Facing the Emerging Security Challenges

From Crimea to Cyber Security

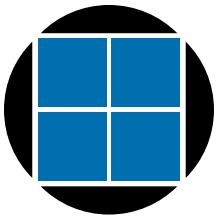
PROCEEDINGS OF THE 32*nd* INTERNATIONAL WORKSHOP ON GLOBAL SECURITY

Mr. Jean-Yves Le Drian
Minister of Defense of France & Workshop Patron

Général de corps d'armée Bernard de Courrèges d'Ustou
Directeur, Institut des hautes études de défense nationale

Dr. Roger Weissinger-Baylon
Workshop Chairman

Anne D. Baylon
Editor



32*nd* International Workshop on Global Security

Proceedings of the 32nd International Workshop on Global Security

Anne D. Baylon, *Editor*

PATRON
Mr. Jean-Yves Le Drian
Minister of Defense of France

THEME
Facing the Emerging Security Challenges
From Crimea to Cyber Security

WORKSHOP CHAIRMAN & FOUNDER
Dr. Roger Weissinger-Baylon
Co-Director, Center for Strategic Decision Research

PRESENTED BY
Center for Strategic Decision Research (CSDR)

AND
Institut des hautes études de défense nationale (IHEDN) within the French Prime Minister's organization, including the Castex Chair of Cyber Security

PRINCIPAL SPONSORS
French Ministry of Defense

United States Department of Defense
Office of the Director of Net Assessment

North Atlantic Treaty Organization
Public Diplomacy

MAJOR SPONSORS
Lockheed-Martin · McAfee, Intel Security
MITRE · Tiversa · Area SpA · FireEye

ASSOCIATE SPONSORS
Kaspersky Lab · AECOM · Quantum Research International

The *32nd International Workshop on Global Security* is presented by the Center for Strategic Decision Research (CSDR) and Institut des hautes études de défense nationale (IHEDN), with the Patronage of Defense Minister Jean-Yves Le Drian and the sponsorship of the following organizations:

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE LA DÉFENSE

UNITED STATES DEPARTMENT OF DEFENSE
Net Assessment

NATO OTAN
PUBLIC DIPLOMACY

Center for Strategic Decision Research

IHEDN

MAJOR SPONSORS

LOCKHEED MARTIN

intel Security

MITRE

TIVERSA

AREA

FireEye

ASSOCIATE SPONSORS

KASPERSKY lab

AECOM

QUANTUM RESEARCH INTERNATIONAL

ACKNOWLEDGEMENTS OF PAST HOST AND SPONSORING GOVERNMENTS

Czech Republic
Kingdom of Denmark
Federal Republic of Germany
Republic of Greece
Republic of Hungary
Kingdom of the Netherlands
Kingdom of Norway
Republic of Poland
Republic of Portugal
Ministry of Defense of Austria
Ministry of Defense of France
Ministry of Defense of Italy
Ministry of Defense of Turkey
Canadian Armed Forces
Russian Ministry of Industry, Science, and Technology

Table of Contents

Welcoming Remarks and Keynote Presentation

Lieutenant General Bernard de Courrèges d'Ustou
Director, Institute for Higher Defense Studies (IHEDN) 8

Overview
Dr. Roger Weissinger-Baylon, Workshop Chairman and Co-Founder 9

Acknowledgments 13
Ms. Anne D. Baylon, Editor

Lieutenant General Heinrich Brauss
NATO Assistant Secretary General for Defense Policy and Planning 17

Part One: International Perspectives on Cyber Security, including Views from France, the U.S., NATO and the European Union

FRENCH VERSION
Vice-amiral Arnaud Coustillière
Officier général Cyberdéfense, Ministère de la Défense 19

ENGLISH VERSION
Vice Admiral Arnaud Coustillière
General Officer for Cyber Defense, French Ministry of Defense 23

FRENCH VERSION
Mr. Guillaume Poupard
Directeur Général, Agence nationale de la sécurité des systèmes d'information (ANSSI) 27

