JUSTICE NEWS

# Acting Assistant Attorney General Mary B. McCord for National Security Delivers Keynote Remarks at Second Annual Billington International Cybersecurity Summit Dinner

Washington, DC, United States ~ Wednesday, March 29, 2017

---

Thank you for inviting me to speak with you today. The topics on tap for this summit are precisely the questions that corporate leaders like you must address as we collectively face the ever-evolving threat of malicious cyber activity.

I'm here to speak about protecting our national assets from nation-state threats. You may be wondering why I say "our" national assets. Certainly there are government secrets that the government must protect. But I'm talking about the national assets that are largely in private-sector hands. These assets include our critical infrastructure — the telecommunications systems, financial systems, electric grids and mass transit systems that sustain our way of life — as well as the technology, innovations and other crown jewels that drive our economy and help secure our global leadership.

These assets are targets not just for criminals, but also for nation-states and terrorist groups that seek to exploit vulnerabilities in our networks to probe our critical infrastructure, plan destructive attacks, steal our personal information and intellectual property, threaten violence, and extort money much like hostage takers seeking a ransom.

Today I'd like to talk to you about the risks to your business from threats to our national security, how the Department of Justice is working to address them, and the ways that you can manage them.

As the head of the Department of Justice's National Security Division, my job is to carry out the Department's highest priority — combatting threats to our national security. I lead more than 350 professionals dedicated to this mission — whether the threats come in the form of terrorists, spies and weapons proliferators; or national security-related cyber-attacks and other threats against our national assets. Our broad-based approach reflects our philosophy that our national security priorities must include not only the physical safety of all Americans, but also helping you defend against corrupt insiders, hackers and others who would harm your companies and your customers.

**The National Security Division**

First, I want to provide some brief background about what our experience with other national security threats, like international terrorism, has taught us about combatting cyber and other threats to our national assets, and how the National Security Division came to be.

It's no surprise that 9/11 was a watershed moment in our approach to countering terrorism as a government. It both highlighted weaknesses in our government's approach to addressing the terrorist threat and threw into stark relief how significant that threat had become. In particular, it spurred the government to recognize that, if we are to defeat this threat, we must bring to bear the full complement of the federal government's resources. So, while we used military force, we also recognized that law enforcement is a valuable tool for disrupting plots and neutralizing terrorists, and we leveraged economic sanctions and diplomatic measures to attack this global problem.

Before we could integrate our efforts, we had to bring down the wall that previously existed between the intelligence community and law enforcement — a wall that stood most firmly in the Department of Justice, where some attorneys prosecuted national security crimes and others interfaced with the intelligence community, always from within separate offices. To end that divide, Congress in 2006 created the Department's first new litigating division in almost half a century, the National Security Division. As a Division, we unite prosecutors and law enforcement officials with

intelligence attorneys and the intelligence community to ensure that we approach national security threats using every tool and resource available to the federal government.

Since the National Security Division's creation, it has become increasingly clear that the factors that motivated our creation and guided our efforts to combat terrorism are equally applicable to our efforts to protect our valuable national assets. In recent years, we have seen more and more attempts by foreign nation-states to acquire sensitive technologies and proprietary information from U.S. companies and to disrupt and destroy critical infrastructure.

**Economic Espionage**

NSD's commitment to protecting national assets has grown in proportion to the threat that we are now facing. As with combatting international terrorism, the federal government has developed a broad-ranging suite of tools to tackle these threats — including criminal prosecutions, sanctions, trade pressure and diplomatic options — and, together with our interagency partners, we have the ability to pick the best tool or combination of tools to get the job done under the rule of law.
For example, we seek to mitigate national security threats posed by foreign nation-state actors by reviewing foreign acquisitions — which can give the acquiring company access to critical technologies and increase its reach within the U.S. — and by imposing export controls on U.S. businesses to protect sensitive technologies from reaching the wrong hands.

