Cyber Risk GmbH
Rebackerstrasse 7, 8810 Horgen
Phone: +41 43 810 43 61, Web: www.cyber-risk-gmbh.com
Handelsregister des Kantons Zürich, Firmennummer: CHE-244.099.341

Top cyber risk and compliance related news stories and world events, that (for better or for worse) shaped the month's agenda, and what is next

January 2018, cyber risk and compliance in Switzerland

Computational propaganda is the use of technology for political manipulation.

It becomes increasingly easy to influence emotions, attitudes, opinions, and actions of an audience for ideological or political purposes, through the transmission of messages (factual or not) using technology.

State-sponsored trolling and disinformation have proved to be very effective, and the cost of the implementation is very low, as "bots" are a common type of autonomous agents used in computational propaganda.

But today we have some good news. Do you remember US Executive Order 13800, about "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," calling for "resilience against botnets and other automated, distributed threats"?

According to the Executive Order, the Secretary of Commerce and the Secretary of Homeland Security must "lead an open and transparent process to identify and promote action by appropriate stakeholders" with the goal of "dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets)."

Automated and distributed attacks form a threat that reaches beyond any single country, company or sector. These threats are used for a variety of malicious activities, including distributed denial of service (DDoS) attacks that overwhelm networked resources, ransomware attacks that hold systems and data hostage, and computational propaganda campaigns to manipulate and intimidate communities through social media.

Today we have a draft report to the President, that was developed by the Departments of Commerce and Homeland Security in response to Executive Order 13800. The Departments determined that the opportunities and challenges in working toward dramatically reducing threats from automated, distributed attacks can be summarized in six principal themes:

1. Automated, distributed attacks are a global problem.

2. Effective tools exist but are not widely used.

3. Products should be secured during all stages of the lifecycle.

4. Education and awareness is needed.

5. Market incentives are misaligned.

6. This is an ecosystem-wide challenge.

The Departments identified five complementary and mutually supportive goals that would dramatically reduce the threat of automated, distributed attacks and improve the resilience of the ecosystem.

A list of suggested actions for key stakeholders reinforces each goal.

The goals are:

Goal 1: Identify a clear pathway toward an adaptable, sustainable, and secure technology marketplace.

Goal 2: Promote innovation in the infrastructure for dynamic adaptation to evolving threats.

Goal 3: Promote innovation at the edge of the network to prevent, detect, and mitigate bad behavior.

Goal 4: Build coalitions between the security, infrastructure, and operational technology communities domestically and around the world.

Goal 5: Increase awareness and education across the ecosystem.

You can read more at:

https://csrc.nist.gov/CSRC/media/Publications/white-paper/2018/01/05/enhancing-resilience-against-botnets--report-to-the-president/draft/documents/enhancing-resilience-against-botnets-draft.pdf

Now we will discuss another very important story.

According to UK's National Cyber Security Centre, typosquatting (also known as cybersquatting or url hijacking) is the deliberate act of registering misspelt popular website domains, to capitalise on internet users accidently typing incorrect characters for a website address into the address bar of a web browser.

Instead of visiting the correct website, users will be taken to an alternative website intended for a variety of malicious purposes, including the theft of personal information, fraud, and the installation of malicious software.

A recent study by cyber security company Sophos found that typosquatting is still a huge industry and there are a significant number of fake domains registered, including sites targeting users of popular websites such as Google, Facebook, Twitter, Microsoft, and Apple.

Specifically, it was found that 80% of all possible one-character variants of Facebook, Google, and Apple website domains are registered.

The issue of typosquatting is not new but can seriously impact individual users as well as businesses, organisations and government websites across the globe.

Although there are solutions including the legitimate purchase of common misspelt domains as part of brand protection, this could amount to hundreds of possible domain name variants which might not be practical or cost effective, particularly for small businesses.

Individual users are advised to double check their url spellings before accessing a website. It is also advisable to bookmark favourite websites and, if in doubt, check url spellings in a popular search engine to make sure they are correct.

Welcome to our monthly newsletter.

Best regards,

George Lekatis

George Lekatis
General Manager, Cyber Risk GmbH
Rebackerstrasse 7, 8810 Horgen
Phone: +41 43 810 43 61
Mobile: +41 79 505 89 60
Email: george.lekatis@cyber-risk-gmbh.com
Web: www.cyber-risk-gmbh.com

Cyber Risk GmbH, Handelsregister des Kantons Zürich, Firmennummer: CHE-244.099.341

Cyber Security instructor-led training in Switzerland, Liechtenstein, and Germany

2018

Cyber Risk GmbH

Cyber Risk GmbH, Handelsregister des Kantons Zürich, Firmennummer: CHE-244.099.341,
Rebackerstrasse 7, 8810 Horgen

Page 1 | 70

Our catalog, *in-house* instructor-led training in Switzerland, Liechtenstein, and Germany:
www.cyber-risk-gmbh.com/Cyber_Risk_GmbH_Catalog_2018.pdf

Our events and *open* instructor-led classes:
www.cyber-risk-gmbh.com/Events.html

Number 1 (Page 8)

Configuration Security Program to Make Network-Connected Systems Less Vulnerable

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

The rise of network-connected systems that are becoming embedded seemingly everywhere–from industrial control systems to aircraft avionics–is opening up a host of rich technical capabilities in deployed systems.

Even so, as the collective technology project underlying this massive deployment of connectivity unfolds, more consumer, industrial, and military players are turning to inexpensive, commodity off-the-shelf (COTS) devices with general-purpose designs applicable for a range of functionalities and deployment options. While less costly and more flexible, commodity components are inherently less secure than the single-purpose, custom devices they are replacing.

