FRENCH-AMERICAN FOUNDATION FRANCE

FRENCH–AMERICAN FOUNDATION United States

INTERPOL

WASHINGTON, D.C. • SEPTEMBER 15-16 , 2015

MANAGING
CYBER SECURITY + THE LAW
CYBER RISK

Author: Justin Key Canfil, Conference Rapporteur & Cyber Security Fellow

AIG

AIRBUS GROUP

AXA redefining / standards®

Microsoft

STARR COMPANIES GLOBAL INSURANCE & INVESTMENTS

COVINGTON

SUMMARY REPORT

Table of Contents

Executive Summary[1]

In recent years, France and the United States have witnessed unprecedented cyber attacks, including to sectors not previously considered at high risk. To that end, the French-American Foundation organizes an annual international working group on cyber security to respond to these challenges, convening a distinguished group of experts at its 2015 forum *Cyber Security and the Law: Managing Cyber Risk*. France and the United States have expressed a commitment to the same fundamental principles – freedom of expression, respect for the rule of law, and the protection of individual rights – all of which underscore the opportunity for continued bilateral exchange and collaboration on cyber issues.

Working group participants acknowledged that in the face of rising cyber criminal activity as well as concerted attacks by other actors, including states, it is impossible to achieve zero cyber risk. However, cyber defense measures and improved cyber hygiene provide important protections.

80% of attacks are due to poor cyber hygiene. Preventing these attacks necessitates a corporate culture shift that makes strong cyber defense a priority. In the past, companies may not have recognized the value of cyber defense measures, treating them only as an expense rather than as a necessary investment. The sharing of best practices is equally important, and government has an important role to play in providing services to the private sector. One caveat: participants flagged the concern that current strict definitions of critical infrastructure may mean that certain vulnerable businesses in other sectors only receive limited support. Finally, the cyber insurance qualification process can provide a powerful incentive to improving cyber hygiene. The underwriting process assesses an applicant's overall security posture to ensure that the company has endeavored to minimize cyber risk.

Another 15% of attacks can be prevented through information-sharing, which requires better bilateral and cross-sector cooperation. Trust-building, notably between the public and private sectors, underlies all attempt at greater information-sharing. This effort could be further reinforced by the streamlining of governmental organization with respect to cyber, especially in the United States, and improved legal frameworks (notably greater clarity on computer crime and breach disclosure laws). Participants acknowledged one pressing challenge: cooperation by the private sector with law enforcement investigations, especially in the context of the ongoing debate on encryption and data sovereignty. Overall, participants agreed that the private sector has an obligation to cooperate with law enforcement. At the same time, companies have an obligation to protect user privacy and must also manage potential conflicts of law (especially when companies operate in multiple jurisdictions).

Regarding the 5% of attacks that cannot be prevented, cyber insurance and other liability-shielding mechanisms play an important role in helping the private sector manage risk. Greater clarity about insurance coverage and regulatory and legal frameworks will reinforce the ability of companies to anticipate their exposure to risk and better steward their operations.

Taken together, these measures can address a large proportion of risk and can help entities prepare for when the worst does occur. An integral part of this process is achieving greater trust: bilateral, public-private, and private-

[1] The statements made and views expressed in this report do not reflect the views of the French-American Foundation—United States nor its directors, officers, employees, representatives, sponsors, or the rapporteur. Instead, this report documents the views expressed by participants at *Cyber Security and the Law: Managing Cyber Risk*, September 2015.

private. There is a tendency for immediate concerns to overshadow future security. Positive incentives can help, while limited negative incentives, such as penalties for noncompliance, also have a place for keeping serial rule-breakers in line. However, trust remains the key.

Introduction

Security in cyberspace is a growing priority for the modern world. From Silicon Valley to the Arab Spring, electronic communications have proven a boon for business, education, and personal freedom. But cyberspace also presents new risks and vulnerabilities, with mounting criminal, terrorist, and state-sponsored cyber attacks that pose a threat to privacy and security. Losses for governments, companies, and individuals can be expensive, but so can be efforts to defend against them. Although everyone acknowledges that cyber security is important, it has been difficult for the private and public sectors to agree on how to strengthen it. Coupled with the idea that defense measures should not compromise the underlying freedom, entrepreneurship, and social fabric that makes the Internet great, it is obvious why consensus has been elusive.

With this in mind, the French-American Foundation organized its second annual international working group on *Cyber Security and the Law: Managing Cyber Risk* in September 2015 in Washington, D.C. Both France and the United States (US) face similar opportunities and threats in cyberspace, yet often adopt different solutions. Consequently, an important opportunity exists for an exchange of ideas and for greater collaboration between the two allies.

Organized under the patronage of INTERPOL and the French Minister of the Interior, and with the support of the International Forum on Technology & Security for a Safer World (FITS), *Cyber Security and the Law: Managing Cyber Risk* brought together approximately 50 European and US government officials, industry leaders, and internationally-recognized security and insurance professionals and experts to discuss the changing dimensions of cyber threats and cyber criminality, as well as methods to mitigate liability exposure for cyber security breaches.

This report presents the themes addressed during two days of conference discussions, identifies several challenges to cooperation on managing cyber risk, and describes areas where participants were able to reach consensus. Topics covered included the emergence of new cyber security threats, priorities for international cooperation, the role and limitations of cyber insurance, and the responsibilities and incentives for securing digital assets. To encourage greater discussion and interaction among invited participants, the roundtable discussions were held under the Chatham House Rule.[2]

[2] A public readout of Assistant Attorney General for National Security John P. Carlin's remarks was made available by the Department of Justice's Office of Public Affairs: https://www.justice.gov/opa/pr/readout-assistant-attorney-general-national-security-john-p-carlin-s-address-french-american

Threats to an Interconnected World

Cyberspace is a fascinating and profitable creation, but it is not devoid of risk: malicious users often operate on the same plane as legitimate ones. In February of 2015, US health insurer Anthem disclosed that it had been the victim of a cyber attack that breached a database containing personally identifying information (PID) for up to 80 million customers and employees, including names, addresses, and Social Security numbers. One month later, another insurer, Premera Blue Cross, revealed that it, too, had experienced a cyber attack that had compromised the private data of an additional 11 million people.[3] These are only two of many such examples in the US. In contrast to previous cases where the bulk of cyber crime was perpetrated against the finance, retail, and related sectors, it is rapidly becoming clear that all types of businesses are vulnerable.