ENGLISH VERSION
Mr. Guillaume Poupard
Managing Director, National Agency for Information Systems Security (ANSSI) 31

Ambassador David Martinon
Ambassador for Cyber Diplomacy & Digital Economy, Ministry of Foreign Affairs 35

Mr. Chris Painter
Coordinator for Cyber Issues, U.S. Department of State 37

Ambassador Sorin Ducaru
NATO Assistant Secretary General for Emerging Security Challenges 39

Ms. Heli Tiirmaa-Klaar
Head of Cyber Policy Coordination, Conflict Prevention & Security Policy, EEAS 41

Dr. Steve Purser
Head of Core Operation Department, ENISA (European Union Agency for Network and Information Security) 43

FRENCH VERSION
Sénateur Jean-Marie Bockel
Sénat français, Membre de la commission des affaires étrangères, de la défense et des forces armées 47

ENGLISH VERSION
Senator Jean-Marie Bockel
French Senate, Member of the Foreign Affairs, Defense and Armed Forces Committee 51

Mr. Luigi Piantadosi
Director, International Business Development, Lockheed Martin 53

Mr. Anton Shingarev
Chief of Staff, Kaspersky Lab 57

Part Two: Crimea/Ukraine and the Relationationship with Russia, IRAQ/Daesh, Afghanistan, and Nuclear Developments

Ambassador Ihor Dolhov
Deputy Minister of Defense of Ukraine 59

Ambassador Oleh Shamshur
Ambassador of Ukraine to France 63

Mr. Ioan Mircea Pascu
Vice President of the European Parliament; Former Minister of Defense of Romania 65

Ms. Radoslava Stefanova
Head of Russian-Ukrainian Relations, NATO Political Affairs and Security Policy 67

Ambassador Jaromir Novotny
Advisor to the Prime Minister of the Czech Republic (Foreign Policy and Defense) 69

Ambassador Fareed Yasseen
Ambassador of Iraq to France 71

Mr. Andrea Formenti
Founder and CEO, Area SpA 75

Ambassador Omar Samad
Ambassador of Afghanistan to Belgium 77

Dr. Andrew May
Associate Director, Office of Net Assessment, Office of the U.S. Secretary of Defense 79

Part Three: Countering Cyber-enabled Extremism Online, Protecting Critical Infrastructure From Cyber Attack, Risks of Cyberwar, Privacy, and Cyber Crime and the Dark Web

Ingénieur Général Daniel Argenson
Deputy Director, Institute for Higher Defense Studies (IHEDN) 81

Dr. Frédérick Douzet
Castex Chair of Cyber Strategy, Institute for Higher Defense Studies (IHEDN) 83

FRENCH VERSION
Monsieur Christian Gravel
Préfet, Directeur du Service d'information du Gouvernement (Premier ministre) 85

ENGLISH VERSION
Monsieur Christian Gravel
Prefect, Director of the Government Information Service (Office of the french Prime Minister) 89

FRENCH VERSION
Mr. Jean-Yves Latournerie
Préfet, Conseiller du Gouvernement, Chargé de la lutte contre les cybermenaces, Ministère de l'Intérieur 93

ENGLISH VERSION
Mr. Jean-Yves Latournerie
Prefect, Government Special Advisor for the Fight against Cyberthreats, French Ministry of the Interior 97

Ms. Caroline Baylon
Research Associate in Science, Technology, and Cyber Security, Chatham House 99

Mr. Raj Samani
Chief Technology Officer, Europe, McAfee/Intel 101

FRENCH VERSION
Général (Gendarmerie) Marc Watin-Augouard
Fondateur du Forum international de la Cybersécurité (FIC), 103

ENGLISH VERSION
General (Gendarmerie) Marc Watin-Augouard
Founder of the International Forum on Cybersecurity (FIC) 107

Mr. Jakub Boratynski
Head of Trust and Security Unit, DG Connect, European Commission 109

Dr. Kate Langley
Head of Cyber and Space Policy, UK Ministry of Defense 111

Mr. Koen Gijsbers
General Manager, NATO Communications and Information Agency 113

