INTERPOL

FRENCH-AMERICAN FOUNDATION FRANCE

FRENCH–AMERICAN FOUNDATION United States

September 15-16, 2016

CYBER SECURITY AND THE LAW

Cyber Security and the Terrorist Threat

Washington, DC

Conference Report

Smarter Together

With the support of

FiTS

International Forum on Technology and Security for a Safer World

The statements made and views expressed in this report do not reflect the views of the French-American Foundation nor its directors, officers, employees, representatives, sponsors, or the rapporteurs. Instead, this report documents the views expressed by participants at the conference *Cyber Security and the Law* held on September 15-16, 2016.

To facilitate an open discussion and exchange of ideas, this conference was conducted under the Chatham House Rule. When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.

Steering Committee

The 2016 conference on *Cyber Security and the Law* of the French-American Foundation was organized by a Steering Committee whose members convened every month to select the themes, topics, and questions to be discussed at the conference.

The members of the Steering Committee are:

President of the Steering Committee

Jean-Paul Paloméros
Former NATO Supreme Allied Commander Transformation
French-American Foundation – France

Members

Aurélie M.H. Beaumel
Co-Owner and CEO
Business Interactive Games

David Benichou
Senior Criminal Investigation Judge
French Ministry of Justice

Pierre Calais
Chief Executive Officer
Stormshield

Allan Chapin
Chairman
French-American Foundation – United States

Frédérick Douzet
Professor of Geopolitics and Castex Chair of Cyberstrategy
IHEDN

Herbert Fenster
Senior of Counsel
Covington & Burling LLP

Camille François
Senior Researcher at Jigsaw/Google
Google Ideas

Yves Le Floch
VP, Head of Cybersecurity International Business Development
Capgemini

Jean-Louis Gergorin
Co-Founder
French-American Foundation – France

Pierre Jeanne
VP, Information Technologies Security Domain
Thales Communications & Security

Nicolas Naudin
VP
Airbus Group

Olivier Piou
Founder and Board Member
Gemalto

André Viau
Prefect
Ministry of the Interior
Honorary President
FITS (International Forum on Technology and Security for a Safer World)

Table of Contents

1 Introduction

At a critical moment for international cooperation in cyber security, the French-American Foundation convened its third annual forum on Cyber Security and The Law, focused on The Terrorist Threat, in Washington, DC on September 15-16, 2016. The forum was organized under the patronage of INTERPOL and with the support of the International Forum on Technology & Security for a Safer World (FITS).

This year's international forum brought together approximately 50 French and U.S. government officials, leaders of industry, and other experts to discuss different aspects of the terrorist threat and violent extremist groups' ability to leverage digital tools. It also included a discussion of the current landscape of international governance in cyber security.

Three sessions focused on different aspects of the terrorist threat and on violent extremist groups' ability to leverage digital tools: countering recruitment efforts online, evaluating terrorist groups' ability to launch cyberattacks on critical infrastructure, and finally considering violent extremist groups' use of popular cryptographic tools and its impact on current investigations.

Discussions on international cooperation and governance in cyber security included a panel to discuss norms in cyber space and a brainstorming session to design the mandate and structure of a potential international cyber security agency.

2 Countering Efforts of Violent Extremist Groups in Online Recruiting

Online tools, such as social networks, have become a major component of the propaganda toolkit used by violent extremist groups to recruit new members. A major challenge for law enforcement and the judiciary is to make terrorist-related content less accessible online. Solving this challenge requires identifying questionable online content and linking it to specific threats. Online censorship and learnings from the fight against online child pornography could be adapted for the online fight against terrorism, though challenges remain for governments to work with social networks and hosting companies to remove content from their sites.

Other ways have also proven their effectiveness in reducing general terrorist recruiting, through international cooperation, fieldwork with

local communities, and preventing the inception of propaganda at the source.

