Cyber-Crime, Cyber-Espionage, Cyber-War, & Cyber-Threats: An Exploration of Illegal Conduct & Warfare in the Cyber-World

Moderator: Honorable Preet Bharara, United States Attorney, Southern District of New York

Panelists: Honorable Robert S. Mueller, III, Wilmer Cutler Pickering Hale and Dorr LLP
Honorable Michael Chertoff, The Chertoff Group
Edward M. Stroz, Stroz Friedberg LLC

What are the most significant threats facing the United States as a result of the growth of cyber-crime and related illegal conduct occurring over the Internet? What are governments and the private sector doing to combat the growing threats, and are those efforts sufficient? What are some of the policy and philosophical considerations that should influence our evaluation of efforts to regulate and combat illegal conduct occurring in the cyber-world? These are some of the important issues discussed during the panel discussion, which is summarized below.

Mr. Preet Bharara began the panel discussion by asking the panelists which cyber-threats concerned them the most and which cyber-threats they believed the nation was least prepared to address. Director Robert S. Mueller who served as United States Attorney for the Northern District of California, Assistant Attorney General and Director of the FBI before entering into private practice, asserted that the greatest cyber-threats are to financial institutions and exchanges, followed by threats to infrastructure such as the power grid. Director Mueller stated that the threat to financial institutions is more severe than the threat to infrastructure because financial institutions and exchanges already are on the Internet and are thereby exposed to cyber-threats that could harm not only the institutions and exchanges, but the economic capability of the United States. Infrastructure, by contrast, is less exposed to the Internet.

Secretary Michael Chertoff, who previously served as Secretary of the Department of Homeland Security ("DHS") and Circuit Judge for the United States Court of Appeals for the Third Circuit, agreed with Director Mueller and added that the greatest cyber-threats to national security are those that would allow the United States' enemies to use technology not only to steal information, but to access and damage control systems that affect real-world activities, including air traffic control systems, systems that operate markets or even airplanes, automobiles or other machines that could be accessed and controlled remotely. Mr. Edward M. Stroz, a former FBI Supervisory Special Agent who founded and serves as Executive Chairman of investigative firm Stroz Friedberg, joined in the other panelists' assessments and asserted that risk management principles need to be applied to cyber-threats to ensure that the nation is prepared to address the most severe risks to national security.

Mr. Bharara next asked the panelists whether the government had the ability to recruit and retain people who were smart enough and cutting-edge enough to deal with the cyber-threat, and further whether the government had the resources to combat the threat effectively. Secretary Chertoff contended that the government is moderately successful at attracting top talent, in spite of the inability to pay top talent at levels commensurate with those in the private sector, because it benefits from the ability to draw individuals attracted to the cutting-edge technology problems handled by the National Security Agency and other government agencies. Secretary Chertoff added, however, that most infrastructure is in private hands, thus rendering the government unable to protect that infrastructure directly. He also noted that regulation has been ineffective at securing private sector infrastructure. There is a need, according to Secretary Chertoff, for a new framework that would enable people to share information on cyber-threats without the fear that the information would become public or that people making disclosures would be exposed to liability. There also is a need for a well-developed doctrine and appropriate legal authorities to permit the government to take appropriate steps if a destructive attack occurs and there is a need for the government to be involved directly.

Responding to Mr. Bharara's question concerning the government's ability to hire top talent, Director Mueller stated that the FBI and other federal agencies involved in addressing cyber-threats are able to draw top talent that is able to combat the cyber-threat not only with technical skills but also with the ability to investigate cases using traditional investigative techniques applied to the cyber-arena. Mr. Stroz echoed that sentiment, noting that FBI agents have unique abilities to investigate and solve crimes, giving them an advantage when compared to private sector cyber-industry talent without that experience.