Number 2 (Page 11)

Raising Our Game: Cyber Security in an Age of Digital Transformation

Christopher Wray, Director, Federal Bureau of Investigation.
Fordham University - FBI International Conference on Cyber Security, New York City, New York

“Now…well, let’s just say it’s something that’s a little more on my radar. Today, we live much of our lives online, and everything that’s important to us lives on the Internet—and that’s a scary thought for a lot of people. What was once a minor threat—people hacking for fun or for bragging rights—has turned into full-blown economic espionage and lucrative cyber crime.

This threat now comes at us from all sides. We're worried about a range of threat actors, from multi-national cyber syndicates and insider threats to hacktivists. We're seeing an increase in nation-state sponsored computer intrusions. And we're also seeing a "blended threat"—nation-states using criminal hackers to carry out their dirty work. We're also concerned about a wide gamut of methods, from botnets to ransomware."

Number 3 (Page 22)

Increase in HTTPS phishing attacks

National Cyber Security Centre
a part of GCHQ

Over the past few years website owners have been encouraged to adopt HTTPS website domains rather than HTTP. With HTTPS, data in transit is encrypted; this provides additional security for transiting data, such as login credentials, which may contain information of use to attackers.

HTTPS domains are verified by SSL Certificate Authorities, who issue and authenticate certificates. The padlock symbol in the URL field links to the certificate provider's website, and users are often advised to trust webpages with this symbol.

Number 4 (Page 24)

Ransomware fears cause companies to hoard Bitcoin

National Cyber Security Centre
a part of GCHQ

Companies are reportedly stockpiling cryptocurrencies to hedge against the possible need to pay off cyber criminals.

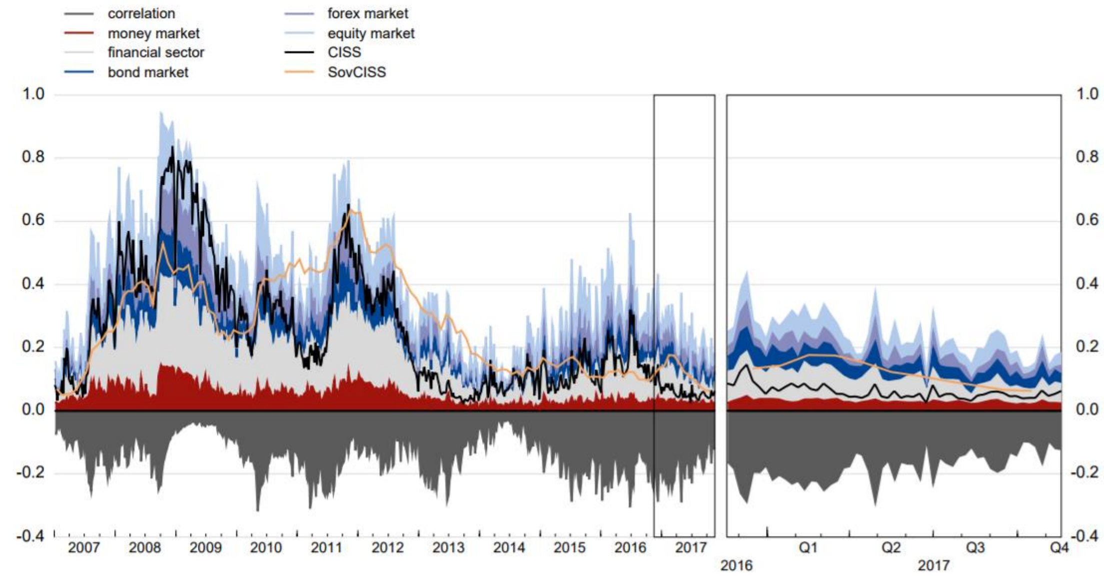
Some firms are said to be investing in Bitcoin and Ethereum to ensure that they have cryptocurrency funds available if they are affected by a ransomware attack.

Number 5 (Page 25)

ESRB risk dashboard

ESRB
European Systemic Risk Board
European System of Financial Supervision

1.1 Composite indicator of systemic stress
(Last observation: 17 Nov. 2017)



Sources: Thomson Reuters, ECB and ECB calculations.
Notes: The CISS is unit-free and constrained to lie within the interval (0, 1). See Hollo, D., Kremer, M. and Lo Duca, M., "CISS - a composite indicator of systemic stress in the financial system", Working Paper Series, No 1426, ECB, March 2012. The Sovereign CISS applies the same methodological concept of the CISS.

Number 6 (Page 27)

The Ten Most Popular DARPA Stories of 2017

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

DARPA's pivotal investments in breakthrough technologies and capabilities for national security take place in about 250 possibility-redefining programs across dozens of fields.

Number 1

Configuration Security Program to Make Network-Connected Systems Less Vulnerable

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

The rise of network-connected systems that are becoming embedded seemingly everywhere–from industrial control systems to aircraft avionics–is opening up a host of rich technical capabilities in deployed systems.

Even so, as the collective technology project underlying this massive deployment of connectivity unfolds, more consumer, industrial, and military players are turning to inexpensive, commodity off-the-shelf (COTS) devices with general-purpose designs applicable for a range of functionalities and deployment options. While less costly and more flexible, commodity components are inherently less secure than the single-purpose, custom devices they are replacing.

“With commodity devices, software and configuration settings now govern behaviors that were physically impossible in special-purpose hardware, creating security risks and increasing system vulnerability,” said Jacob Torrey, program manager in DARPA’s Information Innovation Office (I2O).

“Certain functionality built into COTS components may not be necessary for all users or applications, and unwanted functionality can be hard to detect and turned-off. For instance, an unneeded maintenance or diagnostic service left enabled could create an opportunity for an attacker to circumvent other security controls and use the system’s as-deployed functionality to generate a malicious effect.

This opaqueness is creating challenges for system operators who must rely on component configurations to reduce attack surfaces created by unnecessary functionality.”

To address the challenges created by the proliferation of COTS devices and help harden the security surface of network-connected composed systems, DARPA has launched a new program called Configuration Security (ConSec).

