THE ASPEN INSTITUTE

ASPEN SECURITY FORUM

CONFRONTING GLOBAL CYBER THREATS

Greenwald Pavilion
Aspen, Colorado

Thursday, July 19, 2018

Clark Ervin: Well, good evening, everyone. You may recall from last night that I am Clark Ervin, the Founder and Chairman of the Aspen Security Forum. I'm very pleased to be with you for our second night in HSC. We are excited to have this session titled Confronting Global Cyber Threats. We're very pleased to have with us tonight as our featured speaker, the Deputy Attorney General of the United States Rod Rosenstein. We're especially pleased that General Rosenstein has chosen the Aspen Security Forum as the venue to make tonight a very important policy announcement in the field of cybersecurity. Having said that, his schedule is such that he cannot take the time for questions afterwards as is the norm, but we're very pleased that he's here. And so afterwards, there would be a panel of cyber experts to comment on the general's remarks.

And so, to moderate that panel, our moderator tonight is David Sanger, an old friend of the Aspen Institute in the Aspen Security Forum in particular, the chief Washington correspondent for The New York Times, a cybersecurity expert himself, and the author of the new book, The Perfect Weapon War, Sabotage, and Fear in the Cyber Age. With that, first of all, please join me in welcoming and thanking the Deputy Attorney General Rod Rosenstein.

Rod Rosenstein: Thank you very much. Good afternoon. It's a great privilege. Thank you. Thank you. Thank you very much. Thank you. Thank you. Thank you. Thank you very much. Thank you. All right, it is nice to get out of Washington every once in a while and it's a great privilege to be here with you, but we meet today at a front moment. For too long along with other nations, we enjoyed the extraordinary benefits of modern technology without adequately preparing for its considerable risks. Director of National Intelligence Dan Coats, who I know was here earlier today, elevated the alarm last week when he stated that the digital infrastructure of this country is literally under attack. That's one of the few instances where the word literally is used literally and accurately. Our adversaries are developing cyber tools, not only to steal our secrets and to mislead our citizens but also to disable our infrastructure by gaining control of computer networks.

Every day, malicious cyber actors infiltrate computers and accounts of individual citizens, businesses, the military, and all levels of government. Director Coats revealed that our adversaries target government and businesses in the energy, nuclear, water, aviation, and critical manufacturing sectors. They cause billions of dollars in losses, they pre-positioned cyber tools for future attacks, and they tried to degrade our political system. So combating cybercrime and cyber-enabled threats is a top priority of the Department of Justice. Attorney General Sessions established a Cyber-Digital Task Force in February and he challenged it to answer two questions. What are we doing now to address cyber threats and how can we do better? Today, the Department of Justice is releasing a report that responds to the first question, providing a detailed assessment of the cyber threats confronting America and the Department's efforts to combat them.

The task force report addresses a wide range of issues including how to define the multi-faceted challenges of cyber-enabled crime, how to develop strategies to detect, deter, and disrupt them; how to inform victims in the public about the threats they face, and how to maintain a skilled workforce to detect and to respond to cyber threats. The report describes six categories of cyber threats and explains how the Department of Justice is working to combat them. One serious type of threat involves direct damage to computer systems such as distributed denial-of-service attacks and ransomware schemes. Another category is data theft which includes stealing personally identifiable information and intellectual property. The third category encompasses cyber-enabled fraud schemes. A fourth category includes threats to personal privacy such as extortion, blackmail, and other forms of harassment.

Attacks on critical infrastructure constitute the fifth category. They include infiltrating energy systems, transportation systems, and telecommunications networks. Each of those complex and evolving threats is serious and the report details the important work the Department of Justice is doing to protect America. I plan to focus today on a sixth category of cyber-enabled threats malign foreign influence operations which are described in chapter one of the task force report that I know the panel is prepared to discuss following my remarks. The term malign foreign influence operations refers to actions undertaken by a foreign government often covertly to influence people's opinions and advance the foreign nations strategic objectives. The goals frequently include exacerbating social divisions and undermining confidence in Democratic institutions.

influence operations are a form of information warfare. Covert propaganda and disinformation are the primary weapons. The Russian effort to influence the 2016 presidential campaign is just one tree in a growing forest, focusing merely on a single election, misses the point. As Director Coats made clear, these actions are persistent. They are pervasive. They are meant to undermine democracy on a daily basis regardless of whether it is election time or not. Russian intelligence officers did not stumble on the idea of hacking American computers and posting misleading messages because they had a free afternoon. It's what they do every day, not just attacking America but other countries as well. This is not a new phenomenon. Throughout the 20th century, the Soviet Union used malign influence campaigns against the United States and other countries.

In 1963, for example, the KGB paid an American to distribute a book, claiming that the FBI and the CIA assassinated President Kennedy. In 1980, the KGB fabricated and distributed a fake document, claiming that the National Security Council had a strategy to prevent political activists from working with African leaders. During the Reagan Administration, the KGB spread false stories that the Pentagon developed the AIDS virus as part of a biological weapons research program. As Jonathan Swift wrote in 1710, "Falsehood flies, and the truth comes limping after it." The Reagan Administration confronted the problem head-on. It

established an interagency committee called the Active Measures Working Group to counter Soviet disinformation. That group exposed Soviet forgeries and other propaganda, a modern technology vastly expands the speed and effectiveness of disinformation campaigns.

The internet and social media platforms allow foreign agents to spread misleading political messages while masquerading as Americans. Homeland Security Secretary Kirstjen Nielsen explained last weekend that our adversaries use social media, sympathetic spokespeople, and other fronts to sow discord and divisive among the American people. Elections provide an attractive opportunity for foreign-influenced campaigns to influence our political processes. According to the intelligence community's assessment, foreign interference in the 2016 election demonstrated a significant escalation and directness, level of activity, and scope of effort compared to previous operations. The Department's Cyber-Digital Task Force report contributes to our understanding by identifying five different types of malign influence operations that target our political circumstances.

First malicious cyber actors can target election infrastructure by trying to hack voter registration databases and vote tallying systems. In 2016, we know that five foreign cyber intruders targeted election-related networks in as many as 21 states. There's no evidence that any foreign government has ever altered vote totals, but the risk is real. Moreover, even the possibility that manipulation may occur can cause citizens to question the integrity of elections. Second, cyber operations can target political organizations, campaigns, and political officials. Foreign actors can steal private information through hacking and publish it online to damage a candidate, campaign, or political party. They can even alter the stolen information before they release it. Russia's intelligence services conducted cyber operations against both major political parties in 2016 and the recent indictment of Russian intelligence officers alleges a systematic effort to leak stolen information about one campaign.

The third category of malign influence operations affecting elections involves offers to assist political campaigns or officials by agents who conceal their connection to a foreign government, such operations may entail financial and logistical support to Americans who are unwitting or unaware of the foreign connection. Fourth adversaries covertly use this information and other propaganda to influence American political opinion. Foreign trolls spread false stories online about candidates and issues, amplify divisive political messages to make them appear more pervasive and credible and try to pit groups against each other. They may also try to affect voter behavior by triggering protests or depressing voter turnout. Finally, foreign governments use overt influence efforts such as government controlled media outlets and paid lobbyists.

