THE BROOKINGS INSTITUTION

TACKLING EMERGENCY NATIONAL SECURITY THREATS THROUGH LAW ENFORCEMENT

Washington, D.C.

Thursday, May 22, 2014

PARTICIPANTS:

Introduction and Moderator:

BENJAMIN WITTES
Senior Fellow
The Brookings Institution

Featured Speaker:

JOHN CARLIN
Assistant Attorney General, National Security
U.S. Department of State

* * * * *

P R O C E E D I N G S

MR. WITTES: Welcome to Brookings. My name is Benjamin Wittes. I'm a senior fellow in the Governance Studies Department and very pleased today to welcome Assistant Attorney General John Carlin of the National Security Division to Brookings. Unfortunately, there is just nothing going on in the area of cyber espionage or emerging national security threats these days for him to talk about, so it's going to be a short and relatively uninteresting session. I'm joking.

It's actually an amazing time to have him here. As you all know, or probably if you've not been living in a cave for the last 48 to 72 hours, this is actually a big week in this area and it involves some very significant and unprecedented actions by the federal government. Specifically, in the bringing of indictments against foreign military officials for cyber attacks on U.S. companies and espionage against American business interests.

Separately the House just passed the USA Freedom Act, significantly amending NSA surveillance authorities. So there's a lot going on in the areas both of our own activities with respect to spying and collection authorities and with respect to our response to other country's activities against us.

How similar are these sets of authorities and actions that we are doing to those that are done to us and to which we're responding? How different are they? Are there principle differences between what we acknowledge that we do and what we authorize under our law and what we object to when it's done to us? These are some of the issues that I think we are talking about this week and I hope we'll be talking about today.

And I can't think of a better person to have address them for us. John Carlin has been acting assistant attorney general for some time and was recently

confirmed in the permanent role. He served previously as the chief of staff to his predecessor and principle deputy to Lisa Monaco when she was in the role. And previously he was chief of staff and senior counsel to Robert Mueller when he was director of the FBI. A career federal prosecutor, Mr. Carlin served as national coordinator of DOJ's Computer Hacking and Intellectual Property Program, which consisted of 240 AUSA's and DOJ prosecutors, specially trained to prosecute cyber crime and intellectual property cases. So he has a lot of background in the area that gave rise to this week's indictment.

He has a degree from Harvard Law School and from Williams College. He'll speak for about 45 minutes and then I have a Q&A with him over there and we'll take some questions from the audience. I ask that you all silence your phones because they've got a lot of cameras on in the room, and please join me in welcoming John Carlin. (Applause)

MR. CARLIN: Thank you, Ben, for that kind introduction and I'm grateful to be here at Brookings today discussing emerging national security threats. I'm also a keen fan of the Lawfare blog, as are many who are in this national security field, so we appreciate your work on that, as well.

On Monday, the Department of Justice announced charges against five members of the Chinese military for computer hacking, economic espionage, and other offenses directed at six American victims in the U.S. nuclear power, medals, and solar industries. Today I'll focus on this growing threat, state-sponsored cyber intrusions targeting, for profit, the sensitive and proprietary information of U.S. companies.

These charges against uniformed members of the Chinese military were the first of their kind. Some said they could not be brought. At the department, we follow the facts and the evidence wherever they lead. And sometimes the facts and evidence

lead us to a lone hacker in a basement in the U.S., sometimes they lead to an organized crime syndicate in Russia, and sometimes they lead us to a uniformed member of the Chinese military.

But no matter where they lead, there should be and there are no free passes. We should not stand idly by, tacitly giving permission to anyone to steal from us. We will hold accountable those who steal, no matter where they are, no matter who they are, and whether or not they steal in person or through the internet. Because cyber crime has real victims.

While cases like the one brought in Pittsburgh are extremely challenging, this week we proved that they are possible. The criminal justice system must be a critical component of our nation's cyber security strategy. As long as criminals continue stealing from American businesses, we will continue pursuing those criminals.

The charges announced on Monday were groundbreaking and they represent a significant step forward in our cyber approach. And they were many years in the making. Within the Justice Department, the National Security Division, or NSD, focuses on cyber threats to the national security, those posed by terrorists or nation states.

Our approach to these threats are deeply rooted in our division's history and our success in the cyber arena builds upon a solid foundation. NSD was created in response to the grave threat of terrorism. After the devastating attacks of September 11th, it became clear that the Justice Department needed to reorganize to tackle terrorism and other national security threats more effectively. We needed a single division to integrate the work of prosecutors and law enforcement officials with intelligence attorneys, and the intelligence community.

So, in 2006, Congress created the department's first new litigating

section in half a century, NSD. NSD works closely with partners throughout the government to insure that we leverage all available tools to combat the terrorism threat. And we've proven, in that context, that the criminal justice system is a vital part of our nation's counterterrorism strategy.

Just this week, Abu Hamza al-Masri was convicted by a jury in New York. He was involved in an attack in Yemen in December 1998 that resulted in the deaths of four hostages and provided material support to terrorists, including al Qaeda and the Taliban. In March of this year Sulaiman Abu Ghaith was convicted of conspiring to kill Americans, and other terrorism charges. Abu Gaith was the son-in-law of Osama bin Laden and a senior member of al Qaeda. He was the face and voice of al Qaeda in days and weeks after the 9-11 attacks.

In both of those cases, while it may have taken more than a decade, as a result of our integrated approach to combating terrorism, these men were brought to justice. And these cases are just the two most recent in a long line of successful criminal prosecutions of terrorist offenses.

Recently, we took the lessons we learned from counterterrorism and we applied them to our work on national security cyber threats. In the face of escalating threats, we recognize the need to reorganize and to integrate. When I was chief of staff to Director Mueller at the FBI, we undertook a transformation there to meet the same growing cyber threat. And in 2011, we brought that approach to NSD.

In the late fall of 2011, 10 years after 9-11, we established a review group to evaluate NSD's existing work on national security threats and to chart out a plan for future threats. Six months later, that team issued recommendations that shaped what NSD's national security cyber program looks like today.

Most significantly, in 2012, we created and trained the National Security

Cyber Specialists Network to focus on combating cyber threats to the national security. This network, known as NSCS, includes prosecutors from every United States Attorney's Office around the country, along with experts from the department's Computer Crime and Intellectual Property section and attorneys from across all the different parts of NSD.

Adopting the successful counterterrorism model, we now have prosecutors nationwide routinely meeting with the FBI to review intelligence and investigative files. The creation of the NSCS network was motivated by a desire to make a tangible impact on U.S. cyber security efforts through criminal investigation and through prosecution. By December of 2012, we made public prediction that with the establishment of NSCS -- that is, by empowering more than 100 prosecutors in the field, working with the FBI on these cases -- that one would be brought. And this week we made good on that promise.

It is this new and integrated approach that made the Pittsburgh case possible. As part of the creation of the NSCS, we've brought prosecutors from all around the country -- from Wisconsin and New York, from Georgia -- to help NSD build the case. We partnered with the Western District of Pennsylvania, where the victims were repeatedly hit, and we worked with offices across the FBI from California to Oregon to Oklahoma and back here in D.C. Our team thought creatively, they worked collaboratively, and they explored all available options for stopping this activity.

And that is how we were able to indict five members of the Third Department of the People's Liberation Army -- or 3PLA -- and it's unit, 61398. These men stand accused of cyber intrusions targeting a range of U.S. industries. The indictment alleges with particularity specific actions on specific days by specific actors to use their computers to steal information from across our economy. It alleges that while the men and women of our American businesses spent their business days innovating,

creating, and developing strategies to compete in the global marketplace, that these members of Unit 61398 were spending their business days in Shanghai stealing the fruits of American labor. It alleges that they stole information particularly beneficial to Chinese companies and that they took communications that would provide competitors with key insight into the strategies and vulnerabilities of the victims.

Now, there are some who question this law enforcement action. And, generally speaking, these questions fall into three categories.

First, whether there is a clear line between what these individuals have been accused of and what the U.S. or other nations do. Second, whether charges like these can truly impact cyber security, particularly when there may be significant challenges to arresting and ultimately trying these individuals in criminal court. And third, whether government should instead focus on hardening defenses rather than pursuing charges.

As to the first question, while some commentators may ask whether this is a new line to draw, in fact, we are aware of no nation in the world that publicly states that theft of information for commercial gain is acceptable. Even in this case, China has not attempted to justify the allegations. Instead, they deny them. And this has been a consistent response.

A little over a year ago, the Chinese government flatly denied reports that Unit 61398 was hacking U.S. companies. A spokesman for China's Ministry of National Defense said, Chinese military forces have never supported any hacking activities. China also challenged the United States to present hard evidence, evidence that could stand up in court that cyber attacks against American targets are connected to the Chinese military.

Well, we did. And the response, hours after Monday's announcement,

the Chinese Foreign Ministry called the accusations purely fictitious and extremely absurd. Now we are confident that we have the evidence to back up these specific accusations in a court of law. Read the indictment. It is particular.

For the first time we have exposed the real faces and names behind the keyboards in Shanghai used to steal from American businesses. This is not conduct that responsible nations within the global economic community should tolerate. In the United States we believe that individuals and companies are entitled to the results of our creativity, including our property and our intellectual property. And we believe that one's work should not simply be taken from you and given to others.

But this is not a uniquely American value. Individuals around the world believe that people shouldn't take what others make. Responsible nations do conduct intelligence activities and nations openly acknowledge that they have intelligence services. Like others, our intelligence activities are focused on the national security needs of our country. That is why the President earlier this year reaffirmed in a Presidential Directive that, "it is not an authorized foreign intelligence purpose to collect such information to afford a competitive advantage to U.S. companies and U.S. business sectors commercially."

U.S. foreign intelligence collection occurs under the framework of the rule of law involving oversight by all three branches of government. As the Church committee report recognized back in 1976, the Constitution provides for a system of checks and balances and interdependent power, as between the Congress and the Executive Branch, with respect to foreign intelligence activity.

The very protections that are built into that legal framework subject that information to rigorous oversight and prevent sharing it with private companies for their private gain. But let's be clear, those protections do not exist in certain other countries

that are targeting everyday American trade secrets, sensitive business information, and intellectual property in order to steal specific information and pass it along to their domestic companies in order to give them a competitive edge. And to pretend otherwise is to promote a narrative of false equivalency.

Even though we know of no nation that stands up publicly to defend corporate theft for the profit of state owned enterprises, in the shadows there be some who encourage and support it. In short, we allege that the members of Unit 61398 that we have charged committed theft, pure and simple.

So although this case is the first of its kind, it is also in some respects just business as usual. As they have for decades, prosecutors in the field and at CCIPS use criminal investigation and prosecution to disrupt cyber crime. CCIPS is one of our most important partners in the fight against cyber crime and law enforcement has long been used to combat cyber threats and, as recently as this week, those criminal cases have made a tremendous impact on cyber security.

As you have likely seen, on Monday, the Department of Justice also announced charges in connection with Blackshades malicious software. These charges were part of the largest ever global cyber law enforcement operation, involving more than 90 arrests and taking place in more than 19 countries. Likewise, in the national security arena, when criminal law enforcement is the most effective tool we have to disrupt a terrorist threat, we employ it no matter how far away or shielded from prosecution the defendants may seem today.

When criminal enterprises steal our intellectual property and personal information or threaten our security, we investigate and we prosecute. These are not the first charges that we have lodged against individuals who have stolen from Americans to benefit state-owned enterprises. As just one example, we successfully obtained a

significant conviction for economic espionage -- the first jury conviction -- earlier this year. Walter Liew, an electrical engineer, obtained one of DuPont's secrets –- a process, honed over many decades, for making a multipurpose white pigment –- and he passed it to a large Chinese state-owned company.

What Liew stole was something that Americans see and use daily. Something that does not have any national security implication. Something that simply brings a profit. Liew stole the formula for the color white. He was brought to justice in the U.S. criminal justice system. Like Liew, we allege that the members of Unit 61398 that are charged stole to benefit Chinese state-owned enterprises. The thefts are similar. They both took place here in the United States, but the difference is that Unit 61398 operated remotely from the previously safe spaces of Shanghai. But we will no longer permit safe havens. Individuals, wherever they are, cannot avoid the consequences of their actions simply by capitalizing on 21st century tools and operating from the comfort of their desks half a world away.

These crimes are the same as many crimes that we have investigated and prosecuted before, only the method or means is different. But the threat we face is increasingly moving out of the physical world and into cyberspace, and thus, prosecutions of those who steal from us remotely must and will become the new normal. We will continue to pursue this option, along with others available to us.

The threat of economic espionage is serious and the threat of cyber economic espionage is mounting. Some estimate that every year the United States loses more than $300 billion from theft of our intellectual property. And they say that figure is about equivalent to the current annual level of U.S. exports to Asia. Losses of that magnitude cost the American economy untold numbers of jobs, real jobs. They reduce the profit that American firms make from research and development, which in

turn reduces the incentives and resources for innovation.

As the U.S. Attorney in Pittsburgh, David Hickton, said, “When these cyber intrusions occur, productions slow, plants close, workers get laid off and lose their homes.” And such activity also undermines the trust between countries and companies that is necessary to do business in our global economy. And our companies cannot face it alone. Companies cannot depend solely on their antivirus software to defend against attackers linked to deep state military budgets. It’s not a fair fight. To defend against those empowered by a government, we need our government on our side. We must support our entrepreneurs by using every tool we have to prevent, deter, and disrupt this conduct in any way we can. And likewise, we need you.

Just as the local police can’t control crime without victims calling in those crimes, our law enforcement officials, too, need cooperation from victims. It is our hope that the more cases we bring and the more perpetrators we bring to justice, the higher the level of cooperation we’re likely to receive. We cannot let this conduct go undeterred. Doing so would threaten our nation’s security.

Cases like the Pittsburgh case will have a deterrent effect. To those critics who raise questions about whether these charges will have any impact in light of the challenges associated with arresting and trying the individuals, the deterrent effect of charges can still be significant. General Keith Alexander, former NSA director, explained that, “The only way to deter cyber attack is to work to catch perpetrators and take strong and public action when we do.” FBI Director Mueller called for figuring out who is targeting us and going after them, saying, “We must remember that behind every intrusion is a person responsible for that intrusion -- a warm body behind the keyboard -- whether he or she sits in Tehran or Tucson; Shanghai or Seattle; Bucharest or the Bronx. Our ultimate goal must be to identify and deter the persons behind the keyboards.”

The government and private sector alike are increasing the call for prosecuting cyber theft of trade secrets. We need to prevent attacks and deterrence helps. Prosecutions can simultaneously punish those who have already committed bad acts and deter those who might otherwise commit bad acts in the future. In other words, by going after these crimes, we can help to stop the next group of criminals. It is, of course, possible that we will never obtain custody. But even if these five defendants evade arrest, laying bare this criminal activity takes it out of the shadows.

Law enforcement investigations can also support other valuable tools. Criminal charges can justify economic sanctions from our colleagues in the Treasury Department, sanctions that prevent criminals from engaging in financial transactions with U.S. entities and deny access to the U.S. financial system. They can facilitate diplomacy by the State Department, as our nation's diplomats lay out evidence of state-sponsored cyber theft to foreign government officials and force them to answer for those actions, or as they coordinate with other victimized countries. Furthermore, the investigations themselves can lead other governments to take action, even when the United States doesn't end up doing so.

So, we will continue to bring these kinds of cases. However, it is not easy and prosecutions like this present unique challenges. Cases can take years to investigate, and it can sometimes be tough to attribute the unlawful activity to particular individuals. They involve difficult decisions regarding how to protect sensitive sources and methods and, even after charging, it can be difficult to obtain custody of the defendants and to bring them to justice. But difficult does not mean impossible, and the status quo simply will not do. As the Attorney General said earlier this week in announcing these charges, "Enough is enough." We would not stand idly by as people hauled away our wealth in trucks and, likewise, we cannot allow it to be sucked out

through the Internet.

The indictment I've discussed is an important first step, but it must be just that, the first. Prosecutions will not solve the problem alone. We need to build on this success and keep responding with prosecutions where possible, but also with all of the other tools in our toolkit. We need to keep at it, and we appreciate the bipartisan support we've received from Congress, including particularly supportive words from Senators King and Whitehouse, along with the House and Senate Intelligence and Homeland Security and Judiciary Committees, both before and after this action.

Many of the individuals above provided resources and encouragement as we undertook transformation to combat this threat and we will need their help as we continue this transformation. We must continue until our adversaries realize that the cost of stealing from our companies outweigh the benefits.

So far, we talked primarily about criminal prosecution and other tools, but we recognize that stopping attacks before they ever take place is the ultimate goal. We will have succeeded when there are no more criminal charges to bring. And to that end, we've worked hard to improve cyber defenses, both in government and with the private sector. The FBI works closely with companies that have been the victims of hackers through, among other things, its InfraGard program. That program, which has more than 25,000 active members, brings together individuals in law enforcement, government, the private sector, and academia to talk about how to protect our critical infrastructure. And, likewise, the Department of Homeland Security, the Department of Energy, and other departments and agencies routinely work closely with companies to protect critical infrastructure. And the department heard from you and is taking steps to respond to the concerns of the private sector.

Just last month, we teamed up with the Federal Trade Commission to

issue a policy statement making it clear that antitrust law is not and should not be a bar to legitimate cyber security information sharing. And earlier this month, the Justice Department issued a whitepaper which clarifies that the Stored Communications Act does not ordinarily restrict network operators from sharing certain data with the government to guard information. This guidance will help the private sector collaborate more freely to protect itself. But all of this is just a start and going forward we need legislation to facilitate greater information sharing between the private sector and the government.

The charges announced earlier this week benefit not only victims, but also the broader American people and others worldwide. Chief Justice Burger once noted that criminal prosecutions, as a general matter, have an "educative effect" on the public. And while we may appreciate on a theoretical level that hacking to steal corporate secrets poses a major national security threat, there's no substitute for the educative effect that an indictment has. Putting a face at the keyboard and quantifying the damage done may help to galvanize all of us to improve our cyber security. It may also make us more vigilant to the economic, military, and geopolitical dangers associated with cyber space. For example, it might lead companies and other entities to examine their connection logs a little bit more closely to see what those activities those reveal and from where.

To wrap up, I want to applaud the dedicated investigators and prosecutors whose hard work produced this week's important indictment. It's only a first step, but it's a big step, and it's part of our growing effort to hold accountable those who steal American innovation. At the same time, we must acknowledge that prosecution alone is ultimately just one tool in the broader toolset for addressing the cyber threat and that prosecutions alone will not solve the problem. Trust in government depends, in part,

on our ability to defend, protect, and obtain justice for our citizens. Indictments and prosecutions are one clear and powerful way in which we, the people, governed by the rule of law, legitimize and prove our allegations.

And these actions have real consequences for the criminals they target, and deter those who might otherwise become criminals in the future. We continue to protect Americans from being victimized through cyberspace, and we will need your support to do so.

Thank you for your attention and I look forward to answering questions. (Applause)

MR. WITTES: By pushing you a little bit on the distinction that you've drawn between U.S. activities overseas, of which we've certainly heard a lot over the last year and the sort of activities that form the basis of this indictment. Now, as I understand the U.S. posture, we do not -- first of all, we obviously engage in espionage and we don't deny that some of that espionage involves spying on companies. The distinction that we draw is that when we spy on companies it is in the pursuit of national security objectives, not either in pursuit of economic objectives or the particular objectives of helping U.S. companies at the expense of the companies that we're spying on.

I'm interested in to what extent that is a distinction that sort of only the U.S. could love, in that we're an intellectual property-generating country, China's a giant manufacturing economy, why can't they just define their national security objectives as including the economic health of their companies? I mean, is the distinction that we're drawing really a stable one and that we'll be able to sustain in an international argument over what's legitimate and what's illegitimate in the realm of economic espionage?

MR. CARLIN: Well, let me -- it's a good question. Let's think about it the other way around for a second. Because whether or not we bring prosecutions and

follow the evidence where it leads is a choice, no matter what. And what we're seeing is, we're seeing victim companies -- private entities inside the United States -- and, as the indictment details, they might design a pipe and put a lot of research into designing the pipe. And then there's a question over whether you buy what they have built with their hard work and innovation or steal it. And when we come across a case of somebody stealing it by hacking into somebody's system without their permission and taking the designs that they would otherwise buy -- and sometimes it's right before they're about to get bought, so we know they're interested in it.

If we follow the facts and evidence where they lead, that might lead us to a criminal group. And if it led us to a criminal group -- a standard criminal group with no affiliation with any state -- I think everyone would agree that the proper course of action would to be to try to build an indictment and prosecute them, if we could find them and bring them to the U.S. And to draw a distinction that says when we follow the facts and the evidence and it leads to someone behind a keyboard and they happen to be wearing a uniform, that now there's some type of free pass for what's clearly criminal activity, it's just a theft -- it's the same theft we're seeing from other criminal groups -- is not a distinction I think the American public would want us to make. But, more importantly, I do not believe that there's a country in the world that would idly sit by and accept that type of theft.

MR. WITTES: And yet, we do have an understanding in the government-to-government espionage department that, you know, we do certain things, you do certain things to us, and if we follow that keyboard back and you find on the other end it's NSA spying on your government, you're kind of supposed to leave that alone. And similarly, if we follow that keyboard back and find out it's the People's Liberation Army, we're not going to have quite the same attitude toward an intrusion in a U.S.

Government computer system than we would if it were an organized criminal gang or an individual hacker. Or would we?

MR. CARLIN: Well, what we're talking about here is the theft from private companies for the benefit of other private companies with whom they are in competition. And that's where particular and specific facts, specific actions, and specific actors matter. And when we use a charging instrument like an indictment, we're not charging some abstract entity. We're charging particular people for particular acts and if you look at this indictment, they are stealing pipe designs from one company and, the evidence suggests, for the benefit of another company.

Also, interestingly, and you'll see that they were building a corporate intelligence database for a company and that's what they were paid to do as part of their job. That's theft.

Now, almost every country in the world has some type of intelligence service. And the idea of having an intelligence service to protect your national security is an old concept. But what you don't see is countries saying, we have a service out there whose goal it is to steal what you're making and working and give it to our companies, so that they don't have to buy it or compete.

MR. WITTES: So you had mentioned in the speech that China does not defend this practice. They deny the practice. I'm curious, are you aware of any country that defends this practice doctrinally or is it simply universally denied rather than defended?

MR. CARLIN: Personally, I am not aware of any country in the world that defends this practice and says that we ought to allow -- whether it's the military or a spy service or criminals in your country -- to go hack into somebody else's private company and steal what they're producing.

MR. WITTES: So I want to talk about the value of indictments. You talked about this a little bit in the speech, but, you know, some people will look at this and say, you have no prospect of getting custody of the suspects. China's a big country; it's very amply capable of protecting its people; our jurisdiction is limited. And, therefore, the role that an indictment like this plays is really one more of a kind of combination of an overt diplomatic pressure, a willingness to put facts on the record in a form, as you say, that's provable in law, that's backed up by evidence and has a certain heft. And it's, therefore, a form of very sophisticated legal PR rather than an indictment in the sense that you actually expect to get custody of the suspect and bring him to court and prove the case.

As succinctly as you can articulate it, what's the value of an indictment in a situation in which you have no expectation of obtaining custody?

MR. CARLIN: Well, first I want to challenge the premise. These are real charges based on evidence that was painstakingly compiled by excellent work by FBI investigators over a period of a year that we can, and hope to, present in front of a jury with all rights of due process. And we would not be allowed, under our principles of prosecution, to bring such an indictment unless we believed we had the evidence to secure a conviction beyond a reasonable doubt. And I look forward to having the opportunity to do that.

And we indict individuals all the time who are not currently in the custody of the United States and we may not know their whereabouts. I referenced today two terrorism cases that took more than a decade to bring. And we brought the charge and people may have said then, well, you have no expectation of getting this individual. They're overseas, they're in a cave, they're in ungoverned territory, they're in an unfriendly space. But they committed crimes and we charged it and we waited until we

could bring them before a court.

And similarly, I think you've seen that approach over the years, whether it's in relation to the Mafia or drug conspirators. But sometimes it's true, people evade capture. And even when they do evade capture and never face charges inside a court, I go back to what I was saying before, to not bring the charge is to somehow say that this is not criminal activity and that you're not stealing. But you are.

And that's the effect that it's having on American companies. That's the cost that we're seeing in terms of American jobs. And we're prosecuting the same cases when they're committed by someone physically inside the United States and we're prosecuting those same cases when they're a group that's not affiliated with a government. So, to decide somehow here that we're giving it a free pass not only deters, I think it encourages individuals to pursue this type of theft.

MR. WITTES: So there has been a fair bit of talk since Monday that this is the first of a wave and that we should expect to see a lot more of these. I obviously wouldn't ask you about individual cases, but is this -- you said that there was a transformation going on. As a general proposition, is this something we should expect to see a lot more of and, to the extent it is, how much of it should we expect to be about China versus other countries that we frequently hear are major thieves of intellectual property in the United States?

MR. CARLIN: Yeah, and so part of what I was discussing was we've had a transformation structurally in terms of how we approach these cases. At the National Security Division we trained hundreds of prosecutors in conjunction with our criminal colleagues throughout the country to work on these types of cases and look at the intelligence day-in and day-out.

And the FBI has similarly restructured to put task forces out throughout

the country. And now that people are trying to build this criminal option, as one of the options when they look at the information that they're gathering, I believe they can and will bring additional cases.

Now, these are hard cases to bring. They are technically complex. They cross national boundaries. And so it's always going to be difficult, but now that people are working it, I believe they can and will bring additional prosecutions. They're going to follow the facts and the evidence where they lead and respond to the crimes that they see. And so it's by no means a strategy that's aimed at any particular country. It's aimed at the crime and then following back the crime to see who committed it. And the focus is on economic theft of this unit, so those are the type of charges you may see in the future.

MR. WITTES: So I want to talk about one difficulty, complexity, of this type of case that does not arise, I think, in a lot of other cases where you're primarily looking at witness interviews. You refer to the warm body in back of the keyboard and I know in a lot of these computer forensics cases you can prove that a certain thing happened from a certain account or that a certain thing happened from a particular IP address, but it can be very, very difficult to prove that the individual who's notionally associated with that account was, in fact, the warm body sitting behind that keyboard when the offense took place.

And I'm just interested for your thoughts on how do you -- what are the strategies that one has to go that -- not the extra mile, it's the extra quarter of an inch, right? And that the hands on that keyboard are the person which you've got to know beyond a reasonable doubt -- you've got to be able to prove beyond a reasonable doubt not merely that the account and the particular computer are the instrumentalities of the offense, but that the individual associated with those is the one you think he is or she is? Talk a little bit about that challenge and how you meet it.

MR. CARLIN: And that is a challenge. And I'm not going to give all the means and methods by which the FBI are trying to find those individuals today. I hope you'll forgive me that. But one key step to meeting it is trying to meet it. So one change that takes place when you look to see if you can preserve a criminal option and have the opportunity to bring a criminal case is to focus on that type of specificity and attribution because that is important and a key principle of our criminal justice system.

Whereas, for intelligence purposes, it might be sufficient to do the attribution and say, oh, this is so-and-so nation state and they're trying to take this type of information for intelligence purposes. And that might be enough to do an assessment of what's happening. When you're doing a criminal case, as you say, you need to go that extra step because we're not interested in the overall intelligence service, we're interested in a specific crime conducted in a specific manner by a specific actor.

And one thing that I think that's important to that and which is why we need the cooperation, and to talk to companies and victims, is knowing why. When we're trying to prosecute the theft of corporate secrets, why are they taking it? Not why would a government generally take it, but what business are you competing with that would specifically want that information and why would they want it at the time that they took it? And that can help narrow down the actor.

MR. WITTES: So the basis of this indictment is U.S. domestic criminal law, which provides the theft of intellectual property from U.S. companies. I have not, nor could I, look up Chinese law on the theft of material from Chinese companies for -- not U.S. national security purposes or from Chinese government servers for U.S. national security purposes, but I'm relatively confident that Chinese criminal law has something to say that would forbid a lot of what we routinely defend -- you and I both, I different ways -- that goes on at Fort Meade. That is, we have an open policy that we engage in

espionage, i.e., steal secrets for national security purposes, but probably run roughshod over a lot of country's criminal laws in the course of doing so.

I'm curious whether we should expect foreign indictments of U.S. intelligence officials, and why we would -- other than to say that our law distinguishes between the purposes, why would this be different? How would we react if the Chinese government started indicting NSA officials -- current, former, future -- for acts that we would consider perfectly legitimate espionage?

MR. CARLIN: I've said, again, this is not about intelligence collection by a nation state to figure out what another nation state is thinking or to conduct your diplomacy or to plan or strategize for national security means. Nor is this case an indictment of an intelligence service. It's an indictment of particular people for stealing particular plans that were to benefit companies in China, state-owned enterprises, who are competing with the companies here. That's what we charged and it's specific in doing so.

And we did charge economic espionage and trade secrets. And we also charged violations of the Computer Fraud and Abuse Act and the prong that we were charging is when you commit those acts for economic advantage and personal financial gain. So that is a true distinction. I think it's one that's recognized through the world.

Everyone wants when they work on something, and they put their hard work and their creativity in it, to have the rewards of the fruits of their labor, and certainly China, along with many other countries in the world, has brilliant and creative entrepreneurs that want to have the benefit of what they produce. And when you knock down the door, walk into the office and steal it out of their safe, and then go and use it, instead of buying it, or if you take it by the Internet, that's crime.

MR. WITTES: So I'm going to ask one more question and then we'll go

to the audience. If you have a question, wait for the microphone and please introduce yourself, identify yourself, before you ask the question.

One additional question. What has the reaction from other governments? There are a lot of governments that have anxieties about Chinese activity in this area that have also cried foul in public, but not so far brought criminal cases. And what has the reaction from other intellectual -- you know, other IP-producing countries been to the action this week?

MR. CARLIN: Well, I can only answer what you know. It's been a slightly busy week and I'm not sure I'm in the best situation to give the reaction of countries around the world, but maybe some of my colleagues -- or are you all reading the papers?

MR. WITTES: Fair enough. Gary Mitchell in the front? He's always patient about waiting for the mic.

MR. MITCHELL: I'm trying to remember your question. (Laughter) Mr. Carlin, thank you. I'm Garrett Mitchell and I write *The Mitchell Report.* And when I first heard about the indictment and then, particularly, listening to you today being grilled by one of the best, I had two reactions. One is about cost-benefit and the other is about Mr. Rumsfeld's favorite, the known unknowns.

With respect to cost-benefit, the question that comes up for me is, though it is clear that you've been careful in the indictment to name specific warm bodies sitting behind specific keyboards, as Ben Wittes points out, there's that business about how difficult it is to actually prove they were there when it was happening. I'm thinking about it in slightly larger terms, which is we might look at it -- you might, Justice might look at it -- as a specific indictment of a specific person. It's my assumption that President Xi and Premier Li do not. To them it's a broadside on China. And as a

consequence, if that's true, it seems to me it raises the kind of question the prosecutors must deal with all the time, which is, is the cost of pursuing this indictment worth the benefit of whatever the outcome might be? And, of course, in these terms I'm talking both diplomatically, but the difficulty of demonstrating just how much actual economic harm has been done and will be done by these acts. So there's the cost-benefit question.

And then the second is the known unknowns. And what I mean by that is the minute I heard about this I thought, I wonder what Edward Snowden's doing right now? And what I mean by that is that Snowden has revealed a lot about us and what we're doing that almost no one seemed to know about. So I wonder if Mr. Snowden is saying, okay, and Mr. Greenwald are saying, okay, now it's time. We'll let loose a few other goodies that people don't know about that are going to make this more difficult.

MR. WITTES: All right. Gary's put a lot on the table.

MR. CARLIN: I can try to track all of that with a thoughtful question. So the President had said in the 2013, I believe it was, State of the Union -- and so we publicly announced that the theft of our intellectual property is not acceptable, the trade secrets is not acceptable. And I think that we've tried to deliver -- different folks in the government -- in every way possible the message that that's not intelligence business as usual, that's theft. And the reason why they're making that distinction is because it is immediately causing real harm to private citizens who are losing real jobs and the ability to produce and participate in our economy. And we have a responsibility then when there's real harm occurring in actuality each day to take action and not just to watch it occur. And if we were to watch it, track it, investigate it, follow it, and make a decision that at the end of the day we're just not going to bring criminal charges for these acts, depending on who the actor is, is not an acceptable place to be for American companies

and for American citizens.

So, in terms of the cost-benefit, that's the status quo that's unacceptable. And, if I may flip it slightly, we need to raise the cost and make it extraordinarily clear that the benefits that you're getting from stealing this information do not outweigh the costs. So we need to up the cost until the behavior stops. And in that sense, as I said in the speech, I hope to never bring another criminal case because the activity will stop.

I think you also raised the issue of future disclosures. You never know what the future will bring. I would hope everyone, whatever their persuasion is, would like to see this type of activity stop, the stealing of corporate secrets wherever they're occurring. But the President has also made it clear that this is something that the United States will not do, which is we won't go stealing other people's trade secrets and giving it to our companies to give them an unfair advantage.

MR. WITTES: Carrie Johnson?

MS. JOHNSON: Thanks for doing this. I'm Carrie Johnson from NPR. I have a question more about the U.S. offensive or investigative capabilities.

The other day I read the FBI was purchasing some malware, and I'm wondering what the NSD's role is. In part it was created to oversee some of the intelligence gathering inside the U.S. In general terms, Mr. Carlin, how does the NSD oversee the FBI's investigative/offensive capabilities in this cyber area?

MR. CARLIN: I'm not familiar with the specific report that you're referring to, but we have a couple of different roles. One would be if the FBI were applying before the Foreign Intelligence Surveillance Court, under the FISA -- or the Foreign Intelligence Surveillance Amendments Act -- then before they could present such an application to the court, they would go through lawyers at the National Security Division who would see whether it made out the proper predicate -- probable cause -- under Title 1 of the FISA

Act. And then we'd vet and present those applications to the court for a proper approval, if they were going to use it for an intelligence means.

Similarly, if they were applying to use it through the criminal system, and maybe lawyers from the National Security Division -- either in our counterterrorism section or our counterespionage section -- who would work with them on obtaining the proper permissions or approvals through a criminal court. They need a criminal court process.

We also do have an oversight section that does national security reviews and so it reviews the use of certain national security authorities. And so, if they were attempting to use such a method under one of those authorities, we'd review to ensure that it abided by all applicable legal rules and predicates.

MR. WITTES: Yes, in the back?

MR. LEVINE: Hi, I'm Mike Levine with ABC. Mr. Carlin, so media reports out today are saying that the Justice Department has tapped NSD prosecutor Steve Ponticello to probe the flow of foreign fighters into Syria. I'm wondering if you can talk about what exactly is he going to be looking at, what is he going to be doing, why is this necessary, and who exactly tapped him?

MR. CARLIN: Well, say that the problem of foreign fighters going to Syria is a significant national security threat that we're facing right now. And it's at the top of the agenda for the Department of Justice and the U.S. Government writ large, but also for our European partners and others throughout the world. There's a substantial number of individuals from outside of Syria who are traveling into Syria to commit acts of violent extremism. And just as we were concerned with the conflicts in the Afghanistan/Pakistan region, and with those traveling to Somalia to participate in Al-Shabaab, we're concerned both about those traveling to fight as foreign fighters. And we

need to be concerned, alert, and vigilant to those who may return after committing acts there, with training, with an ideology and desire to commit acts of violent extremism here.

And so we want to make sure that individuals in the counterterrorism section and that U.S. attorneys throughout the country are focused on this threat. And we also want to make sure we work regularly with our partners in Europe and elsewhere to see that we do what we can do to stop the threat.

MR. LEVINE: So what does that mean that he'll be doing, though? In terms of Al-Shabaab, I don't remember a prosecutor being tapped -- sort of lead the effort with that. In similar cases that didn't happen. Why this? Why now? And what is he going to do?

MR. CARLIN: So I think he, in particular, but along with others in the division, are focused on the foreign fighter threat. And it's important to coordinate the different cases across the country to provide relevant expertise that you learn on how to confront this threat. And also then to be available to meet with foreign partners.

MR. WITTES: Sir?

MR. ROMNESS: Hi, my name's Peter Romness. I'm representing myself today, but about a little over a year ago, the Mandiant ATP1 Report came out. What are your thoughts on that? Was that a precursor to what you're doing? Were you already working on this? What are your thoughts on the reaction to that report?

MR. CARLIN: I thought that it was an excellent product, that it was good work that was done and it's important, as we mentioned earlier. And not just that the government's working on these threats, but that the private sector is working on them, as well. And without discussing exactly when our investigation started, it did not start because of the report.

MR. WITTES: Shane Harris, in the back?

MR. HARRIS: Hi. Thanks, Mr. Carlin for being here. You talked about the difficulty of putting these cases together and that they can take years and they have to be -- there's very particular allegations and evidence that's in the indictments. I'm wondering, could you talk a bit about to what extent the victim companies themselves -- and presumably there are many others -- can be useful? And are you reaching out to them to try and encourage them to come forward with information that might be helpful or do you contact them and ask them to participate in the investigations in any way?

MR. CARLIN: So, because this is an open case -- without discussing this case in particular, yes, in general. We at National Security Division, the national security cyber specialists in the field, and our partners at the FBI and other agencies, are definitely reaching out to companies, both to warn individuals about the threat and encourage them to take steps to prevent it from happening, but also to work with them when it does occur. That's critical, that type of partnership. It's critical both so we can learn of the intrusions and take the steps we need to try to protect U.S. companies and it's critical if you're going to try to bring a criminal case to have that sort of cooperation, and to talk to the companies so that you understand what was taken and why it was of importance, what it meant for it to be taken.

MR. WITTES: In the front here?

MR. JIMENEZ: I'm curious how much consideration your department --

MR. WITTES: Please identify yourself to start.

MR. JIMENEZ: Arturo Jimenez, University of California, Irvine. I'm curious how much consideration you gave to the potential consequences of this precedent that you're setting and, especially, you talked about some of the positive consequences, but some of the negative ones, and specifically, so thinking that there's most likely going to be some retaliation in kind, I imagine, either from the Chinese or

other countries. And while the U.S. might make this very clear distinction between economic and national security espionage, others might not.

And so I'm curious if you thought about these potential negative consequences and in worst-case scenario maybe it might lead to a level of legal brinksmanship or lawfare amongst the powerful or something like that. So, I'm curious as to those type of considerations?

MR. WITTES: And just something I might add to that question, for a moment. I imagine the point of view of NSD on this question would be subtly different from the point of view of the intelligence community, which might have some anxieties about the amount of declassification you would have to do to bring a case like this and might similarly be different from the point of view of the State Department, which has to interface with these areas. So, I mean, there's -- everything that the question raises, I imagine plays out in the interagency as you're contemplating something like this, yeah?

MR. CARLIN: I'll say this. In all of our work, criminal prosecution is a tool in the larger set to try to stop threats to the national security. So that's true in terms of stopping the terrorism threat. It's true in stopping the threat from spies in our counterespionage section and it's true in stopping the threat of those who would steal our trade secrets.

And so in each of those instances it won't be the only solution. You won't be able to bring it in every case, but in every other context, it's one of the tools that we have on the table and there's been no unilateral decision to say we'll never bring a criminal case. That should be all the more true when the conduct is such traditional criminal conduct.

And the other thing -- well, as I said earlier, as the Chinese said, bring us hard evidence, evidence that could stand up in a court of this criminal activity. And so,

one hopes and continues to hope that now that we have, that they'll take action to stop this criminal activity. They've never said -- and as I said earlier, I'm not aware of any country that condones this behavior, so now that it's laid out, maybe it will stop.

MR. WITTES: In the back, the very back?

MR. LUGIT: Thanks. Steve Lugit. I work and study here in the city. Thanks a heap, Ben. I appreciate it.

Sir, sort of building on Mr. Jimenez's point and Ben's likewise, this is the largest populated nation in the world; the world's second largest economy in about 20 years, likely by measures -- a number of measures -- the largest economy. Now, they could be trade sanctions, they could be any among a number of routes of retaliation against the United States.

Symbolism is everything, some people say to the VRC, so how broad could the consequences be for bringing these charges against a formidable economic power? Thanks.

MR. CARLIN: We're going to follow specific criminal acts that we find, where they lead. And have been clear that stealing trade secrets from American companies and using it to provide to their companies who are in competition with them is an act that's criminal. And when it occurs inside the United States we'll follow it where it leads. And in this case it lead to five particular individuals who happened to be where they were and happened to have the jobs that they had. And we brought the charges and we laid out the evidence that we had.

And comfortable, that's the proper way to proceed and we're going to continue to follow these cases where they lead.

MR. WITTES: We have time for one more -- wow, I was going to say, one more question, but we actually -- let's get a few people. Let's start with the woman

over there and what we'll do is we'll go around, collect a few, and then we'll give Mr. Carlin a chance to wrap up and address whichever so many of them as he feels inclined.

MS. ZHONG: Hi, I'm Jen Zhong. I go to American University. My question is in regards to the precedents that have been set in white collar crime criminal cases. How does this effect the indictment on this case, especially since these are individuals in the Chinese military? What if -- considering it was their job, how does it effect if they got their instructions from higher ups and how that will effect our Chinese and U.S. relations?

MR. WITTES: Okay, the woman right there and then the gentleman in front of her after that.

MS. SETCH: Hi, I'm Courtney Setch with Real Clear Politics. And this is a bit more of a brag question, but at Director Comey's hearing in front of the Judicial Committee yesterday, he mentioned that there are two types of large American companies: those that have been hacked by the Chinese and those who do not know they have been hacked by the Chinese. Do you expect an overflowing amount of cases to come out now that there are faces put to Blackshades? And if so, how will these cases be divided among all the people working against cyber crime?

MR. MUELLER: Hi, John Mueller from Ohio State and from CATO. Going just to Mr. Wittes' first question, is the United States Government prepared to guarantee that although it does spy on foreign businesses, none of the information gathered makes it into the hands of American businesses?

MR. WITTES: All right, let's add one more, if there is one more. The gentleman in the corner there, and then we'll give Mr. Carlin a chance to wrap things up.

MR. RABIBI: Thanks, Mr. Carlin. Prance Rabibi. I'm an attorney here in D.C. and faculty at Georgetown. I'm curious a little bit about the legal line drawing that

you've been making in discussion throughout between economic espionage and sort of state-driven espionage. As a general matter, how important is it in these cases and cases like it that you're able to make a showing of economic benefit to companies overseas or wherever the case may be?

In particular, how would this look different -- would it look different under the statutes at play here if there was clearly some sort of commercial information taken with no apparent connection to national security, but no real showing that this was going to benefit any particular companies unfairly? How would that change things? I'm just curious as a general matter.

MR. WITTES: All right, the floor is yours. There's a lot of stuff on the table. Have at it.

MR. CARLIN: I suppose I can't just answer yes to all the questions. (Laughter) But in terms of Director Comey's testimony yesterday, I tend to think it's even worse in a way that there are only companies that have been hacked and those that are going to be hacked again. We're just seeing it across the country. And I hope that one consequence of bringing not just this indictment, but others, is that it encourages companies and victims to come forward and to realize that there are steps that we can take. And we won't just watch the activity continue and that we will take however many steps we need to, to make sure that the activity stops and that we won't just leave them out there responsible for their own defenses. And then, as a general rule -- as the President has stated in his Presidential Policy Directive, we do not take information from other people's companies to provide it to our own companies.

On the statutory question, it will depend on which particular prong that you are charging. So, for the particular violation of the Computer Fraud and Abuse Act, or 18 USC 1030, that we charged, it was a prong that was for commercial advantage or

private financial gain. And we charged theft of trade secret, which does not require that you show. It's for a particular foreign company and we charged a prong of the economic espionage. It does have as one of its elements that it's for the benefit of another nation.

MR. WITTES: So we are out of time. Please join me in thanking Mr. Carlin for joining us. (Applause)

MR. CARLIN: Thank you. Thanks again, buddy, for having me.

MR. WITTES: Thanks for coming.

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Carleton J. Anderson, III

(Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2016