Christopher Wray
Director
Federal Bureau of Investigation

Boston College/FBI - Boston Conference on Cyber Security
Boston, Massachusetts
March 7, 2018

Digital Transformation: Using Innovation to Combat the Cyber Threat

Remarks prepared for delivery.

Good morning, it's great to be here. I want to thank Father Burns, Provost Quigley, and Boston College for coordinating this conference. Let me start by saying how honored I feel to be here representing the 37,000 men and women of the FBI.

As I make my way around our 56 field offices, our Headquarters divisions, and our Legat offices around the world, I encounter example after example of selfless, relentlessly hard-working, honest, brave and professional folks. Patriots. And I couldn't be more proud or inspired, but at the same time pretty humbled, to stand with them as we face the formidable challenges of today—and tomorrow.

The work of the FBI, to put it mildly, is complex and covers just about every threat we face. This morning, of course, I'm focused primarily on the cyber threat. Many of you have been thinking about the threats in this particular arena for a long time. Before taking this job, the last time I had to think seriously about cyber security through a law enforcement and national security perspective was 13 years ago. Back then, I was head of the Justice Department's Criminal Division, which included the Computer Crimes and Intellectual Property Section, overseeing cyber investigations. It's fair to say that no area has evolved more dramatically since then, given the breathtaking and blistering pace of technological change. And I've tried over the past six months to start catching 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 importantly, what's the way forward? Where's the threat going? And where do we need to be to meet that threat?

How Things Have Changed

The cyber threat has evolved dramatically since I left DOJ in 2005, partly just reflecting how much the digital world has itself evolved over that time. Back then, "tweeting" was something only birds did. I've noticed it's a bit more popular now. 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 comparatively minor threat—people hacking for fun or for bragging rights—has turned into full-blown economic espionage and extremely lucrative cyber crime.

This threat is now coming at us from all sides. We're worried—at the FBI and with our partners—about a wider range of threat actors, from multi-national cyber syndicates and insider threats to hacktivists. And we're concerned about a wider gamut of methods, from botnets to ransomware, from spearfishing and business e-mail compromise to illicit crypto mining and APTs. We're seeing an increase in nation-state sponsored computer intrusions, like last year's massive WannaCry ransomware attack, recently attributed to North Korea, and NotPetya—the most destructive and costly cyber attack in history. Launched by the Russian military, NotPetya resulted in billions of dollars in damage across Europe, Asia, and the Americas.

We've also begun seeing a "blended threat"—nation-states using criminal hackers to do their dirty work. Nation-state actors are also turning to more creative avenues to steal information. They are no longer dependent on just intelligence services to carry out their aims. Instead, they utilize people from all walks of life—hackers, businesspeople, academics, researchers, diplomats, tourists, and anyone else who can get their hands on something of value.

We at the FBI are in the business of protecting vital assets, whether those are government state secrets or corporate trade secrets, and we look forward to working with folks like you to help protect your crown jewels.

What Are We Doing About Cyber?

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. And we can impose a variety of costs on criminals who think they can hide in the shadows of cyber space. We can do these things—and we are.

We're improving the way we do business and blending traditional investigative techniques with technical capabilities. We're assigning work based on cyber experience and ability, rather than jurisdiction. We have white-hat Cyber Action Teams of highly skilled agents and experts who can deploy at a moment's notice, much like our Counterterrorism Fly Teams. We have Cyber Task Forces in every field office that respond to breaches, conduct victim-based investigations, and collect malware signatures and other actionable intelligence—much like our highly successful Joint Terrorism Task Forces.

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. We're embedding non-cyber agents with cyber squads, so they too can learn how to conduct cyber investigations. We're sending non-cyber personnel to cutting-edge cyber training. We're also bringing intelligence analysts from the field to Headquarters to get more tactical cyber experience. And we're boosting our training for our most cyber-savvy agents, offering interactive, boot camp-type classes to walk agents through simulated cyber investigations—including computer intrusions and phishing schemes.

Raising the average 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. 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,10, or 15 years. We need to not only recruit better from the outside; we need to bolster our training inside the Bureau to give more of our agents and analysts the skill set and experience they need to work cyber cases.

We’ve strengthened our investigative capabilities, but we need to keep doing better 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 going after their criminal infrastructure and we’re seizing their assets.

We’re also building on our partnerships. One of the things that’s jumped out at me coming back to the Bureau is how much more committed and enthusiastically invested the FBI now is in partnerships—especially by comparison to 10 or 15 years ago. It’s much more a part of the DNA of the organization than I, frankly, expected to find, and I think it’s a great thing for the country and for the world. It’s a mindset of: What can we bring to the table? What can they bring to the table? How can we match strengths, so that when we put the two that the FBI has, together with the two that each of our partners has, it makes not four, but five or six or seven?

We’re working more closely with our federal partners. Just as an example: Seven federal agencies, including DHS, have detailed personnel to our Cyber Division. This threat is moving so quickly that any time for turf battles is long gone. To those of you in the private sector, I would say this: 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 have a strong relationship with the European Cybercrime Centre (EC3). We have cyber agents embedded with our international counterparts in strategic locations worldwide, helping to build relationships and coordinate investigations. We're sharing actionable information—details of cyber tools and operational infrastructure. And we're working with our partners around the globe to curb our adversaries' ability to conduct further attacks or generate illicit funding.

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're making progress. Last 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 a number of 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, coordinated with other agencies 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.

And just last month, DOJ extradited the operator of the Kelihos botnet. Last year, the Kelihos botnet distributed hundreds of millions of fraudulent e-mails, stole banking credentials, and installed ransomware and other malicious software on computers all over the world. We worked with our foreign law enforcement partners in both Spain and the Netherlands to identify and apprehend the Russian hacker and dismantle the botnet.

Through our continuous work together, we're forming stronger partnerships and adapting our strategy to be more nimble and effective. But the bad news is, we're not the only ones building partnerships and adapting—the criminals do that too.

I mentioned the blended threat earlier. You’re probably aware of 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. Last 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, which means their vacation destinations are more limited.

We’re making strides, but the FBI needs to do more to meet the cyber challenge. For example, we want to do more to mitigate emerging threats. 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. But we need the private sector to work with us. At the FBI, we treat victim companies as victims. So, please, when there are indications of unauthorized access to—or malware present on—critical IT systems, when an attack results in a significant loss of data, systems, or control of systems, when there’s a potential for impact to national security, economic security, or public health and safety, or when an intrusion affects critical infrastructure, call us. Because we want to help you, and our focus will be on doing everything we can to help you.

The Way Forward—Digital Transformation

As cyber threats evolve, we need to evolve as well. This means evolving both our day-to-day operational strategies and our broader approach to handling global digital challenges.

To combat these blended threats and worldwide computer intrusions, we can no longer just investigate individual parts of a criminal scheme occurring in one jurisdiction. We need to focus our efforts on dismantling the entire cyber enterprise. We’re prosecuting the actors, burning their infrastructure, and seizing their illicit proceeds. We’re taking down the groups running malware campaigns and the criminals who support them—those who operate the dark markets, compromise networks and servers, and the people who buy and sell stolen data. Think of it as going after the distribution ring and the manufacturer rather than simply taking out the drug dealer on the corner. And we need to have a global perspective. We need to delegate roles and responsibilities across multiple field offices and to international partners—so that we can share information in real time, as we target and dismantle the most significant cyber enterprises.

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

Transnational crime groups, sexual predators, fraudsters, and terrorists are all transforming the way they do business as technology evolves. Huge swaths of these crimes have a digital component or occur almost entirely online. And new technical trends are making the investigative environment a lot more complex. Just a few months ago, for example, three young men pled guilty to creating the Mirai botnet—malware that exploited more than 100,000 devices connected to the Internet of Things. The botnet overwhelmed websites, like the attacks that took down Netflix and Twitter last year.

The digital environment presents new challenges that the FBI has to address in terms of what’s coming down the pike. Advances like artificial intelligence or cryptocurrencies have implications not just for the commercial sector, but for national security. Encrypted communications have changed the way criminals and terrorists plan their crimes. More on that in just a moment. And the avalanche of data created by our use of technology presents a huge challenge for every organization.

I’m convinced that we, the FBI—like a lot of other organizations—haven’t fully gotten our arms around these new technologies and how they may impact 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, of what we’re not seeing yet—but soon will. We need to put our heads together in conferences like this and in other ways, to be better prepared. Not just to face current threats, but to face 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. Some of our smartest people are thinking strategically about how the entire FBI can evolve in this rapidly changing environment. To do that we also need to focus more on innovation, approaching problems in new ways, with new ideas—which isn't something that always comes naturally to government. We can't just rely on the way we've always done things. And I don't mean just technological innovation—although that's a huge part of it. I'm talking about 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 of the right people, and more innovation. But the FBI can't navigate that digital landscape alone. We also need to continue building on our partnerships with our counterparts in federal agencies, with our international counterparts, with the cyber research community, and with the private sector.

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-buggy. The digital environment means we don't simply need improved technical tools; we also need legal clarifications to address gaps. Bottom line: We need to be a force of specialized, technically trained personnel that's cutting-edge, forward-leaning and able to fully investigate and combat the diverse cyber threats.

Going Dark

I want to wrap up by talking about one of our biggest challenges connected to the digital revolution. I'm referring, of course, to the Going Dark problem. We face an enormous and increasing number of cases that rely on electronic evidence. And we 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—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. Last fall I spoke to a group of CISOs and someone asked about that number. He basically said, "What's the big deal with 7,800? There are millions of devices out there."

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 plenty of other information available outside of our smart phones and our devices. Information like transactional information for calls and text messages—metadata. While there's a certain amount we can glean from that, for purposes of actually prosecuting terrorists and criminals—to actually prevent attacks and save lives through arrest and prosecution—words can be evidence, while mere association between subjects really isn't.

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 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, which is an increasingly widespread problem. 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. Actually, the FBI is on the front line fighting cyber crime and economic espionage. But information security programs need to be thoughtfully designed so they don't undermine the lawful tools we need to keep the American people safe.

While convinced of the problem, I'm open to all constructive solutions, solutions that take the public safety issue seriously. We need a thoughtful and sensible approach, one that 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 own lawful need to access data be taken just as seriously. 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.

Some of you may know about the chat and messaging platform called Symphony. This was used by a group of major banks, and marketed as offering something called "guaranteed data deletion," among other things. Maybe the labeling, maybe the content didn't sit too well with the friendly regulator down the street—the New York Department of Financial Services. DFS was concerned that the feature could be used to hamper regulatory investigations of Wall Street. In response, the four banks reached an agreement with the Department to help ensure responsible use of Symphony. They agreed to keep a copy of all communications sent to or from them through Symphony for a period of seven years. The banks also agreed to store duplicate copies of the encryption keys for their messages with independent custodians who aren't controlled by the banks.

So at the end, the data in Symphony was still secure, still encrypted, but also accessible to the regulators so they could do their jobs. I'm confident that by working together and finding similar areas to agree and compromise, we can come up with solutions to the Going Dark problem.

After all, America leads the world in innovation. We have the brightest minds doing and creating fantastic things. 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. Again, I'm open to all kinds of ideas. But 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—much less the direction it's going—is acceptable.

Conclusion

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. I look forward to working with you in the years to come. Now I'd be happy to take a few questions.