Those tactics may be employed lawfully if the foreign agents comply with registration requirements, but people should be aware when lobbyists or media outlets are working for a foreign government so they can evaluate the source's

credibility. When respected figures offer opinions about public policy issues, it may matter to know that they are taking instructions from a foreign government. The election interference charges filed in February, demonstrate how easily human trolls can distribute propaganda and disinformation. A Russian man not charged in the case recently admitted to a reporter that he worked with the trolls in a separate department. His job was to create fake news for his own country. He felt like a character in the book 1984 by George Orwell, a place where you have to write that black is white and white is black.

You were in some kind of factory that turned lying into an industrial assembly line. The volumes were colossal. There were huge numbers of people, 300 to 400, and they were all writing absolute untruths. When a man took a test for promotion to the department that focused on America, he explained the main thing was showing that you are able to represent yourself as an American. That former troll said that he believes Russian audiences pay no attention to fake internet comments, but he has a different opinion about Americans. He thinks that we can be deceived because Americans "aren't used to this kind of trickery". That remark is sort of a compliment. I say that because in repressive regimes, people simply assume that the government controls media outlets and they discount everything.

We live in a country that allows free speech. So people are accustomed to taking it seriously when their fellow citizens express their opinions, but not everyone realizes that information posted on the internet may not even come from citizens. Moreover, internet comments may not even come from human beings. Automated bots magnify the impact of propaganda. Using software to mimic actions by human users, bots can circulate messages automatically, creating the appearance, the thousands of people are reading and forwarding information within minutes. Together, bots and networks of paid trolls operating multiple accounts allow foreign agents to quickly spread disinformation and create the false impression that it is widely accepted in America. The United States is not alone in confronting malign foreign influence operations.

Russia reportedly conducted a hack and release campaign against President Macron during last year's French elections and instituted similar operations against political candidates and other European Democracies. Other foreign nations besides Russia also engage in malign operations. So what can we do to defend our values in the face of foreign efforts to influence elections, weaken the social fabric, and turn Americans against each other? Like terrorism and other national security threats, the malign foreign influence threat requires a unified strategic approach across all government agencies. In particular, the Departments of Justice, Homeland Security, State, Defense, Treasury along with intelligence agencies and others play important roles. But other sectors of society also need to do their part. State and local governments must secure their election infrastructure.

Technology companies need to protect their platforms. Public officials' campaigns and other potential victims need to study the threats and protect themselves and their networks. Citizens need to understand the playing field. The Department of Justice investigates and prosecutes malign foreign influence activity when it violates federal criminal law. Some critics argue against prosecuting people who live in foreign countries that are unlikely to extradite their citizens. I think that's a short-sighted view. For one thing, the defendants may someday face trial if there's a change in their government, or if they visit any nation that cooperates with America and enforcing the rule of law. A modern forms of travel and communication readily allow criminals to cross national boundaries. Do not underestimate the long arm of American law or the resolve of American law enforcement.

Thank you. There are plenty of people who thought they were safely under the protection of foreign governments when they committed crimes against America, but they later find themselves in American prisons. Second, public indictments achieve specific deterrence by impeding the defendants from traveling the rule of law nations and by raising the risk that they will be held accountable for future cybercrimes. Wanted criminals are less attractive as employees and co-conspirators. Third, demonstrating our ability to detect and charge hackers will deter. It will deter some others from attacking America. Fourth, federal indictments are taken seriously by the public and the international community. We respect for our criminal justice system including an understanding of the presumption of innocence and the burden of proof beyond a reasonable doubt means that our willingness to present evidence to a grand jury and ultimately a trial elicits a high degree of confidence in our allegations.

Fifth, victims deserve vindication particularly when they are harmed by criminal acts that would normally be prosecuted if the perpetrators were located here in the United States. Sixth, federal criminal prosecutions support other penalties for maligned foreign influence operations. For example, the Department of Treasury can impose financial sanctions on defendants based on evidence exposed in indictments. Voters and foreign democracies and influential citizens in autocratic regimes can consider these allegations in making decisions about their national leadership and foreign alliances. The Department of the Treasury imposed sanctions on the individuals and entities identified in our February election interference indictment along with others involved in malign influence activities. 19 individuals and five entities are subject to sanctions that freeze assets under American jurisdiction which I remind you is vast.

Even if those people are never brought to court, they will face consequences. The sanctions prohibit them from engaging in transactions with Americans and using the American financial system. The administration followed up with similar sanctions for a broad range of malign activities against seven oligarchs, 12 companies, 17 Russian government officials, and two other entities. So prosecutions are one useful tool against modern criminals who operate beyond

our shores. That same approach applies outside the context of election interference. That's why our government regularly files charges against criminals who hide overseas such as the Iranian government hackers who infiltrated, who broke into a computer network of a dam. The Iranian hackers who infiltrated American universities, businesses, and government agencies on behalf of the Islamic Revolutionary Guard Corps, the Iranian hacker who infiltrated and extorted an American television network, the Chinese government hackers who committed economic espionage, and Russian intelligence officers who stole data from an email service provider.

Intelligence assessments and criminal indictments are based on evidence. They do not reflect mere guesses. Intelligence assessments, of course, include analytical judgments based on classified information that cannot be disclosed because the evidence is from sources, people who will be unable to help America in the future if they are identified, and who might be harmed in retaliation for helping America, and intelligence methods techniques that would be worthless if our adversaries knew how we obtained the evidence. Indictments are based on credible evidence that the government must be prepared to introduce in court if necessary. Some people believe that they can operate anonymously through the internet, but cybercrime generally does create electronic trails that lead to the perpetrators if the investigators are sufficiently skilled.

Gathering intelligence about our adversaries, people who threaten our way of life is a noble task. Outside the Department of Justice headquarter is just outside my window, stands a statue of Nathan Hale. Hale was executed immediately without a trial after he got caught gathering intelligence for America during the Revolutionary War. His final words are recorded as follows. "I am so satisfied with the cause in which I have engaged, that my only regret is I have but one life to offer in its service." Thank God that America is blessed by such patriots and rest assure that Director Wray, Attorney General Sessions and I will never shirk our duty to protect them from retaliation. The days when criminals could harm America from abroad without fear of consequences are past. If foreign governments choose to give sanctuary to perpetrators of cybercrimes, those governments will need to take responsibility for the crimes and the individual perpetrators will need to consider the personal cost.

But criminal prosecutions and financial sanctions are not a complete solution. We need to take other steps to prevent malign influence. To protect elections, the first priority is to harden our infrastructure. State governments run American elections and are responsible for maintaining cybersecurity, but they need federal help. The Department of Homeland Security takes the lead in helping to protect voting infrastructure and the FBI leads federal investigations of intrusions. The FBI works closely with Homeland Security to inform election administrators about the threats. DHS and FBI provide briefings to election officials from all 50 states about our foreign adversaries, intentions, and

capabilities. We don't want to wait until after the fact. We want to make sure we give the adequate warnings in advance to try to deter and prevent harm.

We also seek to protect political organizations, campaigns, candidates, and public officials. The FBI alerts potential victims about malicious cyber activities and helps them respond to intrusions. It shares detailed information about threats and vulnerabilities. To combat covert foreign influence on public policy, we enforce federal laws that require foreign agents to register with the US government. Those laws prevent people from tricking unwitting Americans while concealing that they are following orders from foreign government handlers. The Department of Justice is stepping up enforcement of the Foreign Agents Registration Act and related laws and we are providing defensive counterintelligence briefings to local state and federal leaders and candidates. Public attribution of foreign influence campaigns can help to counter and mitigate the harm caused by foreign sponsored misinformation.