Ambassador Lauri Lepik
Estonian Ambassador to NATO 115

Major General David Senty, USAF (Ret)
Director, Cyber Operations, The MITRE Corporation, Former Chief of Staff, U.S. Cyber Command 117

FRENCH VERSION
Mr. Eduardo Rihan Cypel
Député (Seine-et-Marne), Assemblée Nationale 119

ENGLISH VERSION
Mr. Eduardo Rihan Cypel
Deputy (Seine-et-Marne) French National Assembly 121

Mr. Karsten Geier
Head, Cyber Policy Coordination, German Foreign Ministry 123

Mr. Nick Dean
Head of Cyber Policy, United Kingdom Foreign and Commonwealth Office 125

Mr. Atsushi Saito
Director, Space Policy Division, and Senior Negotiator for International Security Affairs, National Security Policy Division, Japanese Foreign Policy Bureau 127

Ingénieur général des mines Henri Serres
High Council for Economy, Industry, Energy and Technology, French Ministry of the Economy and Finance 129

Mr. Jim Cowie
Chief Scientist, Dyn 131

Major General (ret.) Robert Ranquet
Former Deputy Director, Institute for Higher Defense Studies, (IHEDN) 135

Welcoming Remarks to the 32nd International Workshop on Global Security

Lieutenant General Bernard de Courrèges d'Ustou
Director, Institut des hautes études de défense nationale (IHEDN)

Good morning and welcome to the Invalides, a place of history and heritage!

As director of the Institut des hautes études de défense nationale (IHEDN), or the Institute for Higher National Defence Studies, I am very pleased to welcome today, for the sixth time in Paris, the International Workshop on Global Security, under the patronage of the Minister of Defence, Mr. Jean-Yves Le Drian. The IHEDN is co-organising this Paris edition of the seminar with Dr. Roger Weissinger-Baylon, the Chairman and Founder of the Center for Strategic Decision Research.

IHEDN is an inter-ministerial institute which brings together 2,300 civilian and military leaders in order to deepen their knowledge of strategic issues at international, national and regional levels; it is also a tool to address European and international responsibility. This year, we are honored to welcome your very distinguished group including ministers, senators, ambassadors, presidents and directors, chief executive officers, and high-ranking generals.

During the two days of this thirty-second edition of the International Workshop on Global Security, you will be brainstorming on "Facing the Emerging Security Challenges: From Crimea to Cyber Security" with the best experts in their fields. I will leave the floor to the first of these experts and wish you all a fruitful and constructive seminar, and a very pleasant stay in Paris!

Overview

Dr. Roger Weissinger-Baylon
Workshop Chairman and Co-Founder

In the historic King's Council Chamber of the Hôtel National des Invalides, this year's *32nd International Workshop on Global Security* was presented in Paris on 5-6 November 2015. The Invalides, one of France's great national treasures, was built in 1676 by King Louis XIV as a hospital for his soldiers and in order to provide a Royal Chapel for his family (the chapel is now a fitting tomb for Napoleon, instead of the King's descendants.)

Patronage of French Defense Minister & Principal Sponsors. France's Minister of Defense, Jean-Yves Le Drian, was the Patron of the workshop, which was presented by the Center for Strategic Decision Research in partnership with the Institute for Higher Defense Studies (IHEDN) within the organization of the French Prime Minister. The principal workshop sponsors were NATO (Public Diplomacy Division), the French Ministry of Defense, and the U.S. Department of Defense (Office of Net Assessment). The contributions of our industry sponsors—Lockheed Martin, McAfee|Intel Security, MITRE, Tiversa, Area SpA, FireEye, Kaspersky Lab, and AECOM—were equally helpful, especially in the discussions of cyber security, since governments do not always have the knowledge or resources to address these issues by themselves.

French Defense Minister Jean-Yves Le Drian was the Workshop Patron again this year.