Mr. Bharara then asked whether the panelists agreed that the private sector shared responsibility for cyber-security or whether the government was responsible for cyber-security as part of its obligation to provide for "the common defense," in the words of a cyber-security executive. Mr. Stroz replied that the private sector has to play a role in protecting its own property. Mr. Bharara then asked whether private sector entities that are under attack from cyber-threats are doing enough to coordinate their efforts with each other and the government. He used the analogy of a bank robbery to make the point: "In the old days you would never imagine that a financial institution after being robbed at gunpoint by a person with a mask wouldn't immediately call the police or FBI or whoever and report that. And yet often it's the

case in real life experiences that financial institutions are basically the victims of a similar kind of bank heist or robbery and they're delaying days, weeks and sometimes never ever disclose to law enforcement. How big a problem is that and why is that?"

Secretary Chertoff responded that the problem identified by Mr. Bharara used to be bigger, but is improving. He noted that the private sector has to play a role in thwarting and responding to cyber-attacks because the backbone of the internet "is not in the military, not in the government, but is with the private sector." He reiterated his earlier claim that a mechanism is needed for private sector actors to provide intelligence on cyber-threats to the federal government and for federal government agencies to disseminate intelligence to the private sector so that it can respond to cyber-threats more effectively. Mr. Bharara asked what incentive private sector actors have to cooperate with government, given the intrusion of privacy and risk of harm to the company's reputation or its stock price if a cyber-attack is reported to the government and publicized. He asked why private sector actors should not just respond to cyber-threats on their own and "hope that the next guy that gets attacked is their competitor?"

Secretary Chertoff replied that "everybody gets attacked" and that therefore the shame and embarrassment of being attacked by cyber-criminals was diminishing. He also noted that private sector actors are realizing that, as a matter of self-interest, cooperative exchanges of information actually could reduce the risk for everybody. He noted that banks do not want to compete on the issue of cyber-security, much as airlines do not want to compete on the issue of safety, because it was not in their interests to have consumers thinking about cyber-security when banking. He added that it is in the private sector's interest to beef up cyber-security to avoid a scenario in which the government has to monitor a company's activities to guard against and respond to cyber-threats.

Mr. Stroz stated that there are reasons for delayed reporting and responses, both by the government and the private sector. He stated that sometimes the government can delay responses to cyber-threats as it attempts to investigate and apprehend the perpetrators of cyber-attacks. He also raised the concern that, in many cases, cyber-attacks are stealthy, and the only individuals in a position to detect attacks—employees of company IT departments—are the same individuals who stand to get in trouble for reporting those attacks. He noted that this potential conflict of interest may cause delays in reporting and that the threats need to be managed more effectively to avoid delays or problems in reporting in the future.

Mr. Bharara then asked whether the culture of sharing information in order to increase safety found in the airline industry, referenced earlier by Secretary Chertoff, is found in the private sector in dealing with cyber-threats. Director Mueller stated that Silicon Valley's competitive environment provides disincentives for cooperation. Secretary Chertoff argued that, while the private sector needs to do a better job of cooperation, the government also needs to "share back." He noted that sometimes the government will receive a report of a cyber-attack from the private sector, and the government's only response will be to say "thank you." He stated, "I think there's got to be a certain amount of mutuality" so that private sector actors running critical infrastructure "get the benefit of some of what the government knows." Director Mueller responded that information-sharing is in fact happening. He cited statistics

indicating that, in 2013, about 3,000 entities were informed by either the FBI or DHS that their networks had been compromised, principally by Chinese actors. Fully 70 percent of those notified did not realize that their networks had been compromised. Mr. Stroz noted that in some cases, it may be helpful to victims of cyber-attacks for the victims or law enforcement to monitor attackers before taking steps to stop the attack in order to avoid bigger problems. He gave as an example situations in which a client wanted to change passwords immediately upon detection of a threat. He stated that he would advise clients in those circumstances not to do so because, "if you do that, A, they're going to know you're inside, and B, they're going to get all the changed passwords."

Mr. Bharara then turned to the question of what roles various government agencies play in preventing and responding to cyber-attacks and whether lines of responsibility were clear. Both Director Mueller and Secretary Chertoff stated that, when serving in their roles as heads of the FBI and DHS, respectively, they worked diligently with each other and with other federal agencies to delineate clearly the various lines of responsibility. They noted that while turf fights might arise on occasion, there is "plenty of work to go around."