Nor has the public sector been immune. In June of the same year, the US Government's Office of Personnel Management (OPM) announced that it, too, had been breached by hackers; by July, it was estimated that 22.1 million Americans had been affected, including anyone who had undergone a security clearance background check since 2000. In one embarrassing episode, US Central Command's (CENTCOM) social media accounts were hacked and defaced while President Obama was delivering a speech on cyber security to the Federal Trade Commission in January.[4] Less than a month later, Newsweek's Twitter account was hacked by the same group, calling itself the "CyberCaliphate," which crassly referenced the Charlie Hebdo incident by displaying the words, "Je suis IS" [the Islamic State].[5]

France's experience has been similar to that of the US. An April 2015 cyber attack, thought to have been launched by ISIS sympathizers, brought down all 11 of TV5Monde's television channels, an act it later decried as "unprecedented in the world history of broadcasting" (as quoted by CNN).[6] This was reminiscent of an earlier wave of cyber attacks in January that had disabled or defaced as many as 19,000 French websites with pro-ISIS and "Death to France" slogans. These incidents raise concerns about the growing threat posed by not only cyber crime but also cyber terrorism and state-sponsored hacktivist groups.

Around the world, more than one million malware threats are reportedly released each day,[7] with more than 800 million people around the world affected each year.[8] The cost to society is staggering: a 2014 study by McAfee and the Center for Strategic and International Studies[9] estimated the annual global cost of cyber intrusions at $445 billion, including the possibility of 200,000 lost American jobs. And such attacks are on the rise: according to PwC,[10] the number of cyber incidents has "increased 66 percent year-over-year since 2009." Worldwide information security spending in 2015 approached $76 Billion,[11] much of it borne by private companies.

Global problems require global cooperation.

[3] Granville, Kevin. "9 Recent Cyberattacks Against Big Businesses." The New York Times. 5 Feb. 2015.

[4] Zetter, Kim. "Central Command's Twitter Account Hacked…As Obama Speaks on Cybersecurity." WIRED. 12 Jan. 2015.

[5] Mosendz, Polly. "Newsweek Twitter Account Hacked By Group Claiming ISIS Affiliation." Newsweek. 10 Feb. 2015.

[6] Melvin, Don, and Greg Botelho. "French TV Network TV5Monde Hit by Massive Cyberattack" CNN.com. 9 Apr. 2015.

[7] Harrison, Virginia and Jose Pagliery. "Nearly 1 million new malware threats released every day." CNN Money. 14 Apr. 2015.

[8] McAfee and Center for Strategic and International Studies. "Net Losses: Estimating the Global Cost of Cybercrime." June 2014.

[9] *Ibid*.

[10] PwC. "The Global State of Information Security Survey 2015." Sept. 2014.

[11] "Gartner Says Worldwide Information Security Spending Will Grow Almost 4.7 Percent to Reach $75.4 Billion in 2015." 23 Sept. 2015. https://www.gartner.com/newsroom/id/3135617

Reaction and Prevention

Recognizing that 100 percent security is not possible, participants at the 2015 working group asked how risk might be managed when the worst does occur. The upside is that common vulnerabilities mean common ground for business and government with a stake in cyber defense. For government, cooperation can lead to better protection against threats to national security, while for the private sector, losses due to cyber threats are linked to reputation and overall profitability. In a world where everyone is vulnerable, risk mitigation should be recognized as an economical business strategy.

Themes

Recognizing the need to control threat exposure before an attack occurs, this year's conference focused on **prevention** and **risk mitigation.** According to participants from the cyber security community, cyber criminals are increasingly shifting their focus from data theft to more direct harm, including breaches intended to embarrass cyber operators. Government representatives concurred, remarking on the consequences for firms in all industries. Among private actors, healthcare and higher education were identified as the most at-risk as these two industries collect the most personal information over time. Second, they are at higher risk for insolvency in the event of an intrusion that compromises this information since their revenue is often designed only to cover operating costs. Credit agencies, too, may be especially vulnerable since cyber criminals tend to follow the money. Yet, of course, recent experience has shown that no one is immune.

Proactive Defense

"The costs stemming from liability [related to such breaches] can be enormous, enough to kill companies – especially smaller ones [which cannot absorb the cost of lawsuits]. Leaks are much more permanent than a DDoS [distributed denial of service attack]. In the future, information manipulation will pose even more risk."

While cyber attacks can target anyone, they pose the most serious threat to firms with inadequate security postures. Data breaches can affect the bottom line through the prospect of consumer torts, damage to brand, and loss of trade secrets. Knowing this, investing in cyber *security* should be a priority economic decision for companies. By sharing best practices, we can ensure everyone is able to equip themselves with the best available defenses.

Risk Management

"While we should do our best to protect against attacks before they occur, it is crucial to have a plan in case the worst does happen."

Not all defensive gaps are foreseeable, and would-be cyber attackers often operate by exploiting vulnerabilities common to more than one network. Sharing information about best practices, as well as current and expected threats, is the optimal way to stem the spread of cyber contamination. In an interconnected world, we are only as strong as our weakest link.

Complementary Effects on Threat Exposure

In addition to the sharing of best practices and threat intelligence, security can also be achieved through collective response and other risk mitigation strategies, such as cyber insurance. If losses to cyber criminals are inevitable, the private sector should seek to minimize these losses by having a plan in place for how to respond, both individually and collectively. Additionally, while expeditious responses can limit the extent and spread of network threats, cyber insurance can help absorb the losses that do occur in the precious time that elapses before a breach is identified and neutralized. Even the insurance qualification process itself can help incentivize the adoption of best practices, network fortification, and better defensive postures.

However, cyber insurance functions best as a risk management strategy, not a panacea. Greater collaboration among different actors will require surmounting the latent trust deficit. The private sector must be cognizant of the government's needs in effectively combating cyber threats. Governments, on the other hand, must respect companies' obligations to customers. Fortunately, public-public, public-private, and private-private interests do overlap in some areas, making cooperation an attainable goal.

Issues and Challenges

Several questions are as of yet unresolved. Forum participants, whose collective expertise spanned the intelligence, law enforcement, cyber security, academic, and business sectors at the highest levels within France and the US, represented a cross-section of wider society active in cyberspace. Together, they identified several questions to address:

Respective Roles of the Private and Public Sectors

Echoing a common refrain, government officials at the conference expressed frustration with perceived private sector resistance, while several from the business community voiced the feeling that that they are expected to aid law enforcement efforts but receive little protection against ongoing cyber attacks. Is cooperation a one-way street? If not, how can government alter this impression? With no obvious "911" (or "112," in the French case), who do companies call for help? Are companies solely responsible for their own cyber defense, and, if so, why should they go out of their way to aid the government?

Trust Deficit and Incentives to Disclose

The private and public sectors often have disparate (and sometimes conflicting) interests and obligations. Moreover, private sector actors are often of the mind that they are battling with one another for market share, leading to a justified concern that disclosure about an attack when one does occur will signal weakness to customers and competitors, thereby damaging the brand. Adding to this, how can bilateral and public-private synergy be encouraged in the wake of the Snowden disclosures and amid the ever-present concern regarding economic espionage?

Reconciling Differences in Comparative Law

Bilateral cooperation can be impeded by the suspicion that an international partner might not be totally forthright. For example, a common concern is favoritism toward domestic industries. Transatlantic law enforcement efforts are further complicated by the fact that criminal acts are defined differently by different countries (for instance, definitions of what qualifies as protected online speech). Similarly, conflicts of disclosure law can also lead to confusion for companies that operate in multiple jurisdictions; in the US, these often vary state-by-state.[12] France's preference for a highly-centralized framework and the US' tendency to treat cyber security as a team sport via specialized agencies, coupled with disparate juridical requirements, may lead to communication difficulties between community emergency response teams (CERTs) in time-sensitive or emergency situations. Finally, different governments may disagree on priorities; for example, should agencies be oriented toward combating cyber crime, potential cyber terrorism, or inter-state threats? Efforts to harmonize law and reporting requirements, most prominently through mutual legal assistance treaties (MLATs), can resolve some of these issues – but not all.

Key Questions

- Given these challenges, how can France and the United States work together to combat cyber threats?
- How might governments elicit more trust and voluntary cooperation from the private sector?
- How can the private sector collectively protect itself against cyber threats, with or without government intervention?
- How can information-sharing, education, and conversations about best practices minimize risk in the first place?

Propositions

Forum participants worked toward accord on these challenges and made several suggestions for ways to advance the agenda (detailed below). The format of the working group presented an invaluable opportunity for various types of actors at the forefront of these issues to engage candidly with each other under the Chatham House Rule. This section details the solutions advanced collectively by conference participants.[13]

The Role for Government:

Promoting New International Norms, Updating International Frameworks

Recognizing the novelty of some of the problems posed by cyberspace, participants called for renewed emphasis on three emerging norms in cyberspace.

(1) In the absence of an international convention clearly prohibiting transnational cyber attacks, governments have a responsibility to police cyber criminals within their borders. This fits with the general principle of "good neighborliness" in international law.[14]

[12] National Conference of State Legislatures. "Security Breach Notification Laws." http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

[13] Consensus was not, of course, achieved in every case. On the whole, these are complicated sets of issues, and progress will be an ongoing process. France and the US will need to continue the conversation in areas where consensus was not readily forthcoming in light of the two countries' longstanding international partnership.

[14] According to the maxim *sic utere tuo ut alienum non laedas* (use your property so as not to harm another), countries may not knowingly allow their territory to be used for acts injurious to another country.

(2) As law enforcement delegates pointed out, it is typically impossible to stop cyber crime of foreign origin from reoccurring without the assistance of foreign governments. Countries that are host to suspected cyber criminals should be expected to offer assistance in tracking them down and bringing them to justice.[15]

The first problem here is whether the criminal law of one country ought to be respected when the host country shares no similar provision. Putting this issue aside for the moment, many types of cyber crime (such as theft) could easily be construed to be discouraged everywhere. Yet diplomatic and law enforcement channels in these areas can be critically slow, even among countries with compatible legal philosophies. Another problem is that even when host governments are sympathetic, the information needed to track criminals is in the hands of corporate data operators, who have a dual and conflicting obligation to aid law enforcement but also protect customer privacy and brand integrity. For the many companies that operate in multiple jurisdictions and may receive multiple, simultaneous requests, it is not always clear with *which* government or agency to cooperate.

"Even among allies this is very difficult. For example, [one European country other than France] requires a ton of documentation before taking something down within their territory."

Such delays can result in cold trails, or even inflated losses when the criminal activity is serial or continual. Governments should continue to cooperate by negotiating mutual legal assistance treaties (MLATs), establishing communications hotlines, investing in community emergency response team (CERT) centers, and regularly exchanging threat information to help streamline cooperation and minimize bureaucratic or political lag. When acts are not dually criminal, however, requestors must realize that providers have legitimate reasons for refusing to comply. Similarly, domestic courts should defer to the competency of host countries to manage criminal affairs internally if it is in the capacity of those countries to manage them.

(3) Lastly, attacks on critical infrastructure in peacetime is "increasingly" seen as wrong and impermissible – not only in that it poses dangers for civilian populations but could also risk escalation.[16]

States should be concerned about escalation. Respect for cyber norms is inherently linked to stability in conventional spaces, and violations could have dangerous consequences. According to one conference participant, the recent indictment by the US Department of Justice of five members of the Chinese People's Liberation Army for alleged industrial espionage was intended as a signal that the US maintains an "all-tools" approach to dealing with cyber threats. These tools include domestic criminal law but also other types of coercive force, such as sanctions, as deemed appropriate. Norms are most likely to be internalized when they benefit everyone involved. Some participants theorized that, because all countries benefit from a rule against attacking critical infrastructure, the emergence of such a norm is preordained.

[15] Still in line, of course, with the principle of comity or reciprocity, which says that countries should extend reasonable jurisdictional courtesies to one another.

[16] US officials were quick to note that this norm applies in peacetime, perhaps implying that cyber attacks that target critical infrastructure might in some circumstances be permitted under international humanitarian law.

Promote Public-Private Synergy

Since cyber threats can often affect multiple operators using similar software or infrastructure, the best security is joint security. Therefore it behooves industry players to work closely with government and with each other in the fight against cyber crime. Beyond preventing attacks from penetrating defenses, rapid and reliable threat information-sharing can actually shape the preferences of bad actors through deterrence.

For instance, imagine a cyber criminal invests a certain number of hours in writing malicious code (or pays x dollars to buy information on a zero-day exploit). The effort (or cost) might be worth it if the hack is expected to affect multiple targets. But if information is shared in a timely manner and other operators are able to patch their systems after an attack is detected by another firm, contagion is avoided. Such cooperation has the potential to not only offer better returns to scale for individual businesses but also to ensure that crime does not pay for adversaries. If, however, companies continue to silo their information security practices, the exploit can be used repeatedly.[17] Mistrust of one's competitors is the biggest obstacle to more cooperative practices. Yet the participants maintained that it is better to trust the (marketplace) "adversary" one knows than invite cyber attacks by truly malicious entities. Building trust will require government incentives, more leadership among private sector actors, and the consideration of cyber defense as factoring in to each company's profit margin.

How can governments promote collective action? This may be an easier proposition for French officials, given the more centralized nature of France's cyber regime and institutions. The US government has also suffered damage to its reputation in recent years in the wake of disclosures about surveillance programs. Yet the latter is earnestly engaged in a concerted effort to repair its image with the private sector. President Obama has reached out to Silicon Valley for assistance in the fight against online terrorism, for example, and some forum participants recalled how the administration consulted with more than 25 companies in the wake of the Sony attacks on an appropriate and measured response. Trust between the public and private sectors, not just private-private, is still the missing ingredient, but it can only be regained through continued overtures and demonstrated commitment.

Provide Coherence and Clarity on Domestic Laws

By law, cyber attacks that have resulted in the exposure of PID must be disclosed to customers. Yet, especially in the US, the law on this is sometimes overly complicated and inconsistent. It also fails to cover cyber attacks that do not result in customer data breaches but still raise economic or national security concerns. On the domestic front in both France and the US, work remains to be done to further develop, clarify, and streamline computer crime/breach disclosure law. Some participants called for new laws to punish nondisclosure as negative incentives for victim companies to come forward. This is already the case in both countries, especially France.

On the other hand, victims may already face broad liability exposure from customers, brand damage, and loss of proprietary information such as intellectual property: too many obligations and too much risk could begin to cause firms to leave the market. Another point to note is that sometimes only the company itself has knowledge that it has been breached, and thus some more risk-tolerant firms might not come forward in order to avoid punishment.

[17] On the other hand, representatives from both countries recognized that terrorists are unlikely to be deterred in the same way as states or criminals. This calls for strengthened bilateral cooperation in combating terrorism through preventative measures and law enforcement, but also raises complicated issues for data operators such as customer privacy, data sovereignty, and encryption (discussed within).

Rather than punitive laws, government might instead encourage cooperation by ensuring confidentiality when possible.[18]

(1) One solution is to have governments take steps to protect the anonymity of firms that come forward. Government can serve as an intermediary that shares crucial information about how the attack was successful while preventing damage to the company's image. Such a step is not always possible, of course; for instance, when breaches compromise the PID of users. Beyond protecting discloser anonymity, government can also do more to stand up for companies that have been victimized by employing countermeasures against attackers. In the US, the law enforcement community claims to consider this a priority, but private sector participants expressed the view that too little is done in response. Business must be cognizant that, by giving away too much information, law enforcement compromises its investigations, yet law enforcement must also realize that businesses need to know something is being done to protect them. Society must find the right balance on a case-by-case basis.

"We are creating a new narrative – the bad guy was North Korea, not Sony!"

(2) A second solution is that government could institute basic standards for cyber defense. Victims are just that – victims. They should only be sanctioned or reproved when it can be shown that breaches were the result of a lack of responsible security protocols or a failure to take reasonable, proactive defensive measures, with the recognition that some margin of error is always to be expected. If everyone is vulnerable in cyberspace, actors should not be punished simply because they were targeted.

(3) Finally, both governments should work to implement more uniform computer crime laws in order to promote international norms about what constitutes "cyber crime" as well as expedite the MLAT process. The Budapest Convention on Cybercrime,[19] which seeks to harmonize rules on cyber crime and which both France and US have ratified, is an imperfect but important first step in this direction.

Provide Assistance and Services to the Private Sector

"We get better and better at this every day… unfortunately it's because we're getting a lot of practice."

Government can serve as a prevention resource by facilitating the exchange of information about current and future threats (including the provision of threat information legally sourced by intelligence or law enforcement). It can also place more emphasis on developing programs to help train, educate, and encourage the sharing of best practices among industry players, which would raise the level of collective defense against the universe of cyber threats.

Caution should be taken, though, that government does not become a market player. Cyber security providers have a comparative advantage with respect to their existing relationships, expertise, experience, and business models. Conference participants also noted that much is already being done to facilitate a more efficient exchange of information. In the US, the Department of Homeland Security (DHS) established the Computer Emergency Readiness Team (US-CERT)[20] in 2003 for this purpose. US-CERT maintains a database of threats, seeks to coordinate responses, and releases information as it becomes available. France maintains its own CERT, as well,

[18] Something that DHS-CERT already claims to do.
[19] Council of Europe. "Convention on Cybercrime." https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
[20] US-CERT. http://www.us-cert.gov/

and the C3VP[21] program shares information between countries. Recognizing that previous practices (command chains, email exchanges) are not fast enough to keep up with pervasive cyber threats, some officials advocated for the software standards in Trusted Automated Exchange of Indicator Information (TAXII), Cyber Observable Expression (CybOX), and Structured Threat Information Expression (STIX),[22] which allow CERTs to generate reports on cyber attackers containing *"over one hundred fields of intruder characteristics [and] 28 fields of actionable information."* The chief problem is that not much of this is common knowledge. Government must do more to promote its efforts.

The international working group agreed that US and French CERTs must also improve in two ways. First, CERTs must emphasize to the private sector that they are defense-facilitators, *not enforcers*. This is meant in two ways: a) it is the job of law enforcement, not CERTs, to pursue and punish criminal attackers; b) CERTS are not in the business of punishing businesses when they are attacked and that sharing information with them will not automatically trigger legal sanctions against disclosing companies for "inadequate" defense. In addition, CERTs will not disclose anything about the company that could disadvantage them vis-à-vis their competitors in the market. One participant used the analogy of a "cyber" neighborhood watch: *"imagine there's a rash of burglaries in your neighborhood and that a house on the block was broken into. You don't need to know what was stolen in order to secure your own property – you just need to know how the burglars were able to get in."* CERT officials must reiterate to the private sector that this is their primary function.

Second, government representatives acknowledged the feeling among some businesses that sufficient help was only forthcoming to those who fit into government's strict definition of "critical infrastructure," (applied to a limited number of industries in France and the US). Several attorneys in the working group complained that pretrial information, for instance, was not protected.

The Agence nationale de la sécurité des systèmes d'information (the French Network and Information Security Agency, otherwise known as ANSSI) has developed highly-targeted, sector-specific security measures, but at the time of the conference the relevant ministries were individually responsible for protecting critical infrastructure sectors, and the country still lacks a national critical infrastructure protection plan (though recent legislation has the potential to change this). Similarly, in the US, President Obama's Executive Order 13636[23] was intended to "widen the aperture"[24] to protect additional industries, but greater clarity is needed on the definition of "critical infrastructure," and more work needs to be done to assuage the concerns of non-privileged sectors.

[21] US-CERT. "Critical Infrastructure Cyber Community Voluntary Program." https://www.us-cert.gov/ccubedvp

[22] US-CERT. "Information Sharing Specifications for Cybersecurity." https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity

[23] DHS. "Fact Sheet: Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD)-21 Critical Infrastructure Security and Resilience." https://www.dhs.gov/publication/fact-sheet-eo-13636-improving-critical-infrastructure-cybersecurity-and-ppd-21-critical

[24] Participant quote.

Facilitate Better Cooperation within Government

Within government**,** law enforcement and intelligence agencies must improve their level of cooperation, albeit without transgressing civil and constitutional protections. As one official remarked, cyber security is a

"…team sport. The different agencies complement each other. We model our activities for incident response based on partners who already have clear protocol, such as FEMA [the Federal Emergency Management Agency]. This also allows us to get specialized agencies involved when it pertains to specific sectors; for example, Treasury for financial."

French officials expressed a shared vision for preventative defensive measures, rapid response, and stronger cooperation between all players, including internet service providers (ISPs), cyber security service, and industry. Unlike the US, the majority of French participants favored a vision of centralized control, with close relationships between CERT, strategy, law enforcement, and intelligence leadership. In their view, this provides the basis for effective responses to terrorist threats, which "necessitate better and faster cooperation."

Officials in both countries complained about the sense that an intelligence arm that "sees everything but does nothing," and a law enforcement arm that has the power to act but is blindfolded by due process standards, can hamstring rapid responses to threats. At the same time, there was some concern that too little separation between law enforcement and intelligence would only create the potential for abuse, undermining individual privacy and further broadening the trust deficit. Intelligence and law enforcement in both countries must find a way to tear down some of the cultural barriers between them in order to maximize efficacy, albeit without sacrificing basic democratic principles.

On espionage, American officials reiterated that they considered providing industrial intelligence to domestic corporations about their competitors to be off-limits. One recommendation was that the US government should reduce the incentive for economic espionage by making it easier for international businesses to operate in American markets with a reduction in trade barriers.

Finally, there was general consensus that the threat of financial manipulation or sabotage represents a grave risk to national and international security. American officials, in particular, urged joint cooperation against such threats.

Tasks for the Private Sector:

Foster New Industry Norms

Norms have already been proposed for the conduct of states in their international relations, but participants also recognized that a new set of industry norms is still needed – a "corporate culture shift." Participants highlighted the following priorities for businesses:

Prevention: Encourage Timely Disclosure of Data Breaches

This includes cooperation with law enforcement on disclosure. The stigma carried by cyber attack victims will inevitably fade as society realizes that perfect security is impossible, and that no one is immune from a determined and sophisticated attacker.

“We need victims in the private sector to come forward voluntarily and cooperate with us so we can figure out who did it and share best practices to prevent it from happening again. Survival should trump secrecy in the business community.”

Because the number of cyber threats is likely to continually proliferate, firms should recognize that the long-term, industry-wide benefits to collective security greatly outweigh any near-term concerns about disclosure. Government also has the opportunity to make disclosure safer and less costly for business, a point discussed within.

Prevention: Share Threat Information

Participants agreed that more information about threats can help protect data operators against intrusions. Part of this can be achieved through government laws and institutions, such as US-CERT. However, information-sharing is a two-way street. Companies victimized by cyber attacks must be more forthcoming about how attackers were able to penetrate their networks. Both US government and insurance representatives remarked that lessons could be learned from the banking sector, which has a

“Culture of information-sharing [dating from] the American Wild West; they are used to regulatory scrutiny and have access to investigators and [forensic] services.”

The private sector must also learn to share information internally. This is easier said than done. One major French company in attendance indicated that it was very willing to cooperate against threats but that its efforts had been rebuffed by US competitors. Because businesses are used to competing with each other, this will require continued trust-building, open dialogue between Chief Information Security Officers (CISOs), and demonstrated leadership by those who can show they take cyber security seriously.

Reduction: Invest in Robust Defensive Measures

“For [most] firms, right now, the incentives to take cyber security seriously are low. Security can disrupt a company’s day to day operations and so patches get put on the backburner. We need to change that cultural conversation so that security is a priority.”

Participants stressed that private firms should recognize that robust security, not just lots of features at the lowest price, is essential to a profitable business model in the information age, since the consequences of cyber attacks can be so severe. Technology vendors will place increased emphasis on security if their customers demand it.

“[The truth is that] no company can stop a determined [attacker of sufficient sophistication, such as a] state. We can never get to zero percent risk, so it becomes a risk management issue.”

Participants also acknowledged the specter of insider threats, both malicious and unintentional:

“Even if we get to 95 percent security, there’s always that 5 percent who will click a suspicious link even when trained not to. The bad guys only need one opening [in this threat environment].”

The unfortunate reality is that it is only a matter of time until a cyber attack successfully penetrates even the best protections. Risk reduction can delay serious breaches but cannot guarantee against them forever. However, a good prevention program, including up-front investment in appropriate staff and training, incorporating best practices, sharing threat intelligence with other firms, and developing a sound contingency plan, can minimize a company's exposure to most types of threats.

Even when a cyber attack does penetrate a well-defended system, the ability to rapidly respond may boost brand image by signaling competence to the public.

Mitigation: Insulate Against Remaining Risk

Preventing intrusions should be the first and most important step for data operators. But since cyber threats are ever-evolving, what happens when an attack cannot be prevented?

"80 percent of online attacks are due to a lack of basic cyber hygiene. Best practices can fix it. Another 15 percent can be addressed [through] information-sharing – 'see something, say something.' The remaining 5 percent can be contained: have a contingency plan for instant response, a series of backup systems, compartmentalized data [stores]."

Central to the discussion was **cyber insurance as a risk mitigation strategy**. Affected companies are exposed to risk on two fronts: business losses due to the theft of trade secrets, damage to network infrastructure, and brand reputation; and liability when consumer data is compromised. The US cyber insurance market, which arose in the last decade to cover such damages, is already purportedly valued at $2.1 billion and includes roughly 30 providers, including a handful of major players. The market in France is much smaller at €100 million, although insurers at the conference predicted European premiums to exceed $1 billion by 2018. Interest is strong in both countries, although the institution has yet to mature. One of the biggest insurance packages sold was valued at $500 million and insurers are paying out millions of dollars in claims per month to their subscribers. Depending on the provider, packages include coverage for legal defense, settlements, and judgments (third-party liability) as well as costs relating to breach forensics, breach notifications and disclosure, network interruption, extortion, and public relations (first-party losses).

The US is a more litigious society than France, and the US government has long recognized a role for insurance in protecting companies against cascading lawsuits in sensitive industries or with contracts relevant to maintaining national security. Congress passed the DHS "Support Anti-terrorism by Fostering Effective Technologies" (SAFETY) Act in 2002 specifically to prevent potential liability concerns from deterring US companies from developing or manufacturing anti-terrorism products. Under the SAFETY Act, designated products receive unprecedented immunities in civil court in the event they fail to prevent or respond to a "certified" terrorist attack as designed. The Price-Anderson Act, first enacted in 1957, represents a different model, providing for two tiers of liability insurance to nuclear reactor operators. As part of the first tier, reactor operators are required to obtain the maximum amount of insurance available from private sources. If the primary insurance is exceeded following a nuclear incident, a second tier is activated, requiring all operators to contribute to an industry-wide pool of about $12 billion. Similarly, Congress has repeatedly extended the Terrorism Risk Insurance Act (TRIA), which creates a mechanism that allows for primary insurance coverage for catastrophic terrorist attacks. Yet there is some concern about the circumstances in which cyber terrorism, were it to occur, would actually qualify under this law.[25] The

[25] Lang, Molly E. and John F. Mullen. "Is TRIA for Cyber Terrorism?" Insurance Journal, 21 Oct. 2013. Furthermore, even if TRIA were to apply to cyber terrorism, it would not apply to cyber crime or state-launched cyber attacks, although the Health Insurance Portability and

cyber insurance qualification process is also highly ambiguous for potential customers. Insurance providers at the forum acknowledged that some known limitations already apply; for instance, incidents not covered include physical destruction, cyber war (loosely defined), and confiscation of data or network infrastructure by sovereigns.

Despite acknowledged limitations, the demand for cyber insurance is growing in France. According to a PwC study, 52% of companies are ready to purchase cyber insurance, although only 5% currently hold policies.[26] Yet US-based cyber insurers wishing to expand their operations to overseas jurisdictions face numerous obstacles. The first is regulatory; there is no clear governing framework for cyber insurance regulation in either country, and the particular rules can even vary state-by-state in the US. Second, demand for insurance products may be driven by different factors in each country. Notably, the disparity in class-action suit law in each country means companies may face differential exposure to liability claims from French citizens, implying less overall demand for insurance from companies operating in French territory. Third, the cyber insurance market is characterized by considerable ambiguity: can insurers afford to pay out in the event of a catastrophic event? Will TRIA or similar systems apply? How robust is the market and what is its growth potential? On a more basic level, how do insurers decide who to cover – and, when they do, how reliable are forensic investigations, given that some kinds of cyber attacks may go undetected for months or years?

Underwriters describe the process by which applicants are approved as “holistic.” The evaluation process, which aims to ensure applicants have responsibly endeavored to minimize threat exposure before seeking insurance, was described as a qualitative assessment of the security posture of the entire company, from executive officers to lower-level staff (as a reflection of threat exposure). Evaluators also look to quantitative factors, such as the amount of the operating budget dedicated to cyber security. A serious conversation with an insurance broker about how your company is not “ready for cyber insurance” can actually facilitate a more serious approach to security.

On the other hand, cyber security and intelligence community representatives were highly skeptical of this approach, asking how insurers could credibly price their policies without knowledge of companies’ security posture on the technical side. According to one such critic, although seasoned insurance providers may understand traditional credit and market risk, operational resiliency is a “different animal.” Insurance representatives responded that they try to *“Shy away from prescriptive checklists, because if firms feel they’ve checked all the boxes, they’ll get too comfortable [and rest on their laurels].”* While hard to argue with, this rebuttal seemed unsatisfactory to many of the other participants. Presumably there is a methodology insurance companies follow when approving coverage, yet others in the room, which may have included prospective applicants, tended to perceive these standards as highly confusing and opaque.

Limited actuarial data hampers the growth and direction of the insurance market. Part of this is a function of the relative newness of cyberspace, as well as the difficulty involved in quantifying immediate losses when breaches occur. The future of the market will depend on the development and shape of national regulation, perhaps

Accountability Act (HIPAA) and various state-level privacy regulations may provide a template for other types of insurance relating to data loss.

[26] Thevenin, Laurent. “Pourquoi la cyber-assurance peut croire à son essor en France.” Les Echos. 1 Jan. 2016.

especially in Europe.[27] A concerted effort in the US is underway to gather more actuarial data, which may be available as early as 2016. As market actors that thrive on regulation, insurance providers present at the conference expressed a concomitant desire for clearer laws and standards.

Participants engaged in some debate over whether cyber insurance should be market-driven or mandatory. By one provider's own admission, *"without understanding what the risks are, you don't know what insurance you'll need."* The idea that cyber attacks can happen to anyone is an emergent norm that has not yet been fully internalized by much of the private sector. Market-driven demand for insurance may take some time to gain momentum. Mandatory insurance is certainly not an unconventional idea. It was likened to car insurance (although others did not favor this analogy), and even the SAFETY Act makes advance coverage a prerequisite for protection. However, proponents of the "mandatory" scheme were in the minority among conference participants. Another concern is whether cyber insurance offers enough to small- and medium-sized businesses. This particular question was left largely unanswered, perhaps because small business was underrepresented at this working group. It raises the question of whether smaller firms can even afford the security investments, much less the premiums, required by insurers.

The issue is complicated, and cyber insurance has not yet been widely adopted outside the US for many of the reasons outlined above. Nevertheless, participants generally embraced the idea since at the very least, the process promotes better defensive postures among interested applicants. Insurance can help protect companies' pocketbooks against the risk that remains when all reasonable proactive steps have been taken to secure one's networks. Better cyber hygiene minimizes risk and fits with the forum's call for new industry norms, and insurance providers complement this by insulating customers from the unlikely but calamitous.

Private sector participants as well as government officials – especially on the French side – expressed curiosity in cyber insurance, both because they were interested in it as a model for risk-insulation but also because it is still new and little-understood. Several aspects of cyber insurance ought to be made clearer for prospective private sector clients. Companies must understand the cyber insurance model if they are to know, first, whether coverage is justifiable on a cost-benefit level and, second, whether their internal security posture is sufficient to qualify for coverage in the first place. Several agencies in both countries, such as the National Association of Insurance Commissioners and French Federation of Insurance Companies, have already taken notable steps toward this end. However, more research and actuarial data are needed before cyber insurance can be endorsed without reservation.

Second, it is important to recognize that cyber insurance has its promise as a complementary strategy – not a panacea. As participants noted, insurance has the potential to help by transferring risk away from the victim, but it cannot directly displace the broader problem. Beyond this cautious qualification, insurance has an important secondary role to play: it can incentivize users to practice better cyber hygiene, thereby reducing overall risk. Information-sharing, discussed above, is only half of the equation – companies are primarily responsible for protecting their own networks. Because insurance requires prospective clients to reach and maintain certain protective standards before being approved for coverage, it can promote self-help among the most vulnerable

[27] Federation of European Risk Management Associations, "Cyber insurance market: incentives and improved cybersecurity for organisations." 24 Mar 2015.

players. The insurance industry should in turn work to make these standards more consistent and transparent, so that businesses can expeditiously reach the minimum security posture for the type of coverage that is right for them.

Cooperate with Law Enforcement Investigations

All agreed that cooperation with law enforcement is important in spirit, but substantive agreement on this issue was stymied in large part by the ongoing debate on encryption and data sovereignty. Discussing the *Microsoft Corporation v. United States of America* case currently before the US Second Circuit Court of Appeals, which considers whether federal search warrants can be used to procure data held on servers based abroad, tech industry representatives and US government officials engaged in a cordial debate but remained firmly entrenched in their positions. The participants noted that law enforcement's focus on evidence-collection tends to ignore companies' obligation to protect user privacy. Conflicts of law may also block companies from surrendering data even when they would otherwise be willing. Conversely, the private sector's narrow obligation to shareholders can easily overlook the broader mission of law enforcement and intelligence to secure national interests against the universe of threats, including criminals and terrorists, which could destabilize the wider economy.

Unsurprisingly, many in the private sector felt it was important to stand firm against government requests to install "exceptional access" in software (colloquially known as "back doors"), which would allow keyholders to easily decipher encrypted information, out of privacy and data sovereignty concerns. Another argument put forward is that back doors are actually harmful to security in the aggregate since the more countries a company operates in, the more holes will exist in the network.[28] Even if parties could agree that back doors are appropriate, they are "really, really hard to get right," according to cryptography experts.[29] Conversely, the absence of available back doors may provide an incentive for authorities to break in the hard way – or, worse, to refrain from advising companies of underlying security flaws discovered in their networks.

Beyond seamless cooperation and transparency, speed when dealing with foreign-held companies is also a factor. French officials complained that obtaining the data of alleged terrorists through normal channels costs law enforcement authorities precious time needed to prevent possible attacks or apprehend suspects. Government representatives, especially in the US, stressed the need to be able to read encrypted data in order to prevent and punish extraordinary criminal activities. French participants were most concerned about the threat of internet-facilitated terrorist acts. American participants concurred to a large degree, although they were more concerned about industrial espionage, which they held to be the more common and pressing issue. This discussion was especially prescient given the heinous attacks on innocent civilians in Paris and San Bernardino, California, by suspected ISIS operatives three months following the conference. Authorities have speculated that the attacks may have avoided advanced detection because the attackers were using encrypted communications.[30]

Recognizing the delicate balance between security and privacy, the international working group collectively expressed the need to tread carefully on this issue in the future. These debates were not immediately resolvable, and progress will require continued discussion, as well as a greater effort to foster trust on the part of government and more flexibility on the part of private data operators. When exercising discretion over whether to surrender

[28] Healey, Jason. "Opinion: Poisoning the Internet won't stop more Paris attacks." The Christian Science Monitor. 17 Nov. 2015.
[29] Bellovin, Steven. "The danger of 'exceptional access.' " CNN Opinion. 18 Nov. 2015.
[30] Bruer, Wesley. "FBI director reiterates need to be able to read encrypted data." CNN Politics. 18 Nov. 2015.

user data when requested by law enforcement, companies should be especially cognizant of whether cooperation serves justice and security for the whole cyber community, since these issues have far-reaching consequences for the broader public.

Participants drew a distinction between cyber attacks such as computer network attacks or electronic espionage and cyber-*enabled* acts such as hate speech, which may be criminalized in some localities but not others. Bilateral law enforcement should focus primarily on the former; those acts not considered dually or universally criminal should instead be negotiated politically, with deference to the right of countries to manage their own affairs.

Looking Forward

A fundamental tension exists between cooperation in cyberspace – which everyone agrees is necessary for long-term sustainability – and near-term security and economic needs, which often impede cooperation. Cooperation must take place between actors at all levels: bilateral, public-private, and private-private, but there is a tendency for immediate concerns to overshadow future security. Positive incentives can help. Limited negative incentives, such as penalties for noncompliance, also have a place for keeping serial rule-breakers in line. However, trust remains the key.

The US government in particular seems especially appreciable of its trust deficit with US and foreign industry and has been working to rebuild some of that trust. The tactics used to pursue suspected cyber criminals and secure national interests, however, often put governments at odds with the operators it is trying to protect. There is a tendency to rely on government alone to cultivate this environment of trust, but we could also could benefit from greater leadership by the private sector. Business and government may not always see eye-to-eye on the issues, and businesses themselves may very often see each other as competitors in the marketplace, but the cyberspace in which everyone operates is fundamentally interconnected: legitimate users benefit from greater security.

Working group participants, drawn from the intelligence, law enforcement, cyber security, academic, and business sectors in France and the US, identified a number of conclusions as they discussed the nature of evolving cyber threats in the two countries, the respective responsibilities of different actors, and the utility of various risk mitigation strategies.

Achieving greater trust and cooperation remain paramount objectives, since participants identified it as an essential step to achieving greater security. An existing deficit of trust exists:

- Internationally, even between allies such as France and the United States. Moreover, France and the United States can play an important role working together to promote international norms in cyberspace.
- Within the government. This was particularly noted with respect to the US government, where different agencies have overlapping responsibilities, unlike the more centralized structure adopted in France.[31] In both countries, participants noted a persistent problem due to an intelligence arm that

[31] In 2013, the US Government Accounting Office asserted, “Cybersecurity strategy documents have assigned high-level roles and responsibilities but have left important details unclear. Several GAO reports have likewise demonstrated that the roles and responsibilities of key agencies charged with protecting the nation’s cyber assets are inadequately defined.” United States Government

"sees everything but does nothing," and a law enforcement arm that has the power to act but is blindfolded by due process.

- Between the public and private sectors. Cooperation by the private sector with law enforcement represents a particular challenge, one that is complicated by questions related to consumer privacy and data sovereignty.

To that end, much discussion was dedicated to examining the respective roles of the private and public sectors, centered on this tension related to a perceived lack of cooperation with government actors by the private sector and a frustration voiced by the private sector that they are left to fend for themselves in cyberspace.

Government is responsible for promoting new international norms in cyberspace, providing greater coherence and clarity on domestic computer crime and data breach laws, facilitating better cooperation within government, and providing assistance and services to the private sector. Participants explicitly recognized the need for a Cyber 911. In the US, DHS and US-CERT are positioning themselves as a cleanup crew of sorts, but it remains unclear whom to call during an ongoing emergency, especially in the US. Removing the stigma of a breach is an equally important step to achieving greater cooperation between the public and private sectors. Meanwhile, the private sector is tasked with promoting new industry norms, which would incentivize an investment in robust defense measures, encourage timely disclosure of breaches and the sharing of threat information, and promote the adoption of risk mitigation measures when a breach does occur.

As participants acknowledged, improving cyber hygiene is crucial to preventing most attacks, even if it is impossible to achieve zero cyber risk. Consequently, risk mitigation tools, notably in the form of cyber insurance play an important role. Cyber insurance has utility not only for the protection it can provide but because it also can serve as an incentive to promote better cyber hygiene. It remains to be seen whether the adoption of cyber insurance will be driven by a market process or ultimately be made mandatory like car insurance. However, it was a minority view among participants that cyber insurance should be required.

Since the conclusion of the conference, France and the US both passed legislation touching on key issues raised by the international working group. France published its National Digital Security Strategy[32] in October, one month after the forum's conclusion. Prime Minister Valls alluded to his government's recognition of a need to maintain a balance between security, civil liberties, and market fortitude. The strategy includes boosting staffing for ANSSI, a signed charter between French telecommunications firms to fortify email defenses, raising awareness of the importance of cyber security and of the growing problem of cyber risks across French society, and providing additional support to small and medium-sized enterprises, among other measures.[33] Though reporting requirements are stringent in France, the National Assembly followed up in January by passing the Bill for a Digital Republic, which codifies certain digital rights.[34]

Accountability Office. "Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented." Feb. 2013. http://www.gao.gov/assets/660/652170.pdf

[32] Office of the Prime Minister. "French National Digital Security Strategy." 16 Oct. 2015. http://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf

[33] "National digital security strategy: "a good balance between security considerations and economic dynamism." 19 Oct. 2015. http://www.gouvernement.fr/en/national-digital-security-strategy-a-good-balance-between-security-considerations-and-economic

[34] "The Digital Bill." 26 Jan. 2016. http://www.gouvernement.fr/en/the-digital-bill

In tandem, the European Parliament passed the Network and Information Security Directive,[35] which creates new reporting obligations for companies operating in Europe. European member states will be individually responsible for designating which companies within their borders must comply with the new requirements. In a statement on Twitter, Andrus Ansip (European Commission Vice-President for the Digital Single Market) called for increased trust.[36] Given that the new reporting requirements are mandatory (and that companies that violate them are subject to sanction), the law seems unlikely to add much to the fabric of trust but will certainly benefit security in key sectors, if managed adeptly.

After repeated failures by Congress to agree on a cyber security package in recent years, the Cybersecurity Information Sharing Act passed both chambers of Congress with overwhelming support and was signed into law by President Obama in December as part of an appropriations bill. It purports to streamline information-sharing by offering incentives to companies to cooperate. However, some feel that the law is not sensitive enough to data privacy concerns. Before becoming law, the bill had been considered highly controversial by major tech firms;[37] more than 50 digital rights groups wrote a letter to Congress critical of the bill in the days before the vote.[38] The tension between security and privacy is an ongoing one, and US leaders must walk a difficult path between remaining vigilant against pervasive cyber threats and alienating private operators, whose trust must still be earned. Despite this, the law contains provisions that help protect certain companies against liability exposure when surrendering data to law enforcement, promising to help ameliorate an ongoing sticking point between the government and US companies.

Participant recommendations anticipated the direction of US and EU legislation, as participants grappled with the respective responsibilities of the public and private sectors and the need for greater trust between the sectors. Since its first Cyber Security conference in 2012, the French-American Foundation's cyber initiative has promoted frank dialogue on challenging issues related to cyber security by providing an informal discussion setting for a select group of cyber experts. The Foundation has established the utility of such informal forums, since they help set the agenda for policymakers' priorities, encourage the sharing of best practices from both countries across different sectors, and promote new connections among cyber professionals.

Despite several differences in the French and American institutions and approaches, the cooperation framework is underpinned by mutual commitment to the same essential principles, including freedom of expression, respect for the rule of law, and the protection of individual rights. As the cyber domain evolves with new and sustained threats, there will always be room for further collaboration. With an eye to this, the French-American Foundation, with generous support from its partners and sponsors, remains committed to bringing together key decision makers from both countries to address new challenges and propose new solutions.

[35] European Parliament News. "MEPs close deal with Council on first ever EU rules on cybersecurity." 7 Dec. 2015. http://www.europarl.europa.eu/news/en/news-room/20151207IPR06449/html/MEPs-close-deal-with-Council-on-first-ever-EU-rules-on-cybersecurity

[36] Ansip, Andrus. Twitter post. 7 Dec. 2015. https://twitter.com/ansip_eu/status/674132695446888448

[37] Risen, Tom. "Cybersecurity Bill Passes in Senate." US News. 27 Oct. 2015.

[38] Letter submitted by Civil Society Organizations to U.S. Congress. 17 Dec. 2015. https://static.newamerica.org/attachments/12218-51-civil-society-groups-and-security-experts-tell-congress-they-oppose-cyber-legislation/FINAL_Civil_Society_Security_Expert_Letter%20Opposing_CSA_2015.efca7165edbf4beaa392e5ef66cfff70.pdf

ABOUT THE FRENCH-AMERICAN FOUNDATION

Founded in 1976 in New York and Paris and building on more than two centuries of shared ideals between France and the United States, the French-American Foundation works to enrich a transatlantic relationship that is essential in today's world. The French-American Foundation brings together leaders, policymakers, and a wide range of professionals to exchange views and share experiences in areas of mutual concern for mutual benefit.

The Foundation addresses several current policy issues including education; immigration; security and defense; business and the economy; energy and the environment; urban development and renewal; health care; and cultural policy. Programs include its signature Young Leaders program, conferences, high-level professional exchanges, and study tours for leaders in government, business, academia, media, and culture, creating a rich network of people and ideas for action.

FRENCH-AMERICAN FOUNDATION
United States

FRENCHAMERICAN.ORG

FRENCH-AMERICAN FOUNDATION FRANCE

FRENCH-AMERICAN.ORG