But when certain foreign entities eager for sensitive and valuable intellectual property can't acquire it legally and don't want to spend the time or money to develop it on their own, they may take another approach: they may try to steal it. This poses a significant threat to national security — and a major business risk to the victim company. Economic espionage can take a number of forms.

Perhaps the most salient form for this audience is theft by cyber intrusion. In May 2014, in a first-of-its kind case, DOJ indicted five Chinese military hackers for stealing trade secrets and sensitive business information from U.S. companies for the benefit of Chinese competitors. The indictment alleged numerous and specific instances in which uniformed officers of the Third Department of the Chinese People's Liberation Army (PLA) hacked into the computer systems of American nuclear power, metals and solar-products companies to steal trade secrets and sensitive internal communications, such as pricing information and trade litigation strategy, that could be used by Chinese companies for commercial advantage. This was the military officers' full-time day job: our indictment alleged that their activity peaked between 9 a.m. and 12 p.m., their time, stopped for an hour — a healthy lunch break — and then picked up again from 1 p.m. to 6 p.m. No company can expect to always successfully defend against these kinds of organized campaigns.

In another case from last year, Su Bin, a Chinese businessman, pleaded guilty to participating in a conspiracy to hack into the computer networks of U.S. defense contractors to steal sensitive information, including data related to military transport aircraft and fighter jets. Su would tell his co-conspirators, military officers in China, what companies to target. When those co-conspirators had successfully gained access, they would send him the directory file listings and folders so that Su could tell them exactly what to steal and why. Su Bin was indicted, found in Canada, transferred to the U.S., and ultimately sentenced to nearly four years in prison for his crimes. But criminal prosecution wasn't the only tool we used. When Su was first arrested, the Commerce Department listed his companies on the Entity List, making it practically impossible for them to obtain goods and services from the United States.

Cyber intrusions may be the newest form of economic espionage, but they are not the only method of stealing important business secrets. As we have seen over and over again, you should never underestimate insider threats. In 2014, DOJ successfully prosecuted a former DuPont employee and his co-conspirator for stealing trade secrets and selling them to Chinese state-owned companies. The stolen trade secret was the formula for producing the color white (chloride-route titanium dioxide production technology). Its applications are too numerous to list, but needless to say that proprietary process, which took decades to develop and perfect, essentially is priceless to DuPont.

You also can never be too cautious about the physical security of the facilities in which your most sensitive information is stored — even if it is outside. This past year, a Chinese national, Mo Hailong, was convicted and

sentenced to three years in prison for stealing inbred corn seeds, the valuable intellectual property of U.S. agricultural products companies, for the benefit of a China-based seed company. As part of its five-year plan, China is openly seeking to develop a self-sustaining food supply through the acquisition of the most cutting-edge agricultural technology. And to show you that IP theft can be a decidedly low tech endeavor, Mo literally stole the corn seeds from the ground: company employees discovered his scheme when he was observed in the fields, on his hands and knees, digging up the seeds.

**The Importance of Attribution in Responding to Cyber Attacks**

Companies must be ready for all of these varied vulnerabilities, but the threat to your company and our national security is broader than the theft of your intellectual property. We know that state-sponsored actors also exploit vulnerabilities in cyber security for destructive and malicious purposes.

For many years, when acting in cyber space, nation-states and their affiliates enjoyed what they perceived to be a cloak of anonymity — a cloak they hid behind to break our laws and to threaten our security and economic well-being. They had this perceived cover because they thought we couldn't figure out who did it and, if we did figure it out, we would keep it a secret. But in responding to the cyber threat posed by state-sponsored actors, the government has recognized the importance of attribution — to name those responsible for online intrusions with confidence, down to the country, government agency, organization or even individuals involved.

Public attribution alone can have an important deterrent effect. Being publicly identified creates a risk of detention or arrest abroad. It restricts liberty and travel. But perhaps most importantly, hackers, like other thieves, are valued for their ability to get in and get out without getting caught. Anonymity is key for their livelihood and the exposure of public attribution can chill the marketplace for the hacker's services. Public attribution also raises awareness of the threats we face, thereby encouraging resilience and hardened defenses, and it validates victims' sense of violation and loss.