Facing the Emerging Security Challenges. The workshop theme of "Facing the Emerging Security Challenges: From Crimea to Cyber Security" highlights the dangers of a wide range of threats extending from continued Russian aggression in Crimea and Eastern Ukraine; the ISIS/Daesh terrorist threat spreading from Iraq and Syria (where Russia also plays a key role); the unresolved conflict in Afghanistan; and, of equal importance, the growing cyber threat which has already played a role in Russia's repeated use of hybrid warfare. Of course, the cyber threat also extends beyond its role in political-military crises to present an increasingly serious risk affecting our daily lives in very concrete ways. To address these challenges, more than twenty international organizations and countries—NATO, the European Union, France, the United Kingdom, Germany, the Netherlands, Belgium, Ireland, Italy, Estonia, the Czech Republic, Romania, Bulgaria, Turkey, Iraq, Afghanistan, Japan, Ukraine, Russia, and the United States—were represented by senior government, diplomatic, military, academic, and industry representatives who participated actively in the workshop discussions under Chatham House rules.

Politicians may prefer to blame "...the vague threat from "Islam," when the true danger might be more appropriately described as 'Radical Islam,' 'Wahhabism,' or 'Salafism.'"

It is important that the presentations and discussions were "not for attribution," since politicians and government speakers are understandably reluctant to speak openly about certain of the key factors that underlie today's crises. In public discourse, they may find it prudent to employ veiled references to "state actors" instead of directly mentioning, as the case may be, Qatar, Saudi Arabia[1], Pakistan, Russia, or China. In addressing the terror threat, politicians often prefer to mention the vague threat from "Islam," when the true danger might be more appropriately described as "Radical Islam," "Wahhabism," "Salafism," or "Islamism," i.e. political Islam.

1 As a rare exception to the broad efforts to hide Saudi involvement in terrorist attacks, a bill to hold Saudia Arabia potentially liable for attacks on U.S. soil, such as the 9/11 attack on the Twin Towers, has passed the United States Senate with bi-partisan support. Commenting on the significance of the Senate bill and the dangers of Saudi government support of Wahhabism, U.S. presidential candidate Bernie Sanders said, "It is a very destructive religion. I think it's important we do understand the role that the Saudis may have played. As you may know, the Saudi government has been a major proponent of Wahhabism, which is an extremely fundamentalist version of Islam and it is being taught all over the world." http://www.politico.com/blogs/2016-dem-primary-live-updates-and-results/2016/04/bernie-sanders-criticizes-ny-polls-222074#ixzz46C77f2r8

In reviewing the chapters below, it may be helpful to consider that many of the issues are linked in very complex ways to extremely sensitive matters such as the role of oligarchy, corruption, politicization of religion (especially Islamism), organized crime, illegal trafficking including people and drugs, mass incarceration, inequality of income and opportunity, and especially injustice.

Perhaps because of the very complexity required to understand and deal with them, many of these issues have now become full-blown crises that are stretching governments' institutions and resources to their very limits. Core principles of the European Union such as open borders among member states are at stake. It is at least conceivable that Britain could exit the Union. And in the U.S. presidential campaign, dangerous rhetoric that sparks hatred of Muslims, who are held to be collectively responsible for Islamic terrorism or ISIS/Daesh, has been compared to Mussolini's.

In the chapters that follow, you will find the views of forty-five of the workshop speakers on these challenges, which raise a number of puzzling and rather worrisome questions, including the following ones:

- *What Ever Happened to the Cooperative Relationship with Russia?* Despite a successful period of Russia-NATO cooperation (especially during the 1990's with General George Joulwan as SACEUR and with William Perry as the U.S. Secretary of Defense), the relationship with Russia steadily deteriorated—almost coming to a full stop in 2014 when Russia seized Crimea and intervened militarily in Eastern Ukraine under the cover of hybrid warfare (staying just below the armed conflict threshold). What ended the once cooperative NATO-Russia relationship? According to the *Guardian*, former Secretary Perry has described the U.S. attitude toward Russia during the 1990s and early 2000s, "Who cares what they think? They're a third-rate power." Perry believes that Russia would have been more comfortable with NATO's eastward expansion if it had proceeded more slowly. Russia also objected to the expansion of missile defense systems. For both Ukraine and Russia, the introduction of free market economics—which tends to be blamed on the West—has meant a life with widespread poverty, extreme inequality, and a corrupt system in which oligarchs play dominant roles, with President Putin being the ultimate oligarch. The cyber hack now called the "Panama Papers" has called attention to the role of offshore corporations in supporting political corruption, money laundering, and hiding wealth, including two billion dollars that supposedly belong to President Putin. President Barack Obama told the Guardian that "A lot of it is legal, but that is exactly the problem." Given the heavy costs now being borne by all sides (including sanctions on Russia that also hurt Europe), is there a path toward a better future?