When people are aware of the true sponsor, they can make better informed decisions. We also help technology companies to counter covert foreign influence efforts. The FBI works with partners in the intelligence community to identify foreign agents as they establish their digital infrastructure and as they develop their online presence. The FBI helps those companies disrupt foreign influence operations by identifying the activities so the companies may consider the voluntary removal of accounts and content that violate their terms of service and deceive their customers. Technology companies bear primary responsibility for securing their products from misuse. Many are now taking greater responsibility for self-policing including by removing fake accounts. We encourage them to make it a priority to combat efforts, to employ their facilities for illegal schemes.

Even as we enhance our ability to combat existing forms of malign influence, the danger continues to grow. Advancing technology will enable adversaries to create propaganda in new and unforeseen ways. Our government must continue to identify and counter them. Exposing schemes to the public is an important way to neutralize them. The American people have a right to know if foreign governments are targeting them with propaganda. In some cases, our ability to expose foreign influence operations may be limited by our obligation to protect intelligence sources and methods and defend the integrity of investigations. Moreover, we should not publicly attribute activity to a source unless we possess high confidence that foreign agents are responsible for. We also do not want to unduly amplify an adversary's messages or impose additional harm on victims.

In all cases, partisan political considerations must play no role. We cannot seek to benefit or harm any lawful group individual or organization. Our government does not take any official position on what people should believe or how they should vote but it can and should protect them from fraud and deception perpetrated by foreign agents. Unfettered speech about political issues lies at

the heart of our Constitution. It's not the government's job to determine whether political opinions are right or wrong, but that does not leave the government powerless to address the national security danger when a foreign government engages in covert information warfare. The First Amendment does not preclude us from publicly identifying and countering foreign government propaganda. It's not always easy though to balance the many competing concerns in determining whether when and how the government should disclose information about deceptive foreign activities relevant to elections.

That challenge calls for the application of neutral principles. So the Cyber-Digital Task Force report identifies factors the Department of Justice should consider in determining whether to disclose foreign influence operations. That policy reflects an effort to articulate neutral principles so that when the issue that the government confronted in 2016 arises again, as it surely will, there will be a framework to address it. Meanwhile, the FBI's operational foreign interference task force coordinates investigations of foreign influence campaigns. That task force which I know Director Wray spoke about yesterday, integrates the FBI's cyber counterintelligence, counter-terrorism, and criminal law enforcement resources to ensure that we understand the threats and respond appropriately. The FBI task force works with other agencies, federal state and local as well as international partners and the private sector.

Before I conclude, I want to emphasize that covert propaganda disseminated by foreign agents is fundamentally different from domestic partisan wrangling. As Senator Margaret Chase Smith proclaimed in her famous 1950 Declaration of Conscience, "We must address foreign security threats patriotically as Americans and not politically as Republicans and Democrats." President Reagan's Under Secretary of State Lawrence Eagleburger wrote about Soviet active measures in 1983. He said that and I quote, "It is as unwise to ignore the threat as it is to become obsessed with the myth of a super Soviet conspiracy, manipulating our essential political processes."

Eagleburger maintained that free societies must expose disinformation on a persistent and continuing basis. Over the past, year Congress passed three separate statutes, encouraging the executive branch to investigate expose and counter malign foreigns influence operations. Publicly exposing such activity has long been a feature of US law. The Foreign Agents Registration Act which Congress passed in 1938 to counter Nazi propagandists, mandates that the American public know and foreign governments set out to influence them. Knowledge is power. In 1910, Theodore Roosevelt delivered a timeless speech about the duties of citizenship and great republics.

PART 1 OF 3 ENDS [00:29:04]

Rod Rosenstein: ... about the duties of citizenship and great republics. It is best known for his remark that it is not the critic who counts which is important to keep in mind when you're in Washington D.C., but Roosevelt's most insightful observation is

that the success or failure of a republic depends upon the character of the average citizen. It is up to individual citizens to consider the source and evaluate the credibility of information when they decide what to believe. Heated debates and passionate disagreements about public policy and political leadership are essential to democracy. We resolve those disagreements at the ballot box. And then we keep moving forward to future elections that reflect the will of the citizens.

Foreign governments should not be secret participants covertly spreading propaganda and fanning the flames of division. The government plays a central role in combating maligned foreign influence and other cyber threats. The attorney general's cyber digital taskforce report demonstrates that the Department of Justice is doing its part to faithfully execute our oath to preserve, protect and defend America. I regret that my time today is insufficient to go into great detail about that report. It is available on the Department of Justice website. I hope you will read it and find it to be a useful contribution to public discussion about one of the momentous issues of our time.

In brief, the taskforce report explains that we must continually adapt criminal justice and intelligence tools to combat hackers and other criminals. Traditional criminal justice is most often characterized by a police officer chasing a criminal and an eyewitness pointing out a perpetrator in the courtroom. A cybercrime requires additional tools and techniques. We limit cybercrime damage by seizing or disabling servers, domain names and other infrastructure that criminals use to facilitate attacks. We shut down dark markets where cyber criminals buy and sell stolen information. We restore control of compromise computers. We share information gathered during our investigations to help victims protect themselves.

We pursue restitution and we seek attribution and accountability for the perpetrators and we expose governments that defraud and deceive our citizens. The taskforce report is just one aspect of our efforts. It is a detailed snapshot of how the Department of Justice assesses and addresses cyber threats. That work continues and not just within our department. Our government is doing more now than ever before to combat cyber enabled crimes.

Trump administration agency appointees and White House officials work with career professionals every day to prevent cybercrime and protect elections. Our adversaries will never relent in their efforts to undermine America, so we must remain eternally vigilant in the defense of liberty and the pursuit of justice. And we must approach each new threat united in our commitment to the principle reflected in the motto adopted at the founding of our republic. E pluribus unum. Thank you very much.

David Sanger: Thank you. Do I need to be plugged in there then?

Speaker 1: I think you're live.

David Sanger: Okay great. Well, good afternoon. Welcome to another glorious afternoon in Aspen. You'll discover that when you go back home and you tell everybody that you had to sit through these lengthy seminars and stuff, there's going to be a distinct absence of sympathy so sort of prepare yourself now. We've got a great panel to pick up where the Deputy Attorney General left off. I thought it was a really fascinating speech and actually I think it's the first speech I've certainly heard during the Trump administration devoted entirely to the maligned influence issue and I think it gives us a chance to talk about the elements of that and we have the perfect panel to go do that with.

So, to your far right, my far left, Greg Clark from Symantec, a cyber security that I've grown to really respect and rely on. Those of you who saw the documentary Zero Days saw a few of Greg's great employees at work remarkably pulling apart with great accuracy the Stuxnet virus. And really with their work we came to understand where the authors were and what that was headed towards.

Greg Clark: Thank you for the great reporting on that.

David Sanger: Thank you. And in the center here, Tom Bossert who was until just a few months ago the Homeland Security Advisor and oversaw cyber issues in the White House. Tom was persuaded to come out here because the secret vice that he never got to do in the White House was fly fishing. I realized that he and I were going to get along really well one day when I went down into his underground basement office and as we're sitting there talking for the first time I said, that's an Orvis Practice rod you have in the corner. Missing from Lisa Monaco's same office was an Orvis Practice rod.