Moreover, attribution facilitates the use of so many other tools that promote deterrence. Law enforcement agencies and the Department of Justice are particularly skilled at these kinds of investigations, and, in some cases, attribution leads to public charges and a criminal prosecution. In other cases, prosecution may not be possible, but attribution opens the door for other tools that can change our adversaries' calculus by increasing the costs of their activities.

In 2015, President Obama issued a new Executive Order specifically aimed at cyber threats. Pursuant to this Executive Order, the Department of the Treasury can sanction individuals or entities who use cyber operations to harm or compromise critical infrastructure or system networks; those who conduct cyber intrusions to steal information for commercial advantage or private financial gain; or those who merely benefit from knowingly receiving such stolen information.

The availability of this tool has proved useful in forging diplomatic solutions to address the threat of cyber theft for commercial gain. Numerous cyber security experts agree that, coupled with the threat of possible U.S. sanctions, our indictment of the Chinese military hackers resulted in a historic agreement in the fall of 2015 by Chinese President Xi Jinping and other leaders of the G20, that nations should not conduct or support cyber-enabled theft of trade secrets or confidential business information with the intent to provide commercial advantage to companies or commercial entities. This kind of meeting of the minds of the community of nations drives bilateral negotiations and U.N. Security Council actions.

**Disruptive Cyber Attacks**

Although cyber security experts have noted an apparent reduction in cyber-enabled economic espionage by China since that agreement — and it remains to be seen whether that will continue — if anything, we are witnessing a rise in malicious cyber operations conducted by a variety of nation-states and their affiliates. Most recently, in 2016, President Obama amended the cyber Executive Order to allow the Treasury Department to impose sanctions for tampering with or misappropriating information in order to interfere with or undermine election processes. This was of course in response to Russian efforts to interfere with the 2016 presidential election. Along with two Russian

intelligence services, three Russian companies and four individuals that provided material support to those agencies were sanctioned.

We must remain vigilant against malicious cyber operations aimed at disruption and destruction, which have sowed chaos and imposed substantial costs across a number of economic sectors. In the past few years, we have attributed attacks to state-sponsored actors who seek to harm U.S. companies and infrastructure for their own strategic gain, and we have been able to bring charges against those responsible and enable the use of other tools in order to deter future attacks.

In the Sony Pictures hack in 2014, for example, we saw North Korea wage a destructive cyber attack intended to chill the speech of U.S. citizens and a company in the U.S. The attackers destroyed computer systems, stole valuable information, released corporate data and intellectual property at significant cost, and threatened employees and customers. Based on the FBI's attribution, the U.S. government added new sanctions against North Korea.

In March 2016, DOJ unsealed an indictment charging seven Iranian hackers for an extensive campaign of distributed denial-of-service attacks against 46 major financial institutions in 2011 and 2012. These attacks cut customers off from online access to their bank accounts and cost the victim companies tens of millions of dollars. These hackers had ties to the Iranian government, including the Islamic Revolutionary Guard Corps.

One of the hackers was also charged with obtaining unauthorized access into the industrial control systems of the Bowman Dam, located in Rye, New York. Had the dam not been disconnected from the system for maintenance, the intrusion could have given the hacker control of the dam's water levels and flow rates.

The same week that the Iranian DDOS indictment was unsealed, we unsealed a complaint against members of the Syrian Electronic Army — a pro-Syrian regime hacker group — charging them with using spear-phishing and other techniques to collect information used to deface websites, publish pro-Syrian regime propaganda and exfiltrate valuable information. As one of the complaints alleged, the hackers extorted money from victims by threatening further intrusions, defacements and sales of propriety information. In one of these attacks, the Syrian hackers posted a fake news feed on Twitter stating that a bomb had gone off in the White House, injuring the President. In another, the hackers gained access to a recruiting website for the U.S. Marine Corps and posted a defacement encouraging U.S. marines to "refuse 'their' orders."