The program, just announced today, aims to develop a system to automatically generate, deploy, and manage inherently more secure configurations of components and subsystems for use in military platforms.

"Through ConSec we hope to gain a better understanding of the available functionality across COTS devices and what's needed for the task at hand and then use system configurations to create the functionality that's actually required while minimizing the excess that can be used as an attack surface," said Torrey.

"While our objective is to build this capability for military platforms, there is the potential for the program to have broader applications for commercial and industrial systems as well."

Prospective performers are tasked with finding ways to automate the traditionally more manual process of system configuration. To tackle this feat, the program is divided into two technical areas.

The first area focuses on reducing the amount of human-in-the-loop time required to understand what capabilities a system needs to deliver across different operating environments, the functionality required to achieve its mission in each operating environment, and the possible component configurations needed to create the desired functionality.

"Consider, for example, a naval vessel. Its functionality when at sea is likely different than what's required of it while at port, or in dry-dock undergoing maintenance," said Torrey. "Our aim is to automate the process of identifying these different operating environments, the system's expected functionality in each scenario, and the components needed to make it all happen, which is currently a manual, labor intensive process."

To accomplish this, DARPA is asking researchers to develop models and functional specifications of systems based on human-friendly information formats–such as checklists, operating manuals, and other written human standard operating procedures (SOPs)–as well as an analysis of the system's underlying components' hardware and firmware.

Input from these analyses should help determine how settings in a component's configuration space might impact its functionality, how the behavior of human operators impacts system behavior, and what operational and mission contexts pertain for the full, composed system.

The ConSec program's second technical area focuses on uncovering component configurations that will enable the composed system to achieve its mission under different, relevant operational contexts.

Here proposers are asked to leverage the models and functional specifications that emerge from work in the first technical area to find ways of identifying secure configurations that eliminate unused and unnecessary functionality as a way to shrink the system's vulnerabilities to attack.

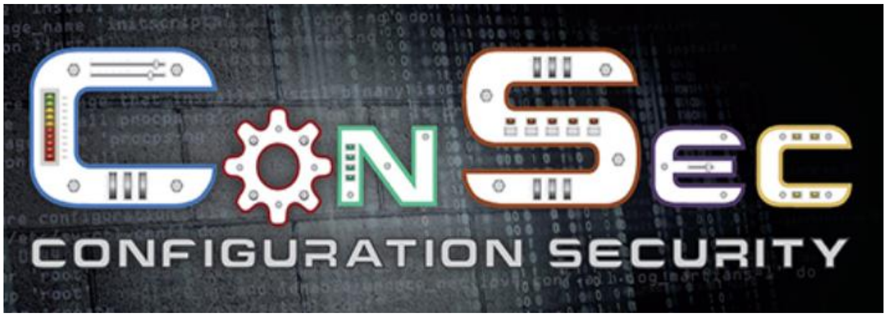
"Essentially we're asking potential performers to determine how to take all of the best pieces and functionality and combine them to fulfill the requirements of a high-level composed system while turning off all of the things we don't need," said Torrey.

Torrey expects that the program will roll out in three phases over the next three-and-a-half years.

The deadline for proposals for the ConSec program is February 8, 2018.

Additional details about the program can be found via the DARPA Broad Agency Announcement, found at:

https://www.fbo.gov/index?s=opportunity&mode=form&id=c889999b044a8b485da8884d7fbab391&tab=core&_cview=1



Number 2

Raising Our Game: Cyber Security in an Age of Digital Transformation

Christopher Wray, Director, Federal Bureau of Investigation.
Fordham University - FBI International Conference on Cyber Security, New York City, New York

Good morning. It's great to be here with you, and great to be back here in my hometown. Thank you all for joining us. I want to thank Father McShane and Fordham for continuing to help us bring people together to focus on cyber security.

Let me start by saying how honored I feel to be here representing the men and women of the FBI. The almost 37,000 agents, analysts, and staff I get to work with at Headquarters, in our field offices, and around the world are an extraordinary, dedicated, and quite frankly, inspiring bunch.

Not a day goes by that I'm not struck by countless examples of their patriotism, courage, professionalism, and integrity. And I could not be more proud, but also humbled, to stand with them as we face the formidable challenges of today—and tomorrow.

The work of the FBI is complex and hits upon nearly every threat facing our country. Today, I'd like to focus on the cyber threat.

Most of you have been thinking about the challenges in this particular arena for a long time. Before taking this job a few months ago, the last time I had to think seriously about cyber security through a law enforcement or national security lens was 12 years ago.

Back then, I was head of the Justice Department's Criminal Division, which included the Computer Crimes and Intellectual Property Section and handled cyber investigations.

It’s safe to say that no area has evolved more dramatically since then, particularly given the blistering pace of technological change. And I’ve spent much of the past few months getting caught up on all things cyber. So maybe the most useful thing I can do today is to offer the viewpoint of someone who’s looking at this world with fresh eyes.

I’d like to talk to you about what the cyber threat picture looks like today; what the FBI is doing about it; and most important of all, what’s the way forward? Where’s the threat going? And where do we need to be to meet that threat? And then if we have time, I hope to answer a few questions.

The cyber threat has evolved dramatically since I left DOJ in 2005. Back then, social media didn’t really exist as we know it today, and “tweeting” was something only birds did.

Now…well, let’s just say it’s something that’s a little more on my radar. Today, we live much of our lives online, and everything that’s important to us lives on the Internet—and that’s a scary thought for a lot of people. What was once a minor threat—people hacking for fun or for bragging rights—has turned into full-blown economic espionage and lucrative cyber crime.

This threat now comes at us from all sides. We’re worried about a range of threat actors, from multi-national cyber syndicates and insider threats to hacktivists. We’re seeing an increase in nation-state sponsored computer intrusions. And we’re also seeing a “blended threat”—nation-states using criminal hackers to carry out their dirty work. We’re also concerned about a wide gamut of methods, from botnets to ransomware.