Lisa Monaco: That's true.

David Sanger: However-

Lisa Monaco: It also would have been taller than me.

David Sanger: That's true. But the office has an extremely low ceiling and I didn't realize that because I was used to Fran Townsend and Lisa in that office and then along came Tom. Lisa was the Homeland Security Advisor. Was in the Obama administration from start to finish in various roles. Taught me a huge amount about some of the challenges that we're going to be discussing today. And I would say ranks among the nation's greatest experts and wisest voices on these issues, so it's great to be here with all three of you.

Lisa, let me start with you and ask you to wind the clock back. When we all think of cyber issues right now, we're thinking Russian hack, the election and so forth. But when you and I were talking about these things back in the midst of the Obama administration, I would say that the maligning influence operations and information operations was pretty low on the agenda. People were thinking

about the cyber Pearl Harbor issues that Leon Panetta was talking about. The hack that unplugs from Boston to Washington or San Francisco to LA.

We were talking about data manipulation but usually in a kind of military and targeting sense. I don't remember much discussion at that time of the vulnerabilities of the election system. And one of the arguments that I came upon as I've been doing writing and research on this both for newspaper work and for my book, were people asking the question, were we so fixated on the big hack, the one that unplugs the country, that we missed some of the more subtle uses that you heard the Deputy Attorney General talking about today.

In other words, that our radar was just sort of pointed in a different direction. Or is that an unfair critique of how we got here?

Lisa Monaco: So, let me go to your question but first take a little bit of first panelist prerogative to say a few words about the speech we just heard.

David Sanger: Great. Yeah.

Lisa Monaco: And the report that the Deputy Attorney General laid out 'cause I think it's important context too to have for our further discussion. I think Rod gave us a very good lay down and a very important lay down on the types of foreign influence operations that happen, the tactics and the techniques. And the very, very important role ... and I'm biased here because before going to the White House I spent 15 years in the Justice Department and in the part of that time in the FBI. So, I am very biased when it comes to my belief in the important role that the justice department plays in meeting new and evolving threats to our national security.

So the context I wanted drawn ... I will get to your question, is I think Rod did a very good service here in laying that out. And making clear that the Justice Department has a very important role in meeting those new and evolving threats and doing so consistent with the rule of law and with our values. The thing ... the context I want to draw here is what's really important in addition to the important neutral principles that he laid out which by the way were all principles that were at play and that we drew upon and evaluated in the decisions that we made and the challenges we faced in the run-up to the 2016 election.

But those principles have to reside somewhere. And they have to be evaluated and used in a framework that resides somewhere. And I would argue they reside in institutions that are governed by in a bipartisan way, one would hope, which is why I think it was very disappointing what we saw in Helsinki and the undercutting of the intelligence community and the law enforcement community. So, I guess what I hope we can also get to today is how important it is to have those neutral principles be operationalized in institutions that are

supported in a bipartisan way. That are grounded in the rule of law and that are led by leaders who are really focusing on that.

Now, to your question. I think that some of that criticism is fair. We heard a lot about the cyber Pearl Harbor. I would argue that the main cyber threats that we faced over my last 10 years in government did trace a steady evolution, right? From destructive attacks from efforts to disrupt public-facing websites. Those of you from the financial services here will remember the summer of 2012 and 2013 with a pit in your stomach. To also though, the first signs of using this hack and release which I really liked the phrase that Rod used, in the Sony hack, right? So there-

David Sanger: Which was also a destructive hack and a hack and release.

Lisa Monaco: Exactly right. So there, that was really it was both destructive and it was coercive, right? So one-

David Sanger: To remind those of you in the audience who may forget this was the attack attributed to North Korea by the Obama administration to try to stop a movie being distributed called The Interview that imagined the assassination of Kim Jong Un. A really bad movie, we'll add to that.

Lisa Monaco: Right. So that was coercive, right? And that was the use of cyber tools to try and coerce our free expression, really, right? To not have people go see that movie. Now, so I would argue that we've seen that escalation. But, as the intelligence community assessment laid out in January of 2017, what we saw in 2016 was a significant escalation and the change here was the weaponization of the information that was stolen from the DNC and other things. And frankly, the abuse and misuse and distribution of false information on social media platforms. We know a lot more about that now than we did then.

So, I don't think we were totally blind to the evolution of the cyber threat and the different tools that were being used. We saw this escalation, but when it comes to the attacks in the election infrastructure, we worked very closely to combat that and we'll get into the decisions we made on that and to help the states push back against that and to protect the actual integrity of the vote count. When it came to the manipulation of social media platforms, that was a new piece that we did not have sufficient visibility into.

David Sanger: Okay. One more for you just following up on the Deputy Attorney General's speech. He raised the attribution problems and this'll take us in a moment to Greg whose company does such interesting work there. But, one of the difficulties here is, if you had had an individual Russian taking out those Facebook Ads and even advertising for Texas succession which was one of the ads. Or the Hillary Clinton ad that showed Satan. But was an individual who you couldn't really establish was working for the government, we wouldn't really have much of a cash would we? So, we've got design these rules in such a way

that individual foreigners don't feel like they can never express an opinion on the internet about our elections. We're trying to get rid of state's from interfering. And sometimes you don't really have the fidelity to know what's a state actor versus what's a patriotic actor.

Lisa Monaco: Sure, this is ... that's one aspect of the attribution challenge which I would argue we're getting a lot better at. And great good work has been done in the last couple of years to continue and accelerate what we did in the Obama administration which was to basically employ a framework that said we're going to pool all the intelligence we can. Law enforcement, signals intelligence, human source intelligence, you name it, to understand the cyber threat. Make sure we understand who done it and then call that out consistent with the obligations we have to protect our sources and protect our national security. And then make a decision about how to impose costs.

And then very importantly, when you impose those costs, all tools ought to be on the table. I liken it to the approach that we took to combating and continue to take to combating the terrorism threat. We need to understand it as an intelligence challenge. But we need to be willing to use law enforcement tools, intelligence, military, diplomatic, financial sanctions. All of those ought to be on the table and I think you've seen a steady drumbeat of the use of all of those tools against malicious cyber actors.

David Sanger: So, Tom when you came in, you arrived in the midst of this hubba about whether or not there was election interference.

Thomas Bossert: Hubbub.

David Sanger: Hubbub. Let's say political firestorm.

Thomas Bossert: No, I like it.

Lisa Monaco: Hubbub.

David Sanger: Yes, hubbub. And we read this morning that the President, of course, had when we knew this at the time, had received a pretty good lay down as President-elect about why the intelligence community came to the conclusions that they came to. That in fact the Russians had interfered. His initial instinct though was not to say establish a national commission to learn lessons from the 2016 election and apply those later on. He did establish a commission but it was a commission to figure out what happened to the three million fraudulent votes.

You however, put together a pretty impressive team. As far as I could tell, perhaps while it wasn't characterized like that, picked up many of the initiatives that you just heard Lisa describe. Extended a few. You named two countries, North Korea and Russia for two big hacks last year. WannaCry and NotPetya. But tell us what the White House view was and particularly your operations view

was about what needed to get done in the malign influence arena that we've just heard from the Deputy Attorney General.