Just this month, we indicted four individuals responsible for the 2014 hack into Yahoo's network, which involved the theft of information about at least 500 million Yahoo accounts and the use of that information to obtain the contents of accounts at Yahoo and other email providers. Two of the defendants named in the indictment are officers of the Russian Federal Security Service (FSB), one of the Russian intelligence agencies sanctioned in 2016 by President Obama, who are alleged to have directed their co-conspirators, two criminal hackers, to collect information through computer intrusions in the United States and elsewhere. The FSB unit that the defendants worked for is also the FBI's point of contact in Moscow for cyber-crime matters. The involvement and direction of FSB officers with law enforcement responsibilities makes this conduct that much more egregious.

Lest you think that we will never be able to bring foreign hackers to justice, our international law enforcement partners have often assisted us in making arrests and extradited those we have indicted for cybercrimes. One of the SEA hackers was arrested at our request in Germany, extradited to the U.S. and pleaded guilty in a U.S. federal court. And one of the alleged co-conspirators involved in the Yahoo hack, Karim Baratov, was arrested in Canada on a U.S. provisional arrest warrant; we are seeking to have him brought to the United States to face charges.

**Evolving Threats**

These examples show that we will find and expose those who threaten our national assets through cyber-attacks or theft. But those who would do us harm are able to reach further than ever before. I am particularly troubled by efforts to take advantage of companies' vulnerabilities in order to victimize those businesses' customers

We now see ISIS crowdsourcing terrorism — using cyber intrusions to obtain information or resources that, when placed in the hands of terrorists, could prove deadly. Ardit Ferizi, the leader of a Kosovar hacking group, hacked into the computer system of a major U.S. retailer, stole the personally identifiable information of thousands of customers, and culled through it to locate the PII of approximately 1,300 American military and government personnel. Ferizi then provided that information to a Syria-based ISIS member, Junaid Hussain, known for calling on aspiring terrorists around the world to commit terrorist attacks at home. Hussain subsequently posted a tweet that linked to a document containing the stolen PII, and threatened:

> We are in your emails and computer systems, watching and recording your every move, we have your names and addresses . . . we are passing on your personal information to the soldiers of the khilifah, who soon . . . will strike at your necks in your own lands!

Ferizi was found in Malaysia, transferred to U.S. custody and was sentenced to 20 years' imprisonment after pleading guilty to providing material support to ISIS. Hussain was killed in a U.S. military airstrike.

The Ferizi case also highlights the importance of working with law enforcement even in light of what might appear to the victim company to be an unsophisticated cyber intrusion. Fortunately, the targeted retailer cooperated with law enforcement, which was able to investigate the incident and identify the terrorists behind the keyboards. Even more fortunately, no physical harm came to any Americans as a result of this breach.

Most recently, we've come to appreciate the vulnerabilities presented by "smart" consumer products. While the connectivity of the "Internet of Things" provides immense technological opportunity, convenience and efficiency, it also opens up significant vulnerabilities.

Just a few months ago, we saw massive DDOS attacks against the website of a security researcher, a French ISP, and a U.S. DNS registrar, as well as the disruption of internet access for nearly a million users in Germany. All four attacks have been linked to a growing botnet composed of cameras, DVRs, and other devices infected with the Mirai malware. And as we learned, attacks like this one, approaching one terabit per second, can destabilize the core infrastructure of the Internet itself.

Most of those in attendance today probably are familiar, as well, with the vulnerability in auto vehicle control systems exposed by cyber security researchers in 2015, who were able to hack into the system of a sports utility vehicle, gaining the ability to shut down the engine, disable the brakes, affect steering, and control turn signals, door locks, the tachometer, radio, HVAC, and GPS. This incident resulted in the recall of nearly 1.4 million vehicles.