So what’s the FBI doing about the cyber threat? Realistically, we know we can’t prevent every attack, or punish every hacker. But we can build on our capabilities. We can strengthen our partnerships and our defenses. We can get better at exchanging information to identify the telltale signs that may help us link cyber criminals to their crimes. We can impose a variety of costs on criminals who think they can hide in the shadows of cyber space.

We can do all these things—and we are doing all these things.

We’re improving the way we do business, blending traditional investigative techniques with technical capabilities. We’re now assigning work based on cyber experience and ability, rather than on jurisdiction. We now have Cyber Action Teams of agents and experts who can deploy at a moment’s notice, much like our Counterterrorism Fly Teams. We also now have Cyber Task Forces in every field office—much like our Joint Terrorism Task

Forces—that respond to breaches, conduct victim-based investigations, and collect malware signatures and other actionable intelligence.

So we've strengthened our investigative capabilities, but we need to do our best to actually lay hands on the culprits and lock them up. And even where we can't reach them, we're now using all the tools at our disposal—we're "naming and shaming" them with indictments, and we're seeking sanctions from the Treasury Department.

We're also building on our partnerships. We're working more closely with our federal partners, because this threat is moving so quickly that there's no time for turf battles. It doesn't matter if you call us, or DHS, or any other agency—we all work together, so your information will get where it needs to go and you'll get the help you need. We care less about who you call than that you call, and that you call as promptly as possible.

We're also working more closely with our foreign partners. We now have cyber agents embedded with our international counterparts in strategic locations worldwide, helping to build relationships and coordinate investigations.

We're also trying to work better with our private sector partners. We're sharing indicators of compromise, tactics cyber criminals are using, and strategic threat information whenever we can. I'm sure you can appreciate there are times when we can't share as much as we'd like to, but we're trying to get better and smarter about that.

The good news is, we've made progress on a number of important fronts. Just this past summer, we took down AlphaBay—the largest marketplace on the DarkNet. Hundreds of thousands of criminals were anonymously buying and selling drugs, weapons, malware, stolen identities, and all sorts of other illegal goods and services through AlphaBay.

We worked with the DEA, the IRS, and Europol, and with partners around the globe, to dismantle the illicit business completely. But we were strategic about the takedown—we didn't want to rush it and lose these criminals. So, we waited patiently and we watched.

When we struck, AlphaBay's users flocked to another DarkNet marketplace, Hansa Market, in droves—right into the hands of our Dutch law enforcement partners who were there waiting for them, and they shut down that site, too.

So we're adapting our strategy to be more nimble and effective. But the bad news is, the criminals do that too.

I mentioned the "blended threat" earlier. Recently we had the Yahoo matter, where hackers stole information from more than 500 million Yahoo users. In response, last February we indicted two Russian Federal Security Service officers and two well-known criminal hackers who were working for them. That's the "blended threat"—you have intelligence operatives from nation-states like Russia now using mercenaries to carry out their crimes.

In March, our partners in the Royal Canadian Mounted Police arrested one of the hackers in Canada. The other three are Russian citizens living in Russia, but we made the judgment that it was worth calling them out, so now they're also fugitives wanted by the FBI—so their vacation destinations are more limited.

So we're making strides and we've had a number of successes—but the FBI still needs to do more to adapt to meet the cyber challenge.

For example, we want to do more to mitigate emerging threats as they spread. While we may not be able to stop all threats before they begin, we can do more at the beginning to stop threats before they get worse. We can share information, identify signatures, and stop similar attacks from happening elsewhere. But to do that, we need the private sector to work with us.

At the FBI, we treat victim companies as victims. So, please: When an intrusion affects critical infrastructure; when there's a potential for impact to national security, economic security, or public health and safety; when an attack results in a significant loss of data, systems, or control of systems; or when there are indications of unauthorized access to—or malware present on—critical IT systems, call us. Because we want to help you, and our focus will be on doing everything we can to help you.

Another thing driving the FBI's work is that at some point, we'll have to stop referring to all technical and digital challenges as "cyber." Sophisticated intrusions and cyber policy issues are very much at the forefront of the conversation. But we also have to recognize that there's a technology and digital component to almost every case we have now.

Transnational crime groups, sexual predators, fraudsters, and terrorists are transforming the way they do business as technology evolves. Significant pieces of these crimes—and our investigations of them—have a digital component or occur almost entirely online. And new technical trends are making the investigative environment a lot more complex. The Internet of Things, for example, has led to phenomena like the Mirai botnet—malware that uses all these connected devices to overwhelm websites, like the attacks that took down Netflix and Twitter last year.

The digital environment also presents new challenges that the FBI has to address—all kinds of twists for us in terms of what's coming down the pike. Advances like artificial intelligence or crypto currencies have implications not only for the commercial sector, but for national security.

Encrypted communications are changing the way criminals and terrorists plan their crimes—I'll have more to say on that in a moment. And the avalanche of data created by our use of technology presents a huge challenge for every organization.

I'm convinced that the FBI—like a lot of other organizations—hasn't fully gotten our arms around these new technologies and their implications for our national security and cyber security work. On our end, we know we need to be working with the private sector to get a clearer understanding of what's coming around the bend.

We need to put our heads together, in conferences like this and in other ways, so we're better prepared, not just to face current threats, but the threats that will come at us five, 10, and 15 years from now.

When I was last in government, I saw how the 9/11 attacks spurred the FBI to fundamentally transform itself into a more intelligence-based national security organization. In the same way, I believe the new digital environment demands further fundamental transformation from us.

Over the years, FBI investigators have made huge strides in responding to the investigative challenges posed by the digital realm. We have pockets of excellence and talent that we've relied on to tackle our most complex technical challenges. But with the wholesale rise of digital challenges, this model won't work for us anymore.

As a big organization spread across 56 field offices and over 80 international offices, we need a new approach. We've got to increase our digital literacy across the board.

Some of our smartest people are looking at these challenges and thinking strategically about how the entire FBI can evolve in this rapidly changing environment. We're focused on building our digital capabilities. We're also focusing on our people, making sure we continue to attract the right skills and talent—and develop the right talent internally.

One issue I'm fixated on is whether we're recruiting, hiring, and training now the kind of tech-savvy people we'll need in five or 10 years. We know that we need more cyber and digital literacy in every program throughout the Bureau—organized crime, crimes against children, white-collar crime, just to name a few.

Raising the average digital proficiency across the organization will allow all of our investigators to counter threats more efficiently and effectively, while freeing our true cyber "black belts" to focus on the most vexing attacks, like nation-state cyber intrusions.

We also need to focus more on innovation, approaching problems in new ways, with new ideas—which isn't something, to be honest, that always comes naturally in government. We can't just rely on the way we've always done things.

And I don't mean just technological innovation; I mean innovation in how we approach challenges, innovation in partnerships, innovation in who we hire, innovation in how we train, and innovation in how we build our workforce for the future.

So we need more innovation, and more of the right people. But the FBI can't navigate the digital landscape alone. We also need to build stronger partnerships—with our counterparts in federal agencies, with our international counterparts, with the cyber research community, and with the private sector.

And we need to do a better job of focusing our combined resources—trying to get our two together with your two to have it somehow equal more than four; to make it five or six or seven.

Finally, in some cases we may need lawmakers to update our laws to keep pace with technology. In some ways, it's as if we still had traffic laws that were written for the days of the horse-and-carriage.

The digital environment means we don't simply need improved technical tools; we also need legal clarifications to address gaps.

I want to wrap up by talking about two challenges connected to the digital revolution.

The first is what we call the "Going Dark" problem. This challenge grows larger and more complex every day. Needless to say, we face an enormous and increasing number of cases that rely on electronic evidence. We also face a situation where we're increasingly unable to access that evidence, despite lawful authority to do so.

Let me give you some numbers to put some meat on the bones of this problem. In fiscal year 2017, we were unable to access the content of 7,775 devices—using appropriate and available technical tools—even though we had the legal authority to do so. Each one of those nearly 7,800 devices is tied to a specific subject, a specific defendant, a specific victim, a specific threat.

I spoke to a group of chief information security officers recently, and someone asked about that number. They basically said, "What's the big deal? There are millions of devices out there." But we're not interested in the millions of devices used by everyday citizens. We're only interested in those devices that have been used to plan or execute criminal or terrorist activities.

Some have argued that having access to the content of communications isn't necessary—that we have a great deal of other information available outside of our smart phones and our devices; information including transactional information for calls and text messages, or metadata. While there's a certain amount we can glean from that, for purposes of prosecuting terrorists and criminals, words can be evidence, while mere association between subjects isn't evidence.

Being unable to access nearly 7,800 devices is a major public safety issue. That's more than half of all the devices we attempted to access in that timeframe—and that's just at the FBI. That's not even counting a lot of devices sought by other law enforcement agencies—our state, local, and foreign counterparts. It also doesn't count important situations outside of accessing a specific device, like when terrorists, spies, and criminals use encrypted messaging apps to communicate.

This problem impacts our investigations across the board—human trafficking, counterterrorism, counterintelligence, gangs, organized crime, child exploitation, and cyber. And this issue comes up in almost every conversation I have with leading law enforcement organizations, and with my foreign counterparts from most countries—and typically in the first 30 minutes.

Let me be clear: The FBI supports information security measures, including strong encryption. But information security programs need to be thoughtfully designed so they don't undermine the lawful tools we need to keep this country safe.

While the FBI and law enforcement happen to be on the front lines of this problem, this is an urgent public safety issue for all of us. Because as horrifying as 7,800 in one year sounds, it's going to be a lot worse in just a couple of years if we don't find a responsible solution.

The solution, I'll admit, isn't so clear-cut. It will require a thoughtful and sensible approach, and may vary across business models and technologies, but—and I can't stress this enough—we need to work fast.

We have a whole bunch of folks at FBI Headquarters devoted to explaining this challenge and working with stakeholders to find a way forward. But we need and want the private sector's help. We need them to respond to lawfully issued court orders, in a way that is consistent with both the rule of law and strong cybersecurity. We need to have both, and can have both.

I recognize this entails varying degrees of innovation by the industry to ensure lawful access is available. But I just don't buy the claim that it's impossible.

For one thing, many of us in this room use cloud-based services. You're able to safely and securely access your e-mail, your files, and your music on your home computer, on your smartphone, or at an Internet café in Tokyo. In fact, if you buy a smartphone today, and a tablet in a year, you're still able to securely sync them and access your data on either device.

That didn't happen by accident. It's only possible because tech companies took seriously the real need for both flexible customer access to data and cyber security. We at the Bureau are simply asking that law enforcement's lawful need to access data be taken just as seriously.

Let me share just one example of how we might strike this balance. Some of you might know about the chat and messaging platform called Symphony, used by a group of major banks. It was marketed as offering "guaranteed data deletion," among other things. That didn't sit too well with the regulator for four of these banks, the New York State Department of Financial Services. DFS was concerned that this feature could be used to hamper regulatory investigations on Wall Street.

In response to those concerns, the four banks reached an agreement with the Department to help ensure responsible use of Symphony. They agreed to keep a copy of all e-communications sent to or from them through Symphony for seven years. The banks also agreed to store duplicate copies of the decryption keys for their messages with independent custodians who aren't controlled by the banks. So the data in Symphony was still secure and encrypted—but also accessible to regulators, so they could do their jobs.

I'm confident that with a similar commitment to working together, we can find solutions to the Going Dark problem. After all, America leads the world in innovation. We have the brightest minds doing and creating fantastic things. If we can develop driverless cars that safely give the blind and disabled the independence to transport themselves; if we can establish entire computer-generated virtual worlds to safely take entertainment and education to the next level, surely we should be able to design devices that both provide data security and permit lawful access with a court order.

We're not looking for a "back door"—which I understand to mean some type of secret, insecure means of access. What we're asking for is the ability to access the device once we've obtained a warrant from an independent judge, who has said we have probable cause.

We need to work together—the government and the technology sector—to find a way forward, quickly.

In other parts of the world, American industry is encountering requirements for access to data—without any due process—from governments that operate a little differently than ours, to put it diplomatically.

It strikes me as odd that American technology providers would grant broad access to user data to foreign governments that may lack all sorts of fundamental process and rule of law protections—while at the same time denying access to specific user data in countries like ours, where law enforcement obtains warrants and court orders signed by independent judges.

I just cannot believe that any of us in this room thinks that paradox is the right way to go. That's no way to run a railroad, as the old saying goes.

A responsible solution will incorporate the best of two great American traditions—the rule of law and innovation. But for this to work, the private sector needs to recognize that it's part of the solution. We need them to come to the table with an idea of trying to find a solution, as opposed to trying to find a way to build systems to prevent a solution.

I'm open to all kinds of ideas, because I reject this notion that there could be such a place that no matter what kind of lawful authority you have, it's utterly beyond reach to protect innocent citizens. I also can't accept that anyone out there reasonably thinks the state of play as it exists now—and the direction it's going—is acceptable.

Finally, let me briefly mention another issue that has a huge effect on the FBI's national security work, including cyber—the re-authorization of Section 702 of the Foreign Intelligence Surveillance Act, or FISA.

The speed and scope of the cyber threat demands that we use every lawful, constitutional tool we've got to fight it. Section 702 is one of those tools.

I want to stress once again how vital this program is for the FBI's national security mission. Section 702 is an essential foreign intelligence authority that permits the targeted surveillance of non-U.S. persons overseas. It's especially valuable to the FBI, because it gives us the agility we need to stay ahead of today's rapidly changing global threats.

I bring all this up today because unless renewed by Congress, Section 702 is set to expire later this month. Without 702, we would open ourselves up to intelligence gaps that would make it easier for bad cyber actors and terrorists to attack us and our allies—and make it harder for us to detect these threats.

We simply can't afford for that to happen. So the FBI has spent an enormous amount of time, as have our partners in the intelligence community, working together with Congress to find a way to re-authorize Section 702 while addressing their concerns.

My fervent hope is that before the extension expires, Congress will re-authorize Section 702 in a manner that doesn't significantly affect our operational use of the program, or endanger the security of the American people.

So that's a perspective on cyber from the new guy back on the block.

If one thing's become clear to me after immersing myself again in this world for the past few months, it's the urgency of the task we all face. High-impact intrusions are becoming more common; the threats are growing more complex; and the stakes are higher than ever.

That requires all of us to raise our game—whether we're in law enforcement, in government, in the private sector or the tech industry, in the security field, or in academia. We need to work together to stay ahead of the threat and to adapt to changing technologies and their consequences—both expected and unexpected. Because at the end of the day, we all want the same thing: To protect our innovation, our systems, and, above all, our people.

Thank you all for everything you're doing to make the digital world safer and more secure, and for joining us here in New York. I look forward to working with you in the years to come.

Now I'd be happy to take a few questions.

Number 3

Increase in HTTPS phishing attacks

National Cyber
Security Centre
a part of GCHQ

Over the past few years website owners have been encouraged to adopt HTTPS website domains rather than HTTP. With HTTPS, data in transit is encrypted; this provides additional security for transiting data, such as login credentials, which may contain information of use to attackers.

HTTPS domains are verified by SSL Certificate Authorities, who issue and authenticate certificates. The padlock symbol in the URL field links to the certificate provider's website, and users are often advised to trust webpages with this symbol.

However, while the padlock shows that encryption is used, it does not guarantee the legitimacy of the website. It is possible for attackers to compromise sites using HTTPS domains and use them to host malicious links. It is also easy for attackers to obtain legitimate certificates (often for free) and use them to set up their own malicious website.

Although this rising attack trend has been previously reported, recent research by cyber security company PhishLabs highlights a common misconception amongst average internet users, that websites using SSL and HTTPS, as signified by the padlock, are safe and secure to use.

This is not necessarily the case and attackers have increasingly exploited this misunderstanding. In the third quarter of 2017, PhishLabs found that nearly a quarter of all phishing attacks observed were hosted on HTTPS domains.

To avoid becoming a victim of HTTPS phishing attacks, users and organisations should not rely on a padlock or link to an SSL certificate alone to verify the legitimacy of a website.

Other methods include paying close attention to the URL spelling and comparing it to a known and trusted version, and looking at the email source code to find the real name of a website or its IP address.

The NCSC provides guidance to help companies and individuals know what to worry about when using HTTPS to protect data. You may visit:
https://www.ncsc.gov.uk/guidance/tls-external-facing-services

Number 4

Ransomware fears cause companies to hoard Bitcoin

National Cyber Security Centre
a part of GCHQ

Companies are reportedly stockpiling cryptocurrencies to hedge against the possible need to pay off cyber criminals.

Some firms are said to be investing in Bitcoin and Ethereum to ensure that they have cryptocurrency funds available if they are affected by a ransomware attack.

A survey carried out earlier this year by Citrix found that 42% of companies surveyed were building cryptocurrency stockpiles for ransomware payments, with 28% holding more than 30 bitcoins.

The cost of paying ransoms is increasing rapidly along with the value of the cryptocurrencies in which they are paid, so by investing now, some companies hope to ensure that the cost of a ransom is less pricey than it might be later.

However, this approach comes with its own risks, as such holdings may themselves be targeted. With a single bitcoin now worth over $17,000 (£12,000), a company's cryptocurrency wallet can be worth a substantial amount to a cyber criminal.