Thomas Bossert: Well let me begin the time frame to the left a little. Okay? I think this is a good story for the three of us and maybe for you as well. I entered the hubbub in the Bush administration and took a lot of the work from Richard Clarke who might be here. I'm struck by the degree of continuity and patriotism experience in this room and evidenced by the heat you're still here. I want to start by saying a little transition story.

I got a bottle of wine. That was the only thing in my office when I sat down on day one and I'll come back to it. But, I got an opportunity to take the hand off her baton from the Obama administration from Lisa into the Trump administration in that position. It took me about 10 years to get promoted 10 feet. I had been the deputy under President Bush. But when I handed the baton from Bush to Obama I handed it to Lisa as well. And to John Brennan. And just a little level setting.

At that time the phone call I got was from then-FBI Director Mueller with then-Chief of Staff Lisa Monaco saying, "The Chinese have hacked the McCain campaign and the Obama campaign." That was a foreign government using cyber tools directly, right? Very similar but this happened then. This isn't known.

David Sanger: They didn't make it public. They were doing it as an espionage operation.

Lisa Monaco: As I recall other people made it public.

David Sanger: Yes, it's my recollection now.

Thomas Bossert: I did say this is a story for the three of us. And so, we did a good job of keeping that quiet and we did what we needed to do to get the campaign staff to understand the threat. I don't agree with your contention that they kept it quiet. I don't know what they did with it. In fact, I don't know what they might have done with it. And if you were any of you on the short to be a senior executive in that administration, and that was kept in an electronic fashion in those databases, your house was subject to surveillance. Your life was subject to some invasion prior to you even knowing that you were being considered.

So, I think there was a significant influence effort going on there. I think there was a significant influence risk there and so to go back I'm going to take your prerogative. Thank Rod for what he did. I thought that speech was spot on because he said knowledge is power and I'm having a hard time in 30-second soundbites explaining what's in that long report. So read it because education's what we need to get in this new area of vernacular.

So let's just, if we set it here because I'll come back to my wine. It's a little warm in here. It was a little warm during that hubbub literally and figuratively. And as I

got into my office nervous on day one, the gift that Lisa gave me was a bottle of wine with the label The Hot Seat.

Lisa Monaco: I passed it on. Somebody had given it to me so I hope you haven't opened it 'cause I'm sure it's really bad.

Thomas Bossert: I will pass ...

Lisa Monaco: I wanted to give it to you, that's the reason I didn't open it.

Thomas Bossert: It is temptation as it sits on your shelf in that job. So, the hot seat that I occupied to answer your question directly, didn't start with a cold President. I was in that room and there's now a lot written about it again by another similar author. The President received that briefing. It was serious. It was comprehensive. In some cases it's now the four people that are the witnesses for the prosecution against him in some fashion. But it was, I thought, a professional briefing. It wasn't Trump being resistant. I think all four of them have gone out and said that at that point they were happy to see the way he received the information and asked some questions.

Somebody, perhaps Director Brennan, I don't want to take too much issue with him, suggested there were no questions asked in that meeting about how we can protect our country. That's the flavor of your question. I contest that. I asked at least five in that session. And the President asked-

David Sanger: You're talking about the session in Trump Tower?

Thomas Bossert: In the session in Trump Tower, yeah. So, the President wasn't cold and we talked about it for hours that day after and for hours thereafter in multiple different sessions. I did have the opportunity to give him a little update from those lessons that we learned. So we weren't failing to look at the problem of cyber security. We weren't failing to look at the potential for information campaign. They're different in some way. I thought we were on top of it as a government.

But I'm going to take one last maybe controversial position here. I don't think it's the government's job and it'll never be the government's full mandate in this country with its size and complexity, to provide for the centralized collective defense of every system, every piece of data, every network connected to the internet. It is not possible under our form of government. And so when you start from the premise, especially the quiet or unstated premise of what are you doing to defend me, you fail to recognize that it's a broader problem.

And even in our daily lives we don't say did the secretary of defense prevent me from being mugged or robbed. There's a larger set of responsibilities and it's not meant to shirk responsibility, but it should level set this conversation.

David Sanger: Well, we'll come back to that because elections because it's a state function pose a particularly difficult issue here. Because you can't have private firms usually take-

Thomas Bossert: Perhaps but as we shift here, I got in trouble for saying at some point just 'cause it was alliterative, but the difference between the DNC and the Dairy Queen, right? What I meant by that is they're all using the same software that has the same vulnerabilities with the same exploits. And so the intent of the attacker matters, but the ability to protect that system-

David Sanger: Does not.

Thomas Bossert: ... does not.

David Sanger: So, it may not be the government's job to protect everybody, but it's Symantec's job.

Thomas Bossert: That's right.

Greg Clark: We're definitely on the call face that's for sure. So, a couple of thoughts for you. I think the speech had some good points in it. If you could summarize one thing, democracy requires safety. We have to be safe. You have to be able to not fear having a contrarian position to the current seating government. There has to be a rule of law. We're in an era now where democracy requires cyber safety. And that is a serious item. And it's nodding for everybody in the room. All of us. All of society.

Cyber safety is essential for democracy. What I liked about today was there was a list of things that happen that need to be sorted out in order for us to have cyber safety to have a democracy for centuries that has now got a dimension of cyber space in it. Social media, all those pieces. So, it is great to see a start on a definition and a set of folks that are working that problem in the government.

The other thing which is absolutely necessary is we had a discussion about consequences. Okay? And if you're overseas and you think you can continue to execute crimes on American civilians, American democratic process, any multinational company without consequences, this is a crisis. And what we heard today was we got consequences. We're starting to lay track on serious consequences using the power of the United States of America.

And for that, we should applaud the improvement in our government. Okay? Now, let's get to the call face of how we actually shut some of this stuff down. I get to see a lot of stuff. We are an incident responder as we say in cyber defense. So we go to the cybercrime scene. And when you show up at the crime scene at a place like the many breaches like Sony that mentioned before, plenty of others. The distress and the damage that is done to those corporations and to those individuals, is emotionally disturbing, right?

These people have worked for years to build these companies and they're getting burnt down by some criminals and it is ridiculous. If you get on the identity protection call center at LifeLock, which is one of our products, the distress of an American citizen that is leveraged up on the credit and now has a debt collector calling because someone got a new credit card, someone took out a second mortgage, somebody bought a car that wasn't them, is disturbing. These people are often crying. They don't know what to do.

And that's the call face of cybercrime. And the effect it has on our society. People estimate it's 2 or 3% of GDP. Where does that amount of money go? Okay. That is a bulk amount of money that's leaving normal society into the hands of these criminals and somehow getting processed through the economy and turned into liquidity. So, we have a crisis and I think it is something that is really essential that we just continue to step up awareness. I don't really know that partnership is the right word, but collaboration between like-minded individuals. Between government organizations. Civilian organizations like Symantec and many of the others that are here sponsoring the event and plenty of others.

And I'll tell you when WannaCry and Petya showed up, we were on the phone with our counterparts from the government. "Hey guys, this is a problem. It's wiping out the world." All of our competitors and us, on same side of the table. "What do you know? How do we fix it? What do we got to do?" And the government big time helping. And I think that was a sea change. What happened around that WannaCry malware and the relationship between private industry and government, was fantastic.

And what I think was really important about the speech today, was that we have a very good start on the problem. And when I'm building a new product at Symantec or we're on a new mission, I just say let's just get it started. Let's get some smart people on it. Let's get some good customers and partners. And let's follow it around and hunt it down and solve it.

David Sanger: Greg, let me ask you one quick question that sort of follows the point that Tom and Lisa were making. So-

PART 2 OF 3 ENDS [00:58:04]

David Sanger: ... was the point that Tom and Lisa were making. You were there through LifeLock and your other products to take care of that 85% or 90% of the criminal activity, the harassment activity, and so forth. Similar to how we're all expected to have locks on our doors and alarm systems and insurance for the household goods, we don't expect the government to protect us against every risk that's wandering out in the mean streets of Aspen, Colorado. But there is a line at which we expect the government to step in. There's nothing you're going to do to your house to protect it from an incoming intercontinental ballistic missile, right? We're expecting the US government to go handle that problem. And what

Rod was discussing today, the general discussion today, was one, not the only, state sponsored activity where you're worried about what it is the government's going to do to stop another government from stepping in. And setting that line, it strikes me, has been a really hard struggle for lots of good reasons. And so I want each one of you to talk about that. We'll start with you, Greg.

Greg Clark: My point of view on that is there isn't like there is in the conventions around kinetic warfare. There is a bunch of rules around what constitutes an act of war. There are not in cyberspace. That has to change.

David Sanger: Because most of what we're seeing is short of war activity.

Greg Clark: But I'll tell you, some of the things that we have reported on, like nation state actors in the control side of power stations, people on the bad part of satellite control systems, these things are serious items. If you look at the nuclear treaties, messing with satellites is a red line in those treaties. So I think this is something that all of the nations in the world have to get behind. It's a hard problem to solve. It's going to take a lot of international work. The right words, I don't know. This is where you guys.

Lisa Monaco: International norms, and that takes international leadership and that takes US leadership, I would argue, to really lead the discussion on what is unacceptable in cyberspace. And so through a lot of work over the last several years, we tried to really drive the discussion in every international fora we could on cyber norms. You think about the G20 is really about economic issues. UN has some other for it. There was no, and there is still today, no one international fora that is really focused on cyber norms and accepted behavior for the international community in cyberspace. And to really advance that discussion, you really need US leadership.

Greg Clark: And you need the president behind that leadership as well.

Lisa Monaco: That's what I mean when I say US leadership.

Thomas Bossert: I've got to jump in here because this is a great opportunity for me to draw a stark line between you and I, which doesn't happen very often, and it also happens to fall along the lines of the larger debate we're having with this presidency and the last one. I firmly believe it in this case, I don't know if I extrapolate it to the world, but I think we will never get where we need to get in this new world moving very quickly of digital risk, by going through these multilateral processes. Ultimately I'd like to see multilateral agreement. I'd like to see a world where we all have an open internet and share those shared norms that you're seeking as an end state. But I think we need to start playing a little jazz music and we need to start acting as United States of America.

In other words we need to improvise because there is no playbook. We need to do it on our own in interests that protect ourselves and ideally do it in bilateral

engagements. I set out to do it that way. I set out first by entering into a bilateral arrangement with Israel. And I subsequently entered into a few others on behalf of the president. He was engaged and aware of all of those things. Authorizing me as far as meeting with foreign heads of state. He wasn't the best guy to sit with the foreign head of state. He was more than comfortable having me do that. And some of those bilateral arrangements we keep quiet. Some of them led to, I think, impressive, exquisite responses to the NotPetya activity and I think that the United States is going to have to lead on that front or we're all going to end up 5, 6, maybe 15 years from now saying, "Boy, I'd like to have some agreement in a UN body. How are we going to attribute and punish somebody and there's a veto vote from the guy that led the hack?"

Lisa Monaco: See, I think that's a completely false distinction. I think this is not an either or. Right? You need to have, at some level, an ability to isolate malicious actors. Right? So you have to have some agreement and some consensus amongst international community about what is unacceptable. That does not mean you should not engage in bilateral discussions. Case in point...

David Sanger: In arms control we do both.

Lisa Monaco: That's true, but I'm going to draw to the cyber point. Which is to say, it was through the imposition of real costs on the five members of the Chinese PLA, which was a case that was started when I was the head of the National Security Division of the Justice Department and then came to fruition under my successor when I was in the White House. Where, for the first time, the United States indicted five members of the Chinese PLA for state sponsored, cyber enabled, economic espionage. Now at the time, people said, "You're never going to get those guys. They're never going to see the inside of a courtroom. Why are you doing that?" Well, first of all, it really exposed that activity. Second of all, it was a signal to our companies who are getting stolen blind that their government was willing to show up, to really press this point, to say this is unacceptable. Right?

Greg Clark: Thank you for that, that was huge.

Lisa Monaco: It was a substantial step, and frankly it got some Chinese attention in a big way. And the way you know that is because they were deathly afraid that we were going to sanction them, which prompted a very last minute trip by President Xi's top guy to come negotiate a agreement with President Obama about cyber enabled economic espionage because they were so afraid that we were shining that light on them. So that was an effort to isolate that activity. Imposing costs with a norm that had been agreed to, by the way, by the G20 previously and also resulting in a bilateral agreement.

Thomas Bossert: I love it. I applauded it when I was on the outside, I applaud it still today, and we acted unilaterally and whether that norm had been agreed upon by the G20 or not we should have and did do it.

Lisa Monaco: Yeah.

David Sanger: Yeah, so let me ask you a question about this? So supposing for a second that we came up with, what Brad Smith at Microsoft is referred to as the digital geneva convention, which would be basically a set of norms. And the thing about the actual geneva conventions is it was convened by the Red Cross. It was necessarily convened by governments. It's got a nice certain appeal here because you don't get hooked into every government ratification process. But supposing we made a little list. What's off limits for everybody? So, we'd focus on civilian related things. Hospitals, nursing homes, emergency communications systems.

Lisa Monaco: Critical infrastructure

David Sanger: Critical infrastructure. And election systems. I mean, after what we've all gone through for the past 2 years, I could imagine that when that list got circulated inside the US government or inside the government that's under it's allies, some of the intelligence communities would come back and say, "Now wait a minute, election interference?" Yeah, 2016 was terrible, but, remember, we did a few things in Italy in the late 1940's and a few things in Latin America in the '50's and '60's and we staged a coup in Iran in the 1950's and if you asked Vladimir Putin we interfered in their parliamentary election during the Obama administration. I think you'd have different interpretations of that, but certainly that's his position. How would we get ourselves around the problem that we have interests ourselves on the offensive side that would probably keep us from signing on to some of those things? Including the possibility that in our military plans we might want to unplug and entire country and that would include hospitals and communications systems.

Thomas Bossert: I think it's led to some paralysis and if I can I want to give a brief educational point here, because I'm proud of it. You worked on it, and I carried that torch, to repair the divide.

Lisa Monaco: Cloud act.