Mr. Bharara then asked the panel to address the cyber-threat posed by foreign nations, in particular China. He asked the panelists whether responses to the Chinese cyber-threat are being affected by "narrow self-interest," in which companies are engaging in a "cost-benefit analysis," essentially balancing the financial benefits of accessing the Chinese market against the costs of the theft through cyber-crime that inevitably will occur in China. Secretary Chertoff stated that there was a "wide variety of views on the issue of China" in the private sector. He agreed that some companies were conducting a cost-benefit analysis of the type described by Mr. Bharara, but added that one of the factors some companies consider is that technological secrets stolen in China may not be usable by Chinese companies until the technology has already been rendered outmoded by ongoing research and development efforts outside of China. Secretary Chertoff also added that Russia posed a significant cyber-threat.

Mr. Bharara asked the panel whether it ever makes sense for a company to take matters into its own hands by engaging in offensive actions, known as "hack backs," against individuals or entities believed to be engaging in cyber-attacks against the company. Mr. Stroz explained his view that the idea was unwise because, among other things, it is difficult for a private company to know the true origin of a cyber-attack. Thus, a hack back presents the risk that an offensive action may target the wrong individual or entity.

Mr. Bharara then asked whether the response to cyber-threats had become too complicated, and whether the most important steps to combat such threats were actually simple, much as the best way to combat infection in hospitals turned out to be a simple one: washing hands. Mr. Stroz agreed, stating that "the simple things go a long way to making it better," including protecting passwords, keeping systems patched with the latest security updates and ensuring that all participants on conference calls are fully identified.

Mr. Bharara concluded the panel discussion by asking whether, in cyber-space, there remained any "pure space for anonymity that is appropriate that law enforcement and intelligence services shouldn't be able to touch?" Secretary Chertoff replied that the question

should be broken up into two parts: first, "should the government be able to build the capability, the potential to elicit or intercept" cyber-communications, and second, "under what circumstances should it have the authority to exercise it?" He said that the answer to the first question was straightforward: the government should be able to build the capability to get into any network, "assuming that it has the legal authority and appropriate permission to do so," with the caveat that, in his personal view, the government should not "make it easier for itself by weakening the overall structure of security for widely distributed products." Secretary Chertoff also contended that privacy interests and security interests are not mutually incompatible, stating: "You can't have privacy without security." Director Mueller joined with Secretary Chertoff in stating that it was essential to national security that the government be able, with appropriate authorization, to access cyber-communications in order to avoid having increasing portions of the Internet "go dark." Mr. Stroz added that, while everyone should have the right to anonymity, it is important to be able to combat criminal operations such as Silk Road that take advantage of anonymity to facilitate crimes.

Mr. Bharara then opened the floor to questions. One audience member asked when a cyber-attack is "big enough" to be reported to law enforcement. Mr. Stroz stated that, while some crimes might be too small to prosecute on their own, "a minor event can be one little tentacle of a much bigger problem," thus calling for some attention to determine whether the reported issue is indicative of a bigger issue that may warrant law enforcement support. Director Mueller stated that the increasing frequency of cyber-attacks at companies such as Target increases public awareness of the necessity of addressing the problem in new and different ways. Mr. Bharara asked whether the Target cyber-attack, which resulted in the termination of the company's CEO, had affected how people in the private sector think about the cyber-threat. Secretary Chertoff responded that it had by raising consciousness about how to respond to cyber-attacks and the risks and costs of failing to address them.

A second audience member stated that the panel's discussion of the cyber-threat to the electric grid was terrifying, and asked whether more could be done to address the threat. Secretary Chertoff responded that, according to surveys, the electric utility industry was one of the industries that was best prepared to respond to the cyber-threat and that because the industry is regulated, utilities already have redundancy and resiliency built into their systems to address cyber-attacks.

A third audience member asked whether the panelists would support tort liability for third-party security software providers or government indemnification of private companies that comply with potential new legislatively-imposed duties in responding to the cyber-threat. Secretary Chertoff stated that he does not support expansion of tort liability, and both Secretary Chertoff and Director Mueller stated their support for "safe harbors," or limitation of liability, for companies that create security tools or provide information to the government to combat the cyber-threat.