Former Secretary of Defense William Perry has described the U.S. attitude to Russia at the time as "Who cares what they think? They're a third-rate power."

President Barack Obama said, "A lot of it is legal, but that is exactly the problem."

- *Can ISIS/Daesh Be Defeated without Ending Saudi and Qatari Funding for Wahhabism and Salafism?* Muslim youth—in France, Belgium, across Europe, and beyond—often suffer from extreme inequalities of income and opportunity, frequent harassment by police, social isolation from other communities, and with few opportunities for a better life. At the same time, they are exposed to the highly conservative religious messages of political Islam (Islamist) from Wahhabi and Salafist groups that are massively funded by Qatar and Saudi Arabia—where they are very often taught to hate other religions. Building on the festering sore of this injustice to Muslim communities and their youth, ISIS/Daesh has developed sophisticated techniques for recruiting soldiers, terrorists, and even wives for ISIS/Daesh fighters. The austerity budgets of European countries deprive Muslim communities of the benefits of adequate infrastructure and social programs that might make their disadvantaged situations more tolerable. Possibly making matters worse, Russian military intervention in Syria has accelerated refugee flows into Europe to such an extent that it may amount to the deliberate "weaponizing of migrants.

"Wahhabi and Salafist groups are massively funded by Qatar and Saudi Arabia...and taught to hate other religions."

- *How Can We Counter Nuclear Proliferation?* New technologies for nuclear weapons, permitting smaller yields and more precise targeting, might increase the likelihood of their development and use. A nuclear escalation of a future Pakistani-Indian conflict is only one of the possible scenarios. Since we are headed for a dangerous future with too many nuclear weapons (and nuclear powers), it may be that both the U.S. and Russia would benefit from thinking about how to delay or at least shape this future.

- *The Face of Future Conflict—Will the Internet and Cyber be at the Center?* As the Islamists' horrible terrorist attacks in Paris and Brussels have shown, ISIS/Daesh depends on a very sophisticated use of the internet to spread its message. In France, the government is taking ISIS/Daesh's utilization of the internet so seriously that the Prime Minister has announced the creation of "battalions of community managers" who will be active within the internet communities of Muslim youth in order to counter ISIS/Daesh's messages and its recruiting. Just as cyber attacks over the internet were important elements of Russia's hybrid warfare in Estonia, Georgia, and Ukraine, militaries are seeking ways to incorporate cyber into their operations. Indeed, the more capable actors are clearly "preparing the battlefield" by hiding logic bombs within the critical infrastructure of their potential adversaries, so that they can be launched once a conflict begins. It may be that such an attack against critical infrastructure could trigger the next major military conflict, unless ways to control escalation are prepared sufficiently in advance.

"Few governments are making whole-hearted efforts to educate their citizens as to the dangers of cyber threats or how to protect themselves."

While it is indeed difficult to foresee exactly how the future will unfold, it does appear that cyber threats are among the gravest security challenges that lie ahead. Yet, with only a few exceptions—such as the efforts by the French National Cyber Security Agency (ANSSI) or the "Stop Djihadisme" project of the French government information service (SIC), few governments are making whole-hearted efforts to educate their citizens as to the dangers of cyber threats or how to protect themselves. This means that populations are potentially quite vulnerable not only to criminal hackers but even to the side effects of cyber attacks by terrorists or nation states which may attack the infrastructures on which everyone depends. Moreover, there also seems to be reluctance to impose cyber security standards even on critical infrastructure including the electrical grid, especially for smaller entities whose financial resources are limited. Instead, the responsibility to inform and defend the public against cyber attacks is often being left to the media and to private companies such as McAfee|Intel, Cisco, Lockheed Martin, FireEye, or Kaspersky Lab (just to name a few major players who have agreed to be sponsors of our research center and workshops).