Given the dynamic intent of our foreign adversaries — who seek to use cyber operations to cause damage as a foreign policy tool, and not just to access sensitive information — we are concerned about new national security risks due to the combination of the Internet of Things' vulnerabilities and an increased ability to remotely access systems.

It is my hope that companies will respond to the threat posed by the Internet of Things in the same vein as social media companies have begun to respond to terrorist use of their platforms. Terrorist groups have leveraged social media tools and mainstream technology to facilitate their operational planning through encrypted communications and to call for sympathizers to conduct their own attacks. After seeing their networks used in ways they neither desired nor even contemplated, social media companies have begun taking steps to reduce the ability to exploit their products. Smart products — also developed with the best of intentions but without adequate consideration of vulnerabilities — demand a similar private sector response. Through our outreach efforts, we are trying to raise awareness about the national security threats interconnectivity poses and to encourage IoT developers and manufacturers to prioritize device security early in the design and manufacturing process, rather than after devices have entered into wide commercial use.

**Partnering with the Private Sector**

So what does this mean for you? When it comes to threats to our national assets, you are on the front lines. In many cases, your adversaries have the full backing of their foreign governments and so should you. We are here to help.

We work with U.S. companies, across all industry sectors, to ensure that our national security interests are protected. NSD and the FBI stand ready to help you understand:

- the vulnerabilities that might exist for your organization,
- how to minimize them, and
- how to respond when those vulnerabilities lead to the wrongful theft, exfiltration, or exportation of your sensitive technologies and information, no matter what the means including, in some instances, raising costs to those who may benefit from the theft.

We have spent significant time and energy in face-to-face sit-downs so that we may better understand the concerns and challenges facing U.S. companies, share guidance and information, and assist with protection, detection, attribution and response.

We can warn companies that manufacture or sell targeted U.S. technology when certain bad actors are seeking the particular technology they make. We hope to prepare industry for these threats and help you stem the flow of sensitive technology out of the United States. In the Iowa seeds case, for example, due to the quick action of security staff, the FBI was able to disrupt the threat and hold the perpetrator accountable.

In the case of cross-border transactions, we can share information with you on the types of technology and intellectual property nation-states are targeting to help you assess your vulnerabilities from asset sales, joint ventures and research collaborations.

And in the case of a cyber-attack, if an organization works with law enforcement, it puts both in the best possible position to find out exactly what happened and to remediate and prevent further damage. The evidence is often fleeting, so early notification and access to the data is extremely important. For example, it was Yahoo's valuable cooperation that allowed us to identify the nation-state-affiliated actors responsible for the attack and build our case.

Law enforcement also may be able to use legal authorities and tools that are unavailable to nongovernmental entities, or enlist the assistance of international partners to locate and take down stolen data or identify a perpetrator.

Early cooperation has many benefits. When we are notified of an intrusion, we share information with other potential victims. In the case of the DDOS attacks on the financial sector, with the cooperation of the private sector, the FBI regularly provided updated information regarding the identity of systems that had been infected with the defendants' malware and were operating as bots within malicious botnets, aiding in the effort to remove the malware to protect customers and other potential victims. One organization's vulnerability is everyone's vulnerability, and it is critical that we work together.

We recognize that there are a variety of reasons that the private sector may be wary of reporting a possible breach to law enforcement. Concerns about regulators, reputational harm and potential shareholder lawsuits are all legitimate. We are willing to talk through a company's concerns at the outset and work with the company and its counsel to address them. A victim of a cyber-attack is not so different from victims of other crimes, and we seek to treat them that way, respecting their boundaries and concerns.

Thank you again for inviting me here today. Our nation is most secure, and our privacy and economic vitality are best protected, when the government and the private sector work together to develop strategies to secure information access, detect threats and respond when incidents do happen.

---

**Topic:**
Counterintelligence and Export Control
Counterterrorism

National Security Division (NSD)

**Speaker:**
Acting Assistant Attorney General for National Security Mary B. McCord

*Updated March 29, 2017*


National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu