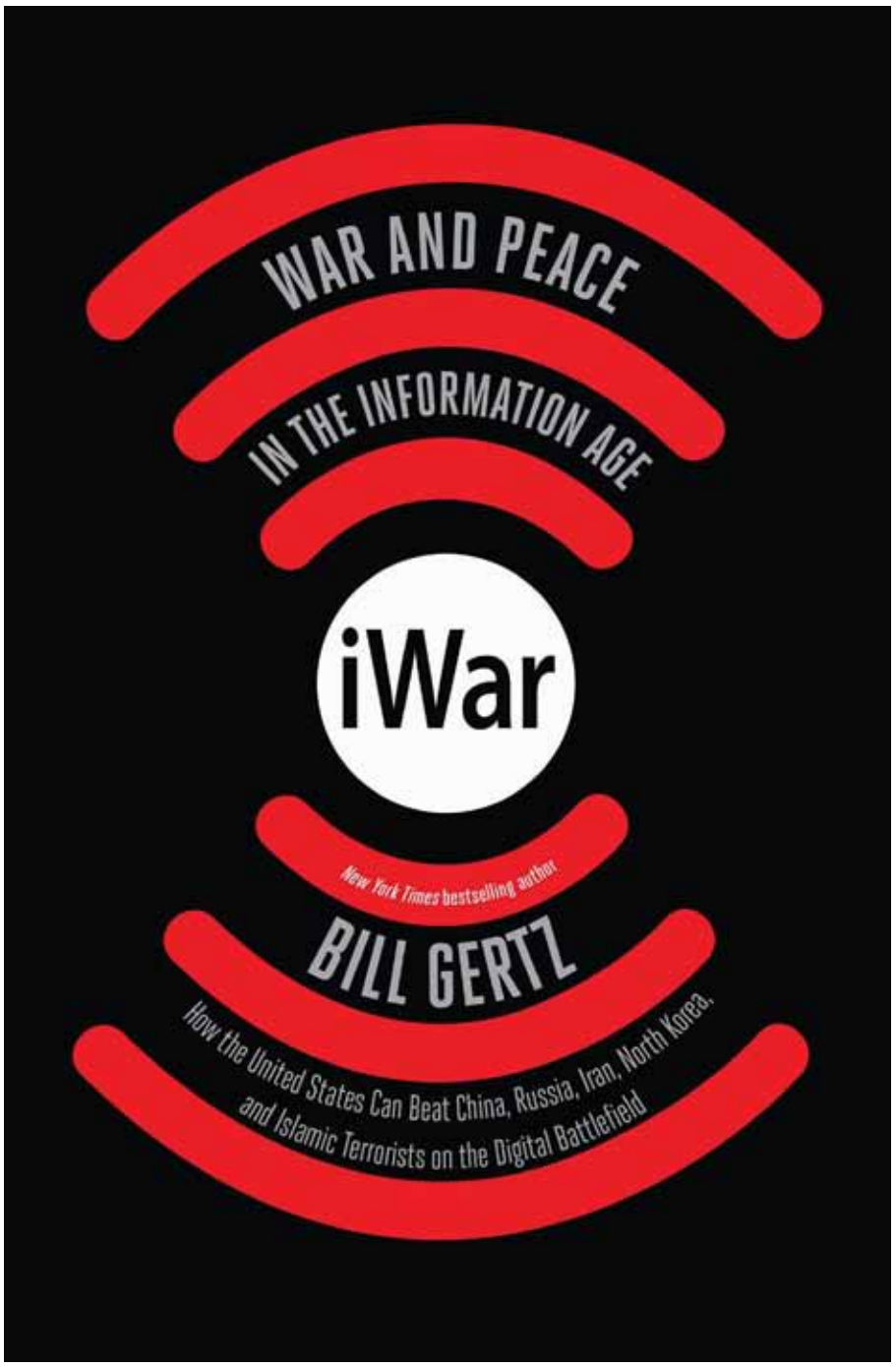
Technically, what China did was a major breakthrough in search engine optimization — the art and science of making sites appear higher or lower in search listings. The feat requires a high degree of technical skill to pull off and would require learning the secret algorithms — self-contained, step- by-step computer search operations — used by Google. The intelligence suggests that Chinese cyberwarfare researchers had made a quantum leap in capability by actually gaining access to Google secrets and machines and adjusting the algorithms to make sure searches are produced according to Chinese information warfare goals.

Those goals are to promote continued rule by the Communist Party of China and to attack and defeat China's main enemy: the United States of America. Thus Chinese information warriors can continue the lies and deception that China poses no threat, is a peaceful country, does not seek to take over surrounding waterways, and does not abuse human rights, and that its large-scale military buildup is for purely defensive purposes.

The dominant battle space for Chinese information warfare programs is the Internet, using a combination of covert and overt means. The most visible means of attack can be seen in Chinese media that is used to control the population domestically, and to attack the United States, Japan, and other declared enemies through an international network of state-controlled propaganda outlets, both print and digital, that have proved highly effective in influencing foreign audiences. One of the flagship party mouthpieces is China Daily, an English-language newspaper with a global circulation of 900,000 and an estimated 43 million readers online. China Central Television, known as CCTV, operates a twenty- four-hour cable news outlet as well to support its information warfare campaigns.

One of the most damaging Chinese cyberattacks against the United States was the theft of federal employee records in the Office of Personnel Management (OPM) in 2015 . That attack took place after an earlier private sector cyber strike against millions of medical records held by the major health-care provider Anthem.

The data theft included the massive loss of 21.5 million records. Worse, the OPM delicately announced that among those millions of stolen records was "an incident" affecting background investigation records, among some of the most sensitive information in the government's possession used in determining eligibility for access to classified information.



It was a security disaster for the millions who held security clearances and were now vulnerable to Chinese intelligence targeting, recruitment, and neutralization. A senior U.S. intelligence official briefed on the classified details of the OPM told me that the early technical intelligence analysis of the data theft revealed that it was part of a PLA military hacking operation. "It is fair to say this is a Chinese PLA cyberattack," said the official, adding that the conclusion was based on an analysis of the software operating methods used to gain access to the government network.

The threat was not theoretical. In the months after the OPM breach, several former intelligence officials began receiving threatening telephone calls that authorities believe stemmed from the compromised information obtained from OPM background investigation data hacked by the Chinese.

One of the most damaging Chinese cyberattacks ... was the theft of federal employee records in the Office of Personnel Management (OPM) in 2015... [which] included the massive loss of 21.5 million records.

By the summer of 2015, the group of sixteen U.S. intelligence agencies — including the CIA, DIA, and NSA — that make up what is called the intelligence community weighed in on the growing threat of strategic cyberattacks against the United States. In their top-secret National Intelligence Estimate, the consensus was that as long as the continued policy of not responding remained in place, the United States would continue to be victimized by increasingly damaging cyberattacks on both government and private sector networks. A strong reaction was essential.

Chinese cyberattacks have been massive and have inflicted extreme damage to U.S. national security.

Among the exotic Chinese information weapons Beijing plans to use in a future conflict are holographic projectors and laser-glaring arms that can present large unusual images in the skies above enemy forces that would simulate hallucinations among troops on the ground, according to one recent translated Chinese military report on the subject.

Traditional propaganda also will be used, including "public opinion propaganda and PSYWAR weapons to execute psychological attacks against the enemy, so as to disrupt the enemy command decision making, disintegrate the enemy troop morale, and shake the enemy's will to wage war," according to recently translated Chinese military writings.

As Jake Bebber, a Navy officer posted with the U.S. Cyber Command, put it, the threat from China and its strategy of seeking the destruction of the United States have been misunderstood by the U.S. government and military. "China seeks to win without fighting, so the real danger is not that America will find itself in a war with China, but that America will find itself the loser without a shot being fired," he wrote in a report for the Center for International Maritime Security.

In the future, an American president must come to the realization that the decades-long policy of appeasing and accommodating the communist regime in Beijing is not just contrary to American national interests, but is in fact advancing a new strategic threat to free and democratic systems everywhere.

China today employs strategic information warfare to defeat its main rival: the United States. China's demands to control social media and the Internet are part of its information warfare against America and must be resisted if free and open societies and the information technology they widely use are to prevail. China remains the most dangerous strategic threat to America — both informationally and militarily.

Bill Gertz is a national security columnist for The Washington Times and senior editor of The Washington Free Beacon. This article is excerpted from a chapter of his book, "iWar: War and Peace in the Information Age." For more information, see iwarbook.com.

For cybersecurity problems, seek bottom-up solutions

By Andrea O'Sullivan

Everyone agrees on the need for strong cybersecurity policy. Each month, we see headlines telling of high-profile hacks and expansive bugs that threaten our nation's commerce, privacy and even our safety. But there is much disagreement on how best to proceed.

Some commentators suggest that a top-down, government-directed solution is the only path forward. Yet history and experience suggests that a bottom-up, decentralized solution to our cybersecurity problems may prove more robust in the long run.

Consider the question of vulnerable devices. Observers like computer security expert Bruce Schneier have argued that there is simply no market incentive for device manufacturers to ensure that their products are reasonably secure before shipping them off to consumers who aren't exactly security-savvy. Businesses, the argument goes, would rather make a short-term buck and risk calamity than take the extra time to probe devices for vulnerabilities.

Indeed, if the marketplace consisted of nothing more than security-ignorant buyers and sellers who care only for short-term profits, we'd have a big problem. Devices would be chronically insecure without some kind of top-down regulation.

But first remember that computing devices are hardly "unregulated." Federal agencies like the Federal Trade Commission (FTC) already have the authority to oversee and investigate when product sellers are suspected of foul play.

For many, this existing regulation is not enough. They propose the creation of some new federal body — specific ideas have included a "Department of Robotics" or "Federal Software Commission" — that would be granted new and expansive authority over vast domains of our economy. The policy details of such proposals are generally short: Create an agency, and expect it to solve our security woes.

There are many problems with the top-down approach. First, it fails to recognize the many real market incentives that contribute to good security. Bad actors already risk being blacklisted by responsible companies, losing customers due to bad reputation, or lawsuits in the courts for negligent behavior. This process may not be immediate, and it may not be perfect, but it does an adequate job of weeding out problems.

Next, the top-down approach imposes real costs on manufacturers and consumers. Oftentimes, regulators are just as much, if not more, in the dark about market risks and opportunities as neophyte producers. Their policies may therefore incorrectly stymie certain areas of production without any real benefit, which ultimately raises the costs to consumers.

What's worse, this misdirection could miss true security threats, ultimately leaving us no safer than before. Consider the federal government's own bad track record of forcing us to comply with checklist-style measures while missing simple blunders like poor employee password management.

But perhaps most importantly, the top-down approach distracts us from the kinds of bottom-up solutions that could truly provide a robust security environment. As my former colleague Eli Dourado explains in his paper, "Internet Security Without Law," Internet Service Providers (ISPs) have developed a system of voluntary notice and blacklisting that promotes proactive security outcomes. This kind of arrangement should be a model for how best to proceed.

Meanwhile, my Mercatus Center colleague Anne Hobson uses the metaphor of disaster recovery to explain the ideal path for cybersecurity policy. The idea that planners can accurately predict and direct producers to prepare for all potential security risks is grounded in folly that will always lead to failure. We will never be able to be 100 percent protected from all risks. We can, however, promote an environment that allows us to adapt to the inevitable hiccups that do arise.

What does this mean in terms of concrete policy?

Thankfully, cybersecurity experts already recognize the importance of resiliency for security. Like the Obama administration, the Trump administration designated resilience-building as a key cybersecurity policy goal. This means that public and private bodies alike are working together to develop and strengthen information-sharing bodies, education and certification programs, and even a cyber-insurance industry.

Policymakers should heed and supplement these existing efforts before attempting to erect an awkward command-and-control style regulatory body to direct security policy.

In general, we should all maintain a posture of humility and open-mindedness when seeking security solutions. The threats are often vast, and the answers to these thorny issues will almost never be as straightforward as simply creating a federal agency to "deal with things." Only decentralized resilience can provide the recovery responses needed to weather the coming digital storms.

Andrea O'Sullivan is a program manager with the Mercatus Center at George Mason University's Technology Policy Program.

Cybersecurity: Is anything really safe?

By Steve Durbin

2017 was a spectacular year for cyberattacks, including some previous ones only recently and reluctantly disclosed by embarrassed victims. They include a veritable who's who of government, business and technology, including some of the world's most technically sophisticated organizations.

Their misfortune raises a critical question: Is anything really safe? Do the security recommendations of experts actually matter? Or do we simply wait for our turn to be victimized, possibly by an attack so massive that it shuts down the entire data-driven infrastructure at the heart of 21st century life?

The answer is that there's both good and bad news. First, the bad news.

Data breaches are likely to grow in 2018, aggravated both by the Internet of Things and security weaknesses in company supply chains. So, major disruptive attacks are indeed possible.

In addition, expect "Crime-as-a-Service" (CaaS) will develop as cybercriminal organizations continue to become more sophisticated. And new regulations, such as the European Union's General Data Protection Regulation (GDPR), will add another layer of complexity to the issue of critical information asset management that many organizations are already struggling with. These are all among the top global security threats I predict businesses will face in 2018.

But there's also good news. As managing director of an organization dedicated to cybersecurity, my view is that these challenges are not insurmountable. A future in which we can enjoy the benefits of cybertechnology in relative safety is within reach — but it will require us to recognize and apply the same dynamics that have tamed other disruptive technologies in the past.

Consider the case of motor cars. It's been more than a century since automobiles began crowding America's streets. At the time, it was seen by many as a deeply disrupting technology, aggravated by reckless driving and an enormous rate of carnage. But by 2016, that death rate had declined by 95 percent. In between, what began as a disruptive toy for the well-to-do had evolved into an integral part of daily life. That transition involved a combination of technical advances, government regulations and shifts in public attitude — a potent combination of factors. That same trifecta can also apply to other transformative creations, including cybertechnology:

■ **Technical advances.** It may seem surprising, but further advances in technology may be the least important of the forces taming cybercrime. Of course, progress in the fields of encryption and related security measures will continue. However, technological advances tend to be a cat-and-mouse game, with hackers in close pursuit of security workers. And security workers themselves can sometimes be drawn over to the dark side. That said, even modest security technology can slow the pace of malicious hacking. By making it more time-consuming for someone to hack into a digital device, an attacker is less likely to try.

■ **Law of cyberspace**. Although the internet's greatest strength is its global reach, there is no worldwide cyber law. Cyber is only about 20 years old and it takes time for a body of law to evolve, as it did with maritime law. While maritime conventions are not perfect, they are largely effective. At the moment, though, cyber is still the Wild West. Essentially anything goes; you are pretty much on your own.

But there are steps that regulatory bodies can take to reduce the risks. One, which was recently adopted by New York state's Department of Financial Services, requires all financial organizations there to institute risk-assessment protocols that examine more than a dozen areas where intrusions are possible and then take steps to fix any problems.

■ **Cyber culture.** In December 2013, the British Bankers' Association reported that "traditional" strong-arm bank robberies had dropped by 90 percent since 2003. Instead, larcenous acts are committed with just a few keystrokes — often from thousands of miles away. So to adolescents, the slope leading from cyber mischief into cybercrime is both gradual and hard to discern.

That's because malice isn't typically what motivates young people to become hackers. A big part of it is just having fun. But even hacking behavior, if properly directed, can have value. At Northeastern University, an informal group of hackers use their skills to win bug-bounty contests held by major organizations, including the Pentagon, to find and fix weaknesses in their defenses. But they're the exception.

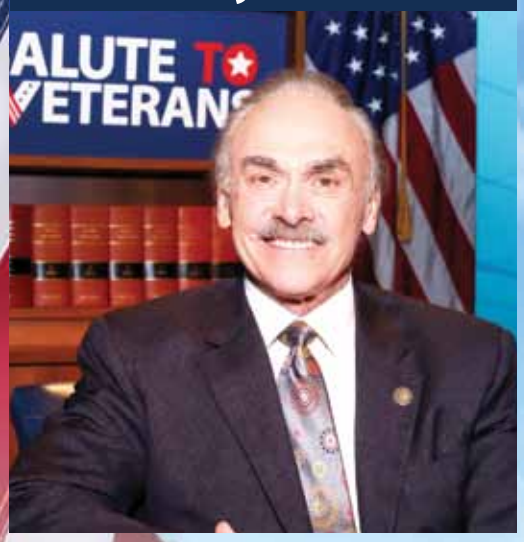
The Wild West brought on by the motor car was eventually absorbed into the mainstream of commerce and culture. But it required a trifecta of improved technology for both vehicles and infrastructure, comprehensive laws coupled with better law enforcement, and a gradual shift in driving culture affecting the perceptions and behavior of motorists.

Imaginative forms of education to enhance cyber culture and support appropriate uses of the technology — including some now underway in school classrooms — will help to shape public expectations and inform responsible behavior for the next generation of cyber citizens.

Steve Durbin is Managing Director of the Information Security Forum (ISF). His main areas of focus include strategy, information technology, cybersecurity and the emerging security threat landscape across both the corporate and personal environments.

SALUTE TO VETERANS

★ Rocky Bleier ★



U.S. Army Veteran, 4-time Champion with Pittsburgh

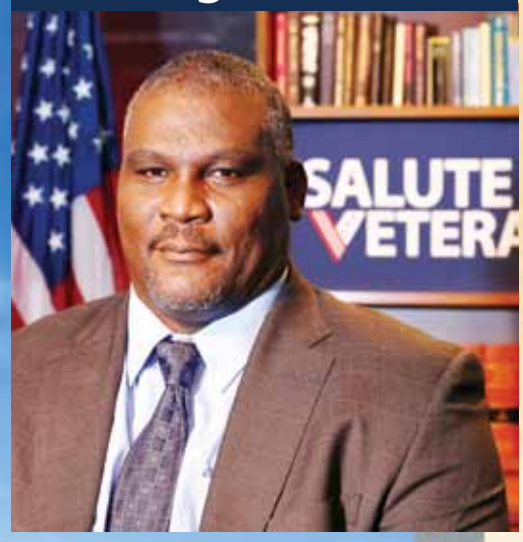
U.S.ARMY

★ Bryce Fisher ★

U.S. Air Force Veteran, 1-time Champion Runner Up with Seattle

U.S. AIR FORCE

★ Greg Gadson ★



U.S. Army Veteran, Honorary Captain & 2-time Champion with New York

U.S.ARMY

Salute to Veterans is a national television series that honors and pays tribute to our nations's veterans, active duty service members, military families and patriotic supporters. The inspirational and educational program offers insightful discussion, resources and solutions for the ongoing issues our veterans face daily. The series tells the stories of distinguished veterans who have served their country, overcome obstacles and made a difference in their communities, while inspiring others to do the same.

SALUTE TO VETERANS

The Salute to Veterans Series was made possible by the generous support of our partners

USAA

SAP

NORTHROP GRUMMAN

Walgreens
at the corner of happy & healthy

Military.com

BJ's
Live Generously.

The Washington Times
www.washingtontimes.com

G.I. JOBS