To make matters worse, the internet of things (IoT) will soon be adding billions of devices to the internet, ranging from picture frames to refrigerators or home security networks: few of the devices will have more than rudimentary security protections, and nearly all will be vulnerable to cyber attacks in some way. In this context, individuals and small organizations will most likely be left to fend for themselves, largely relying on the fact that, until now, potential victims have vastly outnumbered the cyber criminals seeking to prey on them—a situation resembling that of African antelopes in a large herd, stalked by a pride of lions that can only take one of them at a time. As the skills and financial resources of hackers and cyber criminals grow, even the largest companies are being forced to abandon the goal of fully protecting their systems. Increasingly, the emphasis is on maintaining *resilience*—encryption of data or relying on the cloud can help—to ensure that the organization will be able to protect its core functions in the face of a full-fledged cyber attack.

To address this situation, international cooperation is vital in order to share information on threats and responses, since the internet is global. Yet, the obstacles to cooperation are considerable. As to the U.S., it prefers to share only with its so-called "five eyes" partners, the U.K., Canada, Australia, New Zealand, and, for some reason, Israel. Within Europe, larger countries, such as the UK, France, and Germany are reluctant to share with their smaller neighbors, too, and this will make them more vulnerable as a result. As France's Admiral Arnaud Coustillière, the flag officer responsible for cyber, points out in his chapter, the desire of countries to spy on

"The U.S. prefers to share only with its so-called 'five eyes' partners, the U.K., Canada, Australia, New Zealand, and Israel. "

each other is one of the chief obstacles to cooperation since sharing vulnerabilities would make cyber espionage far too difficult. In close cooperation with the British Defense Ministry, his organization is creating a "cluster of cyber commanders," comprising general officers of two-star rank who have agreed to meet twice per year with the intention of building trust among the militaries of their participating countries. Another approach supported by the U.S. State Department's Chris Painter and others is to establish norms for cyber security applicable to conflict between states, such as not attacking national CERTs (Computer Emergency Response Teams) or the critical infrastructure of other countries. Of course, none of these cooperative efforts are easy to accomplish because of conflicts of interest, including the differences of views between the U.S. government and industry on the need for strong encryption.

Closing Remarks: The *Panama Papers—A Game Changer?* As we were completing the final editing of this book prior to publication, the ICIJ (International Consortium of Investigative Journalists) released the so-called "Panama Papers"—11.5 million documents on more than 214,000 offshore companies that were leaked or perhaps even hacked from the private servers of the Mossack Fonseca law firm in Panama. This cyber theft (or hack) may have been the largest in history, with potentially more impact than the Snowden revelations. Senior government leaders of Iceland, the U.K., Azerbaijan, Russia, China, the U.S., and certainly other countries are embarrassed; and there is the possibility that the leak will influence national elections in some nations. The Panama Papers simultaneously spotlight both financial corruption by the economic elite and the difficulty of keeping sensitive information secret.

The "Panama Papers" comprise 11.5 million documents on more than 214,000 offshore companies that were leaked or perhaps even hacked from the Mossack Fonseca law firm in Panama.