Thomas Bossert: Cloud act was great. There's something called the VEP, we do a lot of acronyms, the vulnerability equities process. Let me walk you through what that means in real life. It means that the United States government, for purposes good and bad depending on your moral compass, spends a lot of time with a lot of people trying to purposely find vulnerabilities in software. The software that you all use. And we do that on an order of magnitude that is significant. Engineers with a lot of background do that. And we find vulnerabilities all the time. We now, under two presidents, and we've made the process a little bit more transparent, in fairness we took it from you. We share approximately 90% of those vulnerabilities with the software developers. Now the good ones, like Brad Smith at Microsoft, take those vulnerabilities and they find ways to patch them as quickly as possible. Which is why when you get a patch announcement you

should make that patch update as soon as possible because it's based on the fact that you've been operating with a vulnerability unbeknownst to the software developer, him or herself, for some period of time.

A lot of those software developers let that fall on deaf ears. They don't care, they're an app developer, they've moved on, they've made their money, they've sold their app, it just sits there. The point is, that's only the first step of VEP. So you hear about that, you think, well that's cool, but that's the way the United States government on one level helps each and every one of you. You're now getting patches on your systems and on the systems you rely upon at your banks and power providers that are based off of our discovery of vulnerability. Now hold on...

David Sanger: And the other 10%?

Thomas Bossert: The other 10% we keep and I'm not afraid to talk about. We won't talk about what we do with it, for national security purposes, but it's valid, and it's righteous. We use it for national security purposes for our nation. Now, when it helps others, we'll do it, but we'll do it only when it's in our interests. But when we're into that network, lets say we use that vulnerability to develop an exploit. We use that exploit to get into a bad guys network. When we're in that bad guys foreign nation state, not for commercial gain like President Xi was doing. When we're there, we happen to notice all sorts of things. And when we notice them, we notify. And when we notice them, we tend to notice things like, holy cow, there's DNC emails in there. Holy cow there's the recipe for Coca Cola or Kentucky Fried Chicken. And you get a phone call. A lot of you didn't know it and you didn't think you'd gotten it from the government but you might've gotten that Google alert that says, "We have reason to believe that your Google account was compromised by some foreign entity."

David Sanger: Funny, I've gotten that one.

Thomas Bossert: Well, at some point, the FBI doesn't have the resources to figure out who Bigboybilly32@gmail.com is. And so they call Gmail, and they say, maybe you know. And they say, "Yeah, we'll send a note to that person, we'll take care of notifying that person on your behalf." But a lot of that originates from what the United States government is doing. That's block and tackle, but it's significant. So I didn't mean to suggest that the government has no role, I just wanted to level set it at the beginning, we do a lot.

David Sanger: Greg, when you guys did your work on WannaCry, one of the first things that your engineers noticed was that some of the vulnerabilities and techniques that were being used by the North Koreans and the WannaCry attack, and this is the one that hit the British healthcare system, appeared to come out of the US arsenal. They appeared to have been stolen, leaked, whatever from the tailored access operations unit of the NSA. I have to say, it was not a topic I found the US

government enormously willing to talk to me about at great length but talk to us a little bit about that risk.

Greg Clark: So there are certain kind of vulnerabilities that are a lot lot worse than others and they allow for exponential propagation of malware and there was a couple of those. But in the super geek lair of this craft that we're in, that particular vulnerability was well known. That wasn't like a huge secret.

David Sanger: Right.

Greg Clark: Right? It was the reason why you could print from your home computer to a printer and if you locked it down, it was too hard for people to configure and stuff like that. A lot of issues there. But I can tell you right now, that the bad guys know about a lot of vulnerabilities and now that we have wifi chips everywhere, these wifi chips have a full blown operating system, a computer system in it, burnt into the firmware, which means hard to change. Takes a long time to change. In that thing is a plethora of known vulnerabilities that we can't fix because we have to go visit it. It's economically not worth it if a $32 thing that's in the roof of your house. So we're going to be living with vulnerabilities for a long time, they are going to be a part of the ecosystem, and some of them in the IOT space are very difficult to patch.

In online computers, desktops, phones, they're easier to patch. So we have a serious issue where we're gonna get bad stuff in the infrastructure and anyone that tells you that that's not going to happen is not telling you the truth. It's a fact of life. So what do you need? You need to be able to recover quick. When it gets found, you gotta be able to patch it, you've gotta be able to countermeasure. I was extremely impressed with the governments influence on this piece of malware that got in the home wifi, called VPN filter, and you might have seen the FBI said, "Can you go and turn on and off your wifi router? Well, some people overseas, some bad guys had it, and they were watching what you were doing, and they were stealing things from you." And when you turned it on and off, it went to the US government who had it, who then neutralized that vulnerability.

David Sanger: Because they had taken over the commanding control?

Greg Clark: Because they had taken over the commanding control, the mission control, the operation center that was taking care of this thing. But this is a way of life, and what we have to have is private companies like Microsoft, us, and many others, and the government working together to be able to recover from these things quick, because it's a long way from where we are now to technology that won't be compromised. And I always tell my engineers this story. When I got out of college I went to work at Bell Labs, Bell Labs made operating systems. One of them was famous, called Unix, turned out to be a derivative of a thing called Linux, you might have heard about this stuff, there's some gray hair in the room, maybe not.

We worked on a thing called the trusted computing base, and those of you that have been around awhile, in information systems and dc probably remember this thing, compartmentalize mode workstations, all this kind of stuff. Well I was a junior [inaudible 01:13:42], straight out of school, I worked on some of that stuff. I went into a faraday cage and shut the door when we were writing some of that code because we were worried that the Russians were in the parking lot with an antenna, reading the code off the bus. This was in 1988.

David Sanger: One last question I want to ask all of you before we try to get just a few from the audience. So, if you think about the deputy attorney general's speech. He's laid out this problem. He's described a set of initiatives, as you point out, Lisa, at the beginning, for the justice department, which has an important role, but there are a lot of players here. Department of Homeland Security, the Department of Defense and the newly elevated cyber command. Certainly the National Security Agency. We discovered that groups as arcane as the Office of Personnel Management have significant cyber vulnerabilities we needed to be able to pay attention to when we're probably insufficiently aware of. So where does the kind of initiative that you heard about today, where does this all come together? Who makes this decision? Especially in a world where we've seen the new National Security advisor John Bolton take apart the position of cyber coordinator that both of you worked with in two different administrations. Lisa, you want to start?

Lisa Monaco: So, I'm really glad you highlighted this. Because again, I think the work that Rod highlighted today, and most importantly the work of the career men and women in the justice department and the FBI who contributed to that, my former colleagues, is something that we should be exceptionally grateful and proud of. That work is one piece and it has to feed into a national policy. Right? It has to feed into a national decision so at the end of the day, the decision to call out the Russians for what they're doing is very important and using that criminal justice tool, I think, is very important to be able to use that as one of our ways to impose costs. But at the end of the day, where is it feeding in?

I would argue it should come together in the National Security Council and that process should be led, in the first instance, by the cyber coordinator. The cyber coordinator is somebody who, in the past reported to me and through me to the president and the national security advisor and it was that persons singular focus, this person wakes up every day, 24/7, he is thinking about cyber threats. And why is that important? Because in 2013 the director of national intelligence and the whole intelligence community said that the biggest threat that we face, not terrorism anymore folks, it's the cyber threat.

David Sanger: And that was a big change because in 2007 there was no mention of cyber in that same report.

Lisa Monaco: Yeah, a little known Washington lawyer who was then the head of the FBI made this announcement. And it got a lot of attention. And every year since then...

David Sanger: It has been number one.

Lisa Monaco: It has been number one. So I would argue, to not have somebody who is focusing 100% of their day on that topic and on that threat and synthesizing the inputs from the rest of the government and feeding up to the homeland security advisor, the national security advisor, the president options about what to do about it, that is frankly malpractice in terms of governance and accountability and responsibility on the major threat that we face.

David Sanger: Do you agree it's malpractice?

Thomas Bossert: So, that was me, when I was there and it was Rob Joyce, and we were steeped in this and we were driving it everyday.

Lisa Monaco: And doing a great job.

Thomas Bossert: Thank you ma'am.

Lisa Monaco: Rob Joyce was a tremendous asset to your team and you were right to bring him in.

David Sanger: For those that don't know Mr. Joyce came from the NSA. He had been on both the offensive and defensive side so he knew this pretty well.

Thomas Bossert: Both of us have left and that's the presidents prerogative to have his own staff serve him. I'm not going to belabor it. In fact, I still am completely committed to taking the team that he's replaced us with, who don't have the depth and breadth and background that we have in cyber, and making them smart. We owe it to the team and the country. So I'm not gonna stop for a second, in fact I'm gonna start right here, from this stage. I'm going to offer some advice to Ambassador Bolton, who I think, has this countries interest in his heart. And I know the president does. It's tempting for some of us to take our previous experiences, in fact I think we all do that, we take experiential learning from when we're children even and we apply it to when we're adults and apply it to a new problem. In this case, if he's tempted to, and there's some reason to believe that from writings and speeches and so forth, appearances on television, to apply the thinking of a nuclear deterrent policy or world view, I would encourage him and the president not to, and here's why.

In nuclear war you're either at it, or you're not. And there's a whole lot of complexity and we just saw a lot of that play out. I think a positive way to spin the Helsinki meeting, and I think there's reason to do this, not the Helsinki press conference, was this was the beginning. At least it was round two of these strategic stability talks that we started at the beginning of the Trump administration. It gets complicated, but we are either in or not in nuclear war. News flash, we are in cyber conflict. And we've long joined it. And there's not a country on this planet that's not in it. There's not very many organized crime

groups that are not in it. We are in a constant state of not just low intensity, but in some cases intense conflict online. So the deterrent thinking of nuclear war does not apply. If you think that we're going to deter someone by escalating further the conflict that we're already in, I think you've misapplied your previous thinking. That make sense? So I think that might level set some of our conversation on cyber.

And with respect to me and Lisa, what's the saying of graveyards littered with indispensable people? They'll be new people there. This president and this country will be fine on that and I'm not here rooting for him.

Greg Clark: Tom, you make a good point but on the civilian side, we know a lot about these people. We've been tracking them for a long long time and the issue is, the nation states are really hard to daylight because the consequences are massive for a private enterprise to defend against that. They have great capability. The other thing that needs to stay on the table is it's dangerous to daylight the organized crime. Some of it is massive in concept and for our researchers to come out and say, "Hey, here's what we know" is dangerous for them personally and then on the cooperation for the kind of risk management of all that.

Thomas Bossert: One of the reasons that I wanted attribution to come not just unilaterally, so I don't sound like too much of a madman here, I wanted it bilaterally for a reason. You'll see, and NotPetya was an example, I was adamant about having at least one other partner that contributed to the attribution and the forensic analysis. Not a partner that then piled on afterward. It's useful. We had 14, 15 other countries that piled on immediately afterwards and said, "We looked at your conclusions and your data and we agree with it and we agree with what you've done." That's useful because numbers and strength and so forth. I want one other country to vouch for the actual data and to bring some capability to the table so that we're not paying for all of it and doing all of it. Right?

David Sanger: And the private sector needs that.

Thomas Bossert: That's important here, because for instance, I saw a lot of just social media feedback that said, "Is it bad that I don't believe the attribution coming from the Trump administration but because the British have joined it, I kind of believe it?" Hey, whatever it takes. But we had a bilateral partner with serious capabilities and chops with stakes in the game and took a little bit of risk there to call that out.

Lisa Monaco: No, I thought that it was very important to call that out.

Thomas Bossert: So the lesson in NotPetya was that the Russians did it to the Ukraine. Their intent was to disable the Ukrainian economy. They did it. They succeeded. That's bad and we can talk about that in our geopolitical panel some other time. But if you're going to use a cyber tool to do it, you better have the principles of proportionality. The Russians could have easily constrained the propagation of

that cyber tool to the Ukraine, but they didn't. They said, reckless, let it propagate, I don't care if it takes down ten billion dollars worth of annual damage to US and European countries, which is what they did. I think our penalty imposed on them was pretty harsh. There were a lot of sanctions, a lot of costs, and I didn't want them to stop hacking. That's a fools errand, to say that we're going to impose a cost, now stop hacking. The problems over, now everybody go home. But we're going to impose a pretty big cost in hopes that the next time out, at very least, you'll use proportionality to limit your target.

Greg Clark: I think just to back up for the crowd, what Tom is talking about, that particular piece of malware got into a company, Merck, that was well reported on. Took 7 minutes to wipe out 25,000 end points on desk. 2,500 servers. Cost them over $300,000,000 to repair it and now are out of business for 6 weeks. 7 minutes from when it showed up.

Thomas Bossert: It shut down port operations in three US ports.

Greg Clark: Operating rooms went dark in HS and UK.

David Sanger: And it's not even clear that they were an intended target.

Greg Clark: They weren't.

Thomas Bossert: They weren't.

Greg Clark: The malware was sloppy. They were in a hurry to get the vulnerability exploited so they didn't really take a lot of care in the thing and there were some pieces of it that I would say were not perfect, as a computer scientist.

Thomas Bossert: So I set one group of my staff at that were adamant that we had to have multilateral agreements and we had multilateral norms before we acted. And I said, "Okay, lets do an experiment. Half of you go figure that out. Call all of your European partners. Lets see if we can get them all on board. The other half of you go out, find one partner, lets do the attribution and then lets act under the principles of articulated, lets see which ones of us get it done first." I offered the concept that we were enforcing this policy theory, a little jazz music and improvising, and I said, "Lets apply the theory of proportionality to cyber tools." And we beat them. And I think that it was the right thing to do. And when the other guys came back they said, "Yeah, but ours would have been stronger if you let us go longer." So I think she's going to be right in the long run, but I think we need to a little bit...

Lisa Monaco: Well, and lets be clear, I'm not advocating that the United States shouldn't act, or should wait to act to get the international community on board. I think, if we continue to act consistent with our values, that we can lead the international community to get behind the norms that we set. And so we should act and we

should show what we're going to do and in that way bring the international community along with us and isolate those that would not adhere.

Thomas Bossert: Here here.

David Sanger: Well, I failed at one of my main moderator tasks, which was, my hope was to bring in questions from all of you but the conversation here was so good, and I think, one of the most sophisticated conversations I've heard on the nature of this problem, and I'm acutely aware that we are the last thing, the four of us, between all these people and their dinner.

Lisa Monaco: Their cocktails.

David Sanger: Yes, and their cocktails.

Greg Clark: Very much.

David Sanger: And that could turn ugly in an Aspen crowd. So I thank you, and I ask you to thank our entire panel.

PART 3 OF 3 ENDS [01:25:17]