2.1 Online propaganda for terrorist recruiting

While the use of propaganda by terrorists is not new, the fight against terrorism is now taking place on online media. Over the last fifteen years, terrorist groups have used Internet networks very effectively for fundraising, command-and-control, and communication with a broad international reach. For instance, Al Qaeda was able to cascade information from Pakistan to cells elsewhere in the world through online channels. More recently, intelligence revealed that the top recruiter for jihad in Syria was born and based in Belgium. Among individuals prosecuted in U.S. courts for terrorist-related activities, most are less than 25 years old and a third are less than 21 years old. Online social media plays a key role in radicalizing young people over the Internet and is tied to almost all of these cases. Before the Internet age, one had to meet another person in the real world in order to be recruited and commit terrorist acts. Nowadays, young people, who discover and make friendships online, currently constitute the main recruiting targets for terrorist groups. Anecdotal evidence gathered by French journalists suggests that a young and unstable 16-year-old French-speaking Muslim can face terrorist recruitment online within 2 months after the first contact on social networks.

2.2 Making terrorist-related content less accessible online

The first step in making terrorist-related content less accessible online is to identify questionable content and link it to specific threats. Smartphone applications developed by ISIS are not distributed through Google or the typical app store, but through their own websites. Terrorists have developed specific content for the French-speaking public by people who have been in France and may now be in Syria or other countries. While there exists an online community of radicalized people and thousands of related websites, only a small percentage of them pose a real threat, and the rest are distractions for investigators. This is a typical problem of finding a needle in a haystack. Both U.S. and French investigators agree that a multi-pronged approach, combining undercover operations, human intelligence, and signal intelligence, is the best way to differentiate between real threats and noise. In France, covert investigations have

linked online messages to their specific authors who turned out to be individuals with weapons in their homes and ready to carry out attacks. These people are now under the radar of intelligence services.

Removing or blocking terrorist-related content online is a form of online censorship. One point of view expressed in France defends the legitimacy of the state to censor terrorist-related content online, on the basis that the media is part of the battlefield in the war against terrorism. This group views censorship as a way to enforce community rules and posits that the French state can blacklist websites, i.e. restrict their access in France. The French Parliament has also created a new criminal offense for accessing jihadist websites, punishable by up to two years in prison. However, technical difficulties are inherent to any implementation, as it is challenging to link online activities to specific individuals in the real world. Online censorship ultimately is a question of social responsibility: to what extent should there be frameworks to allow censorship of questionable content, or should the Internet be free and open? In this respect, the U.S. differs from other countries due to its unique First Amendment that guarantees free speech. In addition, the U.S. business environment does not allow online platforms to be held liable for the content they carry. The French perspective is that websites inciting violence should not be protected by any free speech law and that it should be possible to block them. The question then turns to the framework to do so: who defines what is appropriate content, how can one agree on criteria for free speech? While it may be easier to achieve consensus for extreme cases, problems remain in the grey zone. For instance, should pictures taken by witnesses of terrorist attack scenes be blocked?

There may be some lessons to be learned from the successful fight against online child pornography, adaptable to the fight against terrorism online. Restricting the distribution of terrorist-related content is not a free speech issue or a technological problem, but a policy stance. As in child pornography, algorithms could be used to automatically recognize images and videos with content that is unquestionably inappropriate. This content could be hashed and blocked automatically, or websites could be asked to block it. In the past, companies have cooperated with the government to enforce such measures for online child pornography. Those companies can be asked to do the same for terrorist-related content. The objective is not to block or remove all content, but to remove it from obvious places. Framing the debate away from trying to block every instance of objectionable content on the Internet towards working with popular websites to amend their terms of service to prohibit certain kinds

of content can achieve many of the same goals, without the need to censor the web. Any successful transatlantic cooperation on this issue would have to respect the U.S. First Amendment in order to have any chance of going forward on the U.S. side.

It remains a challenge for governments to work with social networks and hosting companies to remove content from their sites, though recently the dialogue with industry has improved regarding the removal of undesirable content. Recent events such as the Apple vs. FBI case show that U.S. authorities can be challenged by perceived alternative centers of decision in Silicon Valley. Companies such as Apple, Google and Facebook are not held accountable for the content they host, but they enforce private rules and community standards. In addition to restrict online content, some of these companies also use a different approach based on developing counter-narratives of unknown effectiveness to counter extremist propaganda. Going forward, there needs to be a common voice on this issue, across industry and government, and across governments of different countries.

2.3 Other ways to reduce recruiting effectiveness

International cooperation is a central component of the fight against terrorism, including terrorist recruiting. The U.S. and France have been close partners on managing threats for a long time. The U.S. started a national initiative in Washington, DC to work with international partners. France is also pushing for the development of a common dialogue within Europe, as well as for better dialogue with the U.S. and other countries. The successful cooperation between the U.S. and France should expand to other countries. The type of joint international investigations led against terrorist online activities are the same as for other international cybercrimes: who developed the website and content, who manages the web servers, how were domain names and servers purchased? However, in the case of terrorist-related propaganda, these investigations may need to be conducted in far-off countries or countries at war, posing serious challenges for investigation, and highlighting the need for international cooperation. Westerns nations can make efforts to remove online terrorist-related content and deny online space, but they need to cooperate with Muslim institutions and nations who can have more influence and authority in the regions where terrorist groups are based.

International cooperation should go hand-in-hand with field work and

outreach to Muslim communities at home. Both the U.S. and France agree that it is of utmost importance to foster a dialogue with Muslim communities at the domestic level. For example, a prevention mechanism used in France is the hotline set up by the program Stop Djihadisme, to enable people to report individuals they know who may be influenced by terrorism propaganda. This is not a fight between positive and negative messages. Counter messages are typically not so effective, especially when coming from governments. Instead, where possible, there needs to be a dialogue between governmental authorities and people within the communities who can influence their peers.

Finally, another way to limit terrorist-related online propaganda is to restrict information distribution at the source. The Internet does not exist by itself. It relies on a small network of satellites and fiber optics, with all major access points controlled by the coalition. Since the beginning of 2016, there has been a significant decrease in online propaganda activities by ISIS, thanks to the coalition military operations ongoing in its region.

2.4 Future outlook

Going forward, several challenges remain to reduce terrorist-related online content. From an investigative perspective, there are questions on which investigative techniques produce the best results, how human intelligence can be used further, and how to work better with partners. Terrorist groups like ISIS are very innovative, adaptive, and have a very integrated digital action based on a multiplicity of distribution systems. They moved to Telegram when Twitter became overly restrictive and will move on to the next set of tools when it becomes necessary. History suggests that they will utilize tools used by the general public, covert enough for their purposes, but not too obscure. For companies developing new communications tools, it must be assumed that they will be used by terrorist groups, and there needs to be a dialogue from the start between these companies and authorities, which is currently not always the case.

The fight against terrorist online recruiting can be framed in two different ways. As discussed in this section, it can be about creating an Internet free of terrorist-related content. However, it is difficult to identify and remove all questionable content on the Internet, and one must tread the path of censorship with great caution to avoid abuses and to not give legitimacy to the practices used by authoritarian regimes. Another way to address the problem is to work with popular sites to remove

highly visible content and thereby prevent terrorists and extremists from effectively reaching out to like-minded individuals. This effort would require also more work and investments in finding and monitoring dangerous individuals so that propaganda can be stopped at its roots. Combating terrorists on-line is ultimately a fight against an ideology, one where the overall objective is to neutralize extremist combatants who aim to kill societies from the inside and not to change societies.

3 Use of Cryptographic Tools by Violent Extremist Groups

Over the years, terrorist groups have become very adept at using new technologies, including encryption. In 2007, terrorist groups already used encryption and disseminated this technology. With the advent of social media and mainstream apps supporting encryption by default, such as WhatsApp, Telegram, or Tails, these cryptographic tools have become so widespread that there is no need for terrorists to create their own software. In contrast with just a few years ago the U.S and France now agree that there is no point in creating backdoors and key escrows which create even more risks; instead there are already other ways available to investigators to counter the terrorist use of cryptography.

3.1 Backdoors and key escrows are not a solution

By definition, an investigation is a breach of privacy. This is not a debate between security and privacy. It is a trade-off between short-term investigations and long-term national security. The issue of encryption is not specific to terrorism, but to all crimes. If investigators cannot listen to phones and conversations, it is harder for them to solve cases. On the other hand, there is widespread support for strong encryption. It is the best security against mass surveillance and a strategic advantage for Western countries and democratic societies.

As the technology and know-how for encryption are freely available, it is impossible to prevent anyone including terrorists from designing and implementing their own encryption.[1] Regulating the availability of strong encryption is not going to prevent terrorists from using it. Even if laws are passed, only honest people will comply.

[1] All of the 8-9 applications that ISIS recommends for encryption are based on open-source libraries and authored by companies outside of the U.S. and France.

Since regulation fundamentally cannot solve this problem, investigators need to turn to other technological approaches to collect lawful evidence. While encryption removes one way of accessing information, technology can enable many more.

3.2 Countering terrorist use of cryptography

Two effective methods for bypassing encryption are human intelligence and device hacking. For device hacking, there is a difference between a backdoor in a device and targeted hacking. Hacking can be used in many ways to bypass encryption, and as long as software is not provably secure, it is almost always possible to break into a device with enough effort. The U.S. has made significant investments in its intelligence organizations to develop tools that are able to work around encryption. However these tools may not readily be available to law enforcement organizations.

When contemplating the investigative challenges posed by encryption, it must be remembered that we live in a golden age of information, with huge amounts of stored communications data on mobile phones and other devices. This presents both challenges and opportunities for investigators. Similarly, in the last century, the appearance of cars provided new opportunities for both criminals and investigators. Criminals use the same infrastructure as normal people. This is ultimately about the security of social infrastructure. It is not only about encryption, but the whole ecosystem that surrounds it. Evidence can not only be found in software, but also on servers. Before, investigators had to deal with physical servers. They had a warrant and knew what to take. Today, the development of Cloud technology has made it more difficult for investigators to identify which data to confiscate. Every new data-related technology will pose challenges to investigations, but will also present opportunities.

3.3 Future outlook

Over the past thirty years, technology has advanced at a very rapid pace, but the law has not followed suit. The existing legal framework is no longer appropriate for handling complex technological issues, and it is necessary to modernize laws in the U.S., France, and other countries. In the U.S., the current legal environment is still largely defined by the Electronics Communications Policy Act of 1986.

There is a fundamental mismatch between the state of technology and the legal frameworks in countries across the board. Governments

and citizens need to think collectively about what they are comfortable with in the digital world. In the U.S., the constitution has historically made the argument that there is nothing beyond the reach of the rule of law. While the legal court system can have access to all information, encryption technology has outstripped that legal framework. The legal framework is no longer sufficient to compel companies or individuals to provide information. However, this type of debate cannot take place in the aftermath of a major trauma to a nation, such as after major terrorist attacks. History has shown that decisions fueled by emotion can have negative long-term consequences.[2]

One must think about all of the stakeholders involved (i.e. companies, governments, academia, individual citizens). Policymakers need to appreciate the technical subtleties, and technology experts need to appreciate that these are policy decisions. The main issue for law enforcement is that technology is evolving very quickly. Law enforcement organizations need to be able to do their job, while respecting individual rights and sovereignty. There needs to be more training of law enforcement officers on understanding technology, with better cooperation at the national, European, and international levels. It is not critical to understand everything, but there needs to be a common understanding of the range of implications.

4 Risks of Potential Cyberattacks against Critical Infrastructure

Over the last year, there has been less focus on potential cyberattacks against critical infrastructure, and more on data manipulation and data theft for strategic purposes. However, the major hack perpetrated against the Ukrainian power grid about a year ago (which could have been a lot worse, save for its older and analog components which limited the reach of the attack) is a stark reminder of the real threats that such attacks embody. In both the U.S. and France, the largest threats for critical infrastructure are considered to originate from aggressive nation-states and to a lesser extent from terrorist groups.

The protection of critical infrastructure against cyberattacks relies on three pillars: (1) the definition of critical infrastructure, (2) the

[2]For instance, the internment of U.S. citizens of Japanese descent during WWII after the attack on Pearl Harbor.

principles of cyber security for critical infrastructure, and (3) the division of responsibilities between governments and private companies managing this infrastructure.

4.1 How to define critical infrastructure

The first step in defining a strategy to protect critical infrastructure against cyberattacks is to define criteria to assess the criticality of every single part of selected systems contributing to essential/vital functions. Here, the challenge is to develop a comprehensive enough approach while keeping it precise and specific in order to avoid exponential inflation in the number of critical systems. Traditionally, critical infrastructure has been associated with heavy industry (e.g. power plants). However, the proliferation of data has created implications for the types of infrastructure that should be categorized as critical. For instance, the recent series of cyberattacks against the Democratic National Committee and the disruption they can cause in the U.S. election cycle may suggest that a voting system, especially an online system, is also critical infrastructure. These experiences show that it would now be preferable to speak of critical systems rather than infrastructure. In France, critical infrastructure companies have been identified by the ANSSI authority as OIV (Opérateurs d'Importance Vitale) and will soon have to comply with cyber security requirements defined by the ANSSI.

4.2 Cyber security for critical infrastructure

There is consensus among experts on the fundamental cyber security principles that must underlie the data and systems of any type of critical infrastructure. They revolve around breaking up, isolating, and segmenting the various components of a system, to minimize the impact of a cyberattack, and hence improve the overall resilience of the system.

A major aircraft manufacturer relies on the following approach to manage cyber risks in its global production chain:

- Domain partitioning / Segregation: Differentiate sensitive and critical systems that require the highest level of security and cannot afford to be breached, from open systems that are less critical
- Security of all interfaces and access points: Identify and protect the areas that are most susceptible to attacks

- Integrity of the overall architecture in service: Ensure that the security principles laid out in the overall system architecture are still respected, even when the system undergoes modifications after its delivery to the customer

Today, Chief Information Officers (CIOs) of companies tend to focus mainly on Information Technology (IT), i.e. data management and protection of data integrity. However, most cyberattacks on industrial systems are targeting Operations Technology (OT), notably supervisory controls. Cyber security of critical infrastructure therefore entails both IT and OT security. There needs to be a shift from IT and compliance towards an integrated approach of Enterprise Risk Management that combines all functional domains (IT, OT, telecommunications, physical silos, etc) and the supply chain, as suppliers who have access to company systems can themselves become sources of threats. Executives in the boardroom should not underestimate the blended cyber threat that can come from so many different areas.

4.3 Responsibilities of governments and the private sector

Public-private partnerships and cooperation are essential to ensure the security of critical infrastructure against potential cyberattacks. However, the specific roles of the private sector vs. public authorities remain to be clearly defined, in order to establish who is responsible for defending against cyberattacks. Public-private partnerships can easily go too far when private companies rely on governments for basic security for which they themselves should be responsible. A suggested leitmotiv could be the following: if a cyberattack on a private company has a national defense implication, then it should be the government's responsibility to address it. The roles of the private sector vs. governments will vary by nation. In the U.S., the key questions revolve around the military, the defense aspect, and the defense implications for the nation. There is therefore an expectation that the military is going to be responsible for defending critical infrastructure against major cyberattacks.

4.4 Future outlook

From established consensus on the general approach and principles to defend critical infrastructure against potential cyberattacks, countries like

the U.S. and France need to continue their efforts to promote partnerships and share valuable information. Partnerships between governments and the private sector must be taken at a higher level and will require innovative approaches. The current approach is not sufficient and doing more of the same is unlikely to generate different outcomes.

There is value in sharing threats between stakeholders within an industry and across industries. If shared openly, the lessons learned from a cyberattack on a given company could benefit many others and help them from repeating the same mistakes, thereby increasing overall industry security. The goal is to share information when a cyberattack happens. Governments need to find ways to encourage companies to share information with each other and with the government regarding cyberattacks. For instance, in France, a new law will allow government agencies to request incident reports from companies.

Potential areas of development to counter cyberattacks include advances in machine learning/AI for better and faster detection of attacks and their mitigation, on the reactive side of cyber security. On the proactive side, simulations also offer great potential to improve infrastructure security, by providing an environment where one can fail safely and learn without consequences. In France and the U.S., public security and military organizations regularly use simulations in labs and integrated cyber trainings to teach cyber security experts and general staff to deal with the consequences of cyberattacks. NATO has developed a Center of Excellence in Cybersecurity based in Estonia. Going forward, even more cooperation will need to be developed between nations that are connecting critical infrastructure.

5 Towards International Norms for Cyber Security

Cyber security has evolved from a niche subject into a national-level challenge that is shared by governments across countries. Unlike the physical world which is fixed, cyber space keeps expanding and cyber threats are evolving rapidly. Different kinds of malicious actors, such as criminals, nation-states, and activists have moved to cyber space. Increasingly, these actors are finding that they can use cyber space to pursue their ends. The number of malicious actors will increase, and they will increase their number of activities. The Internet of Things (IoT) will make this concern only larger by turning cars, household appliances, and

other devices of human daily life into potential threat factors.

Norms are about expectations. In the early days of the Internet, security was taken for granted. Norms became obsolete when the Internet technology outgrew its founders and the web became a space for all sorts of activities (business, social, military, criminal, etc). However, cyber space is not different from other international spaces (e.g. oceans) in terms of establishing and enforcing norms. Progress has been made, notably by the U.S. and its partners, to establish norms for acceptable behaviors in cyber space.

5.1 Norms and cyber espionage

Recently for the first time, the U.S. Justice Department named and prosecuted foreign nationals, leading to the first indictment of citizens of the People's Republic of China for cyberattacks used to steal trade secrets and intellectual property from various U.S. businesses. The Chinese cyberattackers had a joint-venture with a U.S. multinational company and used the full apparatus of the Chinese military (management, labor) to steal information from U.S. companies. The direct involvement of the Chinese military was made obvious by the scale of the cyberattacks.[3]

The same rules should apply to criminals, terrorists, or nation-states for unlawful actions in cyber space, as they do in other spaces. The norms for cyber space are not unique to a culture. They have larger appeal and can be adapted from other spaces. The indictment and the threat of U.S. sanctions made the Chinese government take the issue of cyber espionage seriously. This indictment was an explicit articulation of a norm against commercial (cyber) espionage. Sanctions can help create norms. Violations of norms could lead to deterrence in the form of retaliation hacking. Spies have been prosecuted for ages and there is indeed no reason that cyberspies cannot be prosecuted as well.

5.2 Progress for norms in cyber space

Cases of cyber espionage, such as the one described above and other high-profile cyberattacks like the North Korea cyberattack against Sony, have highlighted the need for norms and rules of the road in the Wild

[3]Recently, the U.S. also named Russia as the foreign power responsible for cyber thefts and disclosures aimed at disrupting a major internal political process, namely the U.S. Presidential election.

West of cyber space. There is an emerging consensus that international laws should also apply in cyber space.

The case of Chinese cyber espionage led to the establishment of a unilateral U.S. doctrine later accepted by China and also the G20, stating that large-scale government- or military-sponsored hacking for economic benefit is unacceptable and will be retaliated against by governments. A hotline was established between Washington and Moscow, and is currently in progress with China. The U.S. expects international laws and other countries to respect the following key norms:

- No disruption or destruction of critical infrastructure
- No government support for stealing trade, economic, and IP data
- No interference with incident response
- Cooperation with request for assistance

The U.S. administration has established a policy framework through Presidential Policy Directive 20 (PPD20) aimed at establishing norms and processes for cyber security, in compliance with U.S. values. Operationally, it has tried to apply lessons from counter-terrorism and has pursued a three-pronged strategy:

- Raise level of defense in short and medium term
- Deter, disrupt, and constrain adversaries
- Improve incident response capability and be more resilient

The objectives are to improve the toolkit to combat adversaries, to increase capabilities in attribution, and achieve strategic stability in cyber space. The U.S. Cyber Threat Intelligence Integration Center was created in 2015 as a national intelligence center focused on "connecting the dots" regarding malicious foreign cyber threats to the nation and cyber incidents affecting U.S. national interests, and on providing all-source analysis of threats to U.S. policymakers.

The U.S. wishes to foster advantages to cooperation and to encourage governments around the world to innovate instead of stealing information. Deterrence in cyber space has been pursued for some years now. It seeks to impose costs through law enforcement. There will always be bad actors. The question is about how costs can be imposed by norms and

international laws so that states have no incentive to engage in disruptive behaviors. Though much remains to be done, the U.S. and their partners have already achieved progress towards establishing norms in cyber space, at a very fast pace for policy.

5.3 Future outlook

Going forward, building on the foundations established by the G20-endorsed doctrine, it will be necessary to find ways to institutionalize these norms and to gain acceptance as well from the private sector. This will require better information sharing between intelligence services and law enforcement. Western allies need to continue to work together to expand these norms. There is more understanding of the issue of cyber security than ever before. What used to be the province of technical geeks and law enforcement has become a mainstream concern. The initial toolbox needs to be made bigger and filled with more tools.

Further progress is also needed in terms of attribution in cyber space. Attribution can influence perspectives and responsibilities. In the Sony case, while the company was initially deemed responsible for not being sufficiently protected, once it was revealed that the attack was conducted by North Korea, the perceived responsibility was shifted away from the company to the governments who let it happen. Though attribution does not necessarily mean public attribution, it can be used for deterrent actions (e.g. naming, shaming, sanctions). If one worries about getting caught, it becomes harder to conduct criminal actions and requires more careful decisions.

6 Brainstorming: Modeling an International Cyber Security Agency

The final session of the seminar consisted in a brainstorming session on how to define a potential international agency for cyber security, using inspiration from similar concepts existing in other fields. Several individual cyber security initiatives already exist across countries and also in international organizations (e.g. NATO Cyber Security Center of Excellence), but there remains a need for more consistent approach, mandates, objectives, and methods.

Based on the discussion, the scope of such an agency could include the following:

- Threat sharing
- Assisting with attribution
- Establishing repository of technology and processes for use by public and private organizations
- Protecting global commons: monitoring, control, and sharing of best practices

Even the promotion of basic principles could go a long way in enhancing overall cyber security. Nowadays, 80% of attacks are simple to detect and defend, 15% could be avoided through better sharing of information and best practices, and only 5% are hard to detect and defend against.

The field of aviation offers a valuable analogy. After the advent of airplanes and their widespread use for private, commercial, and military purposes, international agencies were established to help with the implementation and promotion of norms for security regulations and safer air transport systems, which became widely accepted. However, unlike aircraft control (or space or weapons control) for which new technical capabilities are long to implement and can be foreseen, technology in cyber space evolves at a much faster pace.

The establishment of an international agency requires international cooperation, as well as good public support and participation from both the public and private sectors. One of the key attributes of cyber security is the need for speed, and the private sector often has the information before the government does. It is also important to follow an appropriate process. Experience from other international security agencies such as INTERPOL show that countries can refuse to sign conventions, not because they disagree on the content but on the process. One approach could be to try to establish a new treaty and try to get as many countries to sign it, though this may be very long to achieve. An alternative that may achieve greater acceptance and authority is to expand an existing treaty, such as the International Telecommunications Union (ITU) within the United Nations, or to establish a new framework within a smaller group of like-minded countries such as the OECD. One could also consider expanding the scope of existing governance bodies, for instance by calling a new meeting of the UN Security Council (e.g. UN Cyber Security Council, at least 1 session per year).

7 Conclusion

The topics covered during this year's seminar show that cyber security, especially as it relates to terrorism, continues to pose great challenges. However, there has also been progress, increasing areas of consensus, and a real will to work and achieve solutions together, across the U.S. and France, and across sectors (law enforcement, government, military, business). In todays' digital world, technology and threats are evolving at a very fast pace, forcing laws and doctrines to catch up. It is important to connect the dots and find ways to promote cooperation and information sharing between sectors and between like-minded countries, such as the U.S. and France. The stakes need to be raised, notably in public-private partnerships, in order to effectively prepare against cyber threats. Otherwise, we will be compelled to react as individuals, groups, nations, or leave the floor to other powers. Cyber security will need both cyber defensive and cyber offensive actions to be achieved. Every battle needs human intelligence, and the fight against terrorism and cyber threats is no exception. It will be necessary to redefine the role of human intelligence in a digital world. We believe that no technology can replace human connections and insights. Only mutual trust allows meaningful cooperation to blossom, thereby enabling countries and individuals to succeed together.

8 Appendix

8.1 Potential themes for 2017 Seminar

The following list is not exhaustive:

- Public-private partnerships in cyber security
- Human intelligence and AI in cyber security
- Sharing information in a world of cyber threats
- How to establish cyber security best practices in terms of technology and processes
- The influence of non-destructive cyberattacks on internal politics, democratic processes, and democratic societies

8.2 2016 Sponsors

We thank our sponsors for their generous support:

Conference Rapporteurs:
Thomas W. Dillig, PhD
Aurélie M.H. Beaumel, YL16

Contact Information

French-American Foundation – United States
28 West 44th Street, Suite 1420
New York, NY 10036
email: info@frenchamerican.org
phone: +1-212-829-8800

French-American Foundation – France
34 avenue de New York
75116 PARIS
email: contact@french-american.org
phone: +33 1 45 77 40 01