This vast trove of highly sensitive documents—which arrives in the midst of the 2016 U.S. presidential campaign—reveals tax avoidance schemes, money laundering, hidden assets of doubtful origin, and other excesses of the wealthy. The effects of the Panama Papers leak are amplified by other widely publicized research, including Professor Thomas Piketty's *Capitalism in the 21st Century,* that calls attention to the extremes of the present inequality. This means that the public is increasingly aware that the majority of the economic growth in the U.S., and certainly in other countries as well, goes not to themselves but to a small percentage of the population. In the U.S., one single family has more wealth than the poorest 42% of the population. Similarly, the life expectancy of the wealthiest 1% is now 15 years longer than that of the poorest 1%. As these facts, and other practices seen as unfair, become known, there is almost unprecedented resentment against the political establishments of both the Democratic and Republican Parties, which is fueling the political campaigns of Senator Bernie Sanders and the billionaire Donald Trump. According to former U.S. President Jimmy Carter, the U.S. has actually become an "oligarchy with unlimited political corruption." Under the circumstances, there will need to be profound changes in the policies of government or the forces driving the expansion of ISIS/Daesh—or similar organizations on the extreme right—can be expected to grow. While the consequences of the growing resentment against the elites are nearly impossible to predict, they will almost certainly be unpleasant.

According to former U.S. President Jimmy Carter, the U.S. has become an "oligarchy with unlimited political corruption."

Menlo Park, California and Paris, France
April, 2016

Acknowledgments

Anne D. Baylon, LL.B., M.A.
Editor

In preparing for the publication of these *Proceedings* of the 32nd International Workshop on Global Security, it is a special pleasure to acknowledge the wonderful support of the many individuals and organizations who contributed as vital sponsors, speakers or session chairmen, members of the workshop staff or publishing team, and the many others who contributed in a variety of important ways ranging from planning to logistics. While it would be impossible to recognize everyone, I would like nonetheless to call special attention to the support of the following individuals and organizations:

Patronage of Minister Jean-Yves Le Drian and Institute of Higher Defense Studies Partnership

We are grateful for the Patronage, for the third time, of French Defense Minister Jean-Yves Le Drian, as well as the Patronage of previous French Ministers of Defense, Mme. Michèle Alliot-Marie, Mr. Hervé Morin, and Mr. Gérard Longuet (and for a transitional period, Mr. Alain Juppé. This continued support of successive defense ministers is a real honor which we appreciate immensely. We are also grateful for the close cooperation of our partners at the Institut des hautes études de défense nationale (or Institute of Higher Defense Studies) within the Prime Minister's organization. We particularly appreciate the role and participation of its Director, Lieutenant General Bernard de Courrèges d'Ustou, its Deputy Director, General Daniel Argenson, and Dr. Frédérick Douzet, Castex Chair of Cyber Strategy, as well as its former Deputy Director, General Robert Ranquet.

Workshop Speakers and Session Chairs

Since their contributions are central to both the workshop discussions and this book, I would like to begin by acknowledging the workshop speakers and sessions chairs:

Opening Presentations. Lieutenant General Bernard de Courrèges d'Ustou, Director, Institute for Higher Defense Studies (IHEDN); Lieutenant General Heinrich Brauss, NATO Assistant Secretary General for Defense Policy and Planning; Vice Admiral Arnaud Coustillière, General Officer for Cyber Defense, French Ministry of Defense; Mr. Guillaume Poupard, Managing Director, National Agency for information systems security (ANSSI); Ambassador David Martinon, Ambassador for Cyber Diplomacy & Digital Economy, Ministry of Foreign Affairs; Mr. Chris Painter, Coordinator for Cyber Issues, U.S. Department of State; Ambassador Sorin Ducaru, NATO Assistant Secretary General for Emerging Security Challenges; Ms. Heli Tiirmaa-Klaar, Head of Cyber Policy Coordination, Conflict Prevention & Security Policy, EEAS; Dr. Steve Purser,Head of Core Operation Department, ENISA (European Union Agency for Network and Information Security); Senator Jean-Marie Bockel, French Senate, Member of the Foreign Affairs, Defense and Armed Forces Committee; Mr. Luigi Piantadosi, Director International Business Development, Lockheed Martin; Mr. Anton Shingarev, Chief of Staff, Kaspersky Lab.