The NCSC's website provides further advice to organisations that may be affected by ransomware. The NCSC does not offer advice on whether or not companies should invest in Bitcoin. While it is a matter for the victim whether or not to pay a ransom, the National Crime Agency encourages industry and the public not to do so.

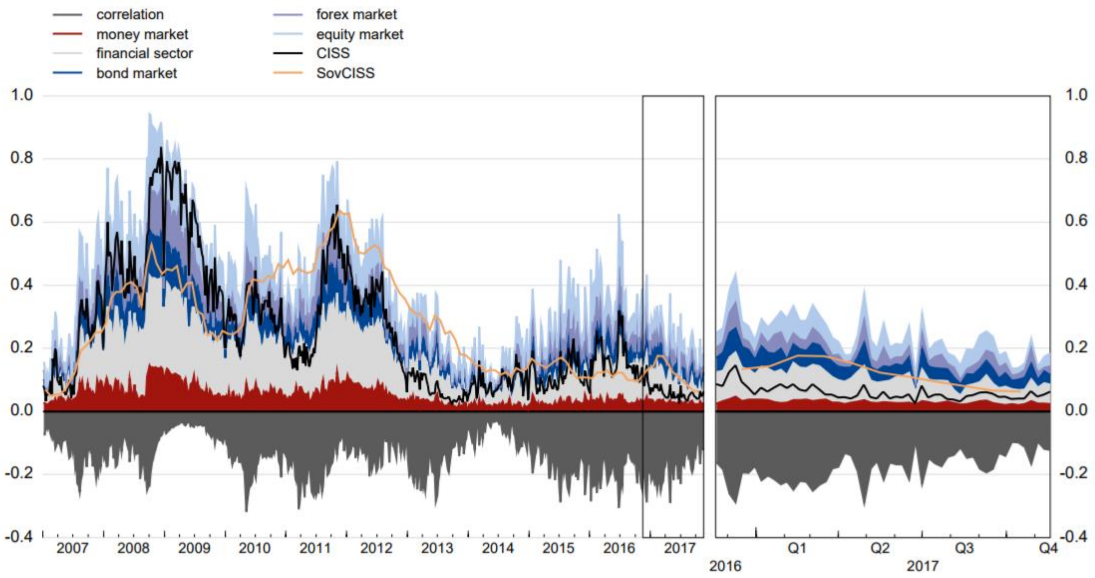
You may visit:
https://www.ncsc.gov.uk/guidance/protecting-your-organisation-ransomware

Number 5

ESRB risk dashboard

ESRB
European Systemic Risk Board
European System of Financial Supervision

1.1 Composite indicator of systemic stress
(Last observation: 17 Nov. 2017)



Sources: Thomson Reuters, ECB and ECB calculations.

Notes: The CISS is unit-free and constrained to lie within the interval (0, 1). See Hollo, D., Kremer, M. and Lo Duca, M., "CISS - a composite indicator of systemic stress in the financial system", Working Paper Series, No 1426, ECB, March 2012. The Sovereign CISS applies the same methodological concept of the CISS.

The ESRB risk dashboard is a set of quantitative and qualitative indicators of systemic risk in the EU financial system.

The composition and the presentation of the ESRB risk dashboard have been reviewed in the first quarter of 2017.

Unless otherwise indicated:

a) all EU indicators relate to the 28 Member States of the EU (the EU28).

b) all data series relate to the Euro 19 (i.e. the euro area) for the whole time series.

For statistics based on the balance sheet of the MFI sector, as well as statistics on financial markets and interest rates, the series relate to the composition of the EU/euro area in the period covered (changing composition).

Statistics based on the balance sheet of the MFI sector are unconsolidated.

To read it:
https://www.esrb.europa.eu/pub/pdf/dashboard/esrb.risk_dashboard171220_22.en.pdf?cd83d22fbe20c78eeefa20bf0954eb28

Number 6

The Ten Most Popular DARPA Stories of 2017

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

DARPA's pivotal investments in breakthrough technologies and capabilities for national security take place in about 250 possibility-redefining programs across dozens of fields, from quantum metamaterials and machine learning to neurotechnology and unmanned system autonomy.

Throughout the year, the Agency produces updates about newly launched efforts, promising results, and major program accomplishments. We post them all on the DARPA news page, which in 2017 received 35 million page views—a 30 percent increase over last year.

The end of the year is the perfect opportunity for the many communities that follow DARPA to revisit favorite articles and discover new ones—so we've compiled a countdown of the year's ten most popular updates to DARPA's news page, based on visits:

10. Removing the Viral Threat: Two Months to Stop Pandemic X from Taking Hold (February 6, 2017).
DARPA is launching the Pandemic Prevention Platform (P3) program, aimed at developing foundational work into an entire system capable of halting the spread of any viral disease outbreak before it can escalate to pandemic status.

Such a capability would offer a stark contrast to the state of the art for developing and deploying traditional vaccines—a process that does not deliver treatments to patients until months, years, or even decades after a viral threat emerges.

You may visit:
https://www.darpa.mil/news-events/2017-02-06a

9. Sharing Battlefield Information at Multiple Classification Levels via Mobile Handheld Devices (January 10, 2017).

DARPA today announced its Secure Handhelds on Assured Resilient networks at the tactical Edge (SHARE) program. SHARE aims to create a system where information at multiple levels of security classification could be processed on a single handheld device using a resilient secure network that links devices without needing to route traffic through secure data centers.

This capability would be able to operate over existing commercial and military networks while maintaining the security of sensitive information and safety of operations.

You may visit:
https://www.darpa.mil/news-events/2017-01-10

8. Toward Machines that Improve with Experience (March 16, 2017).

DARPA's new Lifelong Learning Machines (L2M) program aims to develop next-generation machine learning technologies that can learn from new situations and apply that learning to become better and more reliable, while remaining constrained within a predetermined set of limits that the system cannot override.

Such a capability for automatic and ongoing learning could, for example, help driverless vehicles become safer as they apply knowledge gained from previous experiences—including the accidents, blind spots, and vulnerabilities they encounter on roadways—to circumstances they weren't specifically programmed or trained for.

You may visit:
https://www.darpa.mil/news-events/2016-06-17

7. Smart Quadcopters Find their Way without Human Help or GPS (June 28, 2017).

Phase 1 of DARPA's Fast Lightweight Autonomy (FLA) program concluded recently following a series of obstacle-course flight tests in central Florida.

Over four days, three teams of DARPA-supported researchers huddled under shade tents in the sweltering Florida sun, fine-tuning their sensor-laden quadcopter unmanned aerial vehicles (UAVs) during the intervals between increasingly difficult runs.

DARPA's FLA program is advancing technology to enable small unmanned quadcopters to fly autonomously through cluttered buildings and obstacle-strewn environments at fast speeds (up to 20 meters per second, or 45 mph) using onboard cameras and sensors as "eyes" and smart algorithms to self-navigate.

You may visit:
https://www.darpa.mil/news-events/2017-06-28

6. Radioactive Threat Detection System Completes Emergency Vehicle Test Deployment in Nation's Capital (March 1, 2017).

DARPA's SIGMA program—whose goal is to prevent attacks involving radiological "dirty bombs" and other nuclear threats—concluded its biggest and longest test deployment of vehicle-mounted radiation detectors in Washington, D.C., in February.

For approximately seven months starting in July 2016, the fleet of D.C. Fire and Emergency Medical Services ambulances was outfitted with DARPA-developed nuclear and radiological detectors, providing the first city-scale, dynamic, real-time map of background radiation levels throughout the Capital as well as identifying any unusual spikes that could indicate a threat.

You may visit:
https://www.darpa.mil/news-events/2017-03-01

5. RadioBio: What role does electromagnetic signaling have in biological systems? (February 7, 2017).

DARPA's RadioBio program, announced today, seeks to establish if purposeful electromagnetic wave signaling between biological cells exists—and if evidence supports that it does, to determine what information is being transferred.

The validity of existing and new electromagnetic biosignaling claims requires an understanding of how the structure and function of microscopic, natural antennas are capable of generating and receiving information in a noisy spectral environment.

You may visit:
https://www.darpa.mil/news-events/2017-02-07

4. SideArm Prototype Catches Full-Size Unmanned Aerial System Flying at Full Speed (February 6, 2017).

Few scenes capture the U.S. Navy's prowess as effectively as the rapid-fire takeoff and recovery of combat jets from the deck of an aircraft carrier.

The ability to carry air power anywhere in the world, and both launch those aircraft to flight speed and bring them to a stop over extremely short distances, has been essential to carriers' decades-long dominance of naval warfare.

To help provide similar capabilities—minus the 90,000-ton carriers—to U.S. military units around the world, DARPA's SideArm research effort seeks to create a self-contained, portable apparatus able to horizontally launch and retrieve unmanned aerial systems (UASs) of up to 900 pounds.

You may visit:
https://www.darpa.mil/news-events/2017-02-06

3. TNT Researchers Set Out to Advance Pace and Effectiveness of Cognitive Skills Training (April 26, 2017).

In March 2016, DARPA announced the Targeted Neuroplasticity Training (TNT) program, an effort to enlist the body's peripheral nervous system to achieve something that has long been considered the brain's domain alone: facilitation of learning. Work on TNT has now begun.

The crux of the wide-ranging program is to identify optimal and safe neurostimulation methods for activating "synaptic plasticity"—a natural process in the brain, pivotal to learning, that involves the strengthening or weakening of the junctions between two neurons—then build those methods into enhanced training regimens that accelerate the acquisition of cognitive skills.

You may visit:
https://www.darpa.mil/news-events/2017-04-26

2. Service Academies Swarm Challenge Live-Fly Competition Begins (April 23, 2017).

To help make effective swarm tactics a reality, DARPA created the Service Academies Swarm Challenge, a collaboration between the Agency and the three U.S. military Service academies—the U.S. Military Academy, the U.S.

Naval Academy, and the U.S. Air Force Academy. An experiment at its heart, the research effort is designed to encourage students to develop innovative offensive and defensive tactics for swarms of small unmanned aerial vehicles (UAVs).

Today the effort started its three-day Live-Fly Competition at Camp Roberts, a California Army National Guard post north of Paso Robles, Calif., which is hosting more than 40 Cadets and Midshipmen to demonstrate the highly autonomous swarm tactics they have developed since work started in September.

You may visit:
https://www.darpa.mil/news-events/2017-04-23

1. DARPA Picks Design for Next-Generation Spaceplane (May 24, 2017).

DARPA has selected The Boeing Company to complete advanced design work for the Agency's Experimental Spaceplane (XS-1) program, which aims to build and fly the first of an entirely new class of hypersonic aircraft that would bolster national security by providing short-notice, low-cost access to space.

The program aims to achieve a capability well out of reach today—launches to low Earth orbit in days, as compared to the months or years of preparation currently needed to get a single satellite on orbit.

You may visit:
https://www.darpa.mil/news-events/2017-05-24

Disclaimer

Cyber Risk GmbH enhances public access to information about cyber risk and compliance in Switzerland.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any individual or entity;

- should not be relied on in the particular context of enforcement or similar regulatory action;

- is not necessarily comprehensive, complete, or up to date;

- is sometimes linked to external sites over which Cyber Risk GmbH has no control and for which Cyber Risk GmbH assumes no responsibility;

- is not professional or legal advice;

- is in no way constitutive of an interpretative document;

- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;

- does not prejudge the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts.

It is our goal to minimize disruption caused by technical errors. However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.