Part Two: Crimea/Ukraine and the Relationship with Russia, IRAQ/Daesh, Afghanistan, and Nuclear Developments. Ambassador Ihor Dolhov, Deputy Minister of Defense of Ukraine; Ambassador Oleh Shamshur, Ambassador of Ukraine to France;Mr. Ioan Mircea Pascu, Vice President of the European Parliament; Former Minister of Defense of Romania; Ms. Radoslava Stefanova, Head of Russian-Ukrainian Relations, NATO Political Affairs and Security Policy; Ambassador Jaromir Novotny, Advisor to the Prime Minister of the Czech Republic (Foreign Policy and Defense); Ambassador Fareed Yasseen, Ambassador of Iraq to France; Mr. Andrea Formenti, Founder and CEO, Area SpA; Ambassador Omar Samad, Ambassador of Afghanistan to Belgium; Dr. Andrew May, Associate Director, Office of Net Assessment, Office of the U.S. Secretary of Defense.

Part Three: Countering Cyber-enabled Extremism Online, Protecting Critical Infrastructure From Cyber Attack, Risks of Cyberwar, Privacy, and Cyber Crime and the Dark Web. Ingénieur Général Daniel Argenson, Deputy Director, Institute for Higher Defense Studies (IHEDN); Dr. Frederick Douzet, Castex Chair of Cyber Strategy, Institute for Higher Defense Studies (IHEDN); Mr. Christian Gravel, Prefect, Director of the French Government Information Service (Office of the Prime Minister); Mr. Jean-Yves Latournerie; Prefect, Government Special Advisor for the Fight against Cyberthreats, French Ministry of the Interior; Ms. Caroline Baylon, Research Associate in Science, Technology, and Cyber Security, Chatham House; Mr. Raj Samani, Chief Technology Officer, Europe, McAfee/Intel; General (Gendarmerie) Marc Watin-Augouard, Founder of the International Forum on Cybersecurity (FIC); Mr. Jakub Boratynski, Head of Trust and Security Unit, DG Connect, European Commission; Dr. Kate Langley, Head of Cyber and Space Policy, UK Ministry of Defense; Mr. Koen Gijsbers, General Manager, NATO Communications and Information Agency; Ambassador Lauri Lepik, Estonian Ambassador to NATO; Major General David Senty, USAF (Ret), Director, Cyber Operations, The MITRE Corporation, Former Chief of Staff, U.S. Cyber Command; Mr. Eduardo Rihan Cypel, Deputy (Seine-et-Marne) French National Assembly; Mr. Karsten Geier, Head, Cyber Policy Coordination, German Foreign Ministry; Mr. Nick Dean, Head of Cyber Policy, United Kingdom Foreign and Commonwealth Office; Mr. Atsushi Saito, Director, Space Policy Division, and Senior Negotiator for International Security Affairs, National Security Policy Division, Japanese Foreign Policy Bureau; Ingénieur général des mines Henri Serres, High Council for Economy, Industry, Energy and Technology, French Ministry of the Economy and Finance; Mr. Jim Cowie Chief Scientist, Dyn and Renesys; Major General (ret.) Robert Ranquet, Former Deputy Director, Institute for Higher Defense Studies, (IHEDN).

Principal Sponsors

The workshop would have been impossible without the support of the French government and the Ministry of Defense, NATO, the U.S. Department of Defense and the following industry sponsors: Lockheed Martin, McAfee|Intel, the MITRE Corporation, Tiversa, Area SpA, FireEye, Kaspersky Lab, and AECOM.

French Government and Ministry of Defense. As Director of the Institute for Higher Defense Studies (IHEDN) within the French Prime Minister's Organization, Lieutenant General Bernard de Courrèges d'Ustou gave opening remarks. IHEDN was our principal partner in the preparation of the workshop. Other senior IHEDN representatives included the former director, Lieutenant General Jean-Marc Duquesne; IHEDN's Deputy Director, Ingénieur Général Daniel Argenson; former Deputy Director Major General Robert Ranquet; Dr. Frédérick Douzet, the Castex Chair of Cyber Strategy; and Mr. Thorniké Gordadze, advisor for educational programs, who is a former Deputy Foreign Minister of Georgia. We are grateful to the French Defense Ministry for allowing us to present the workshop sessions in the historic "Grand Salon" of the Invalides—the "Council Chamber" of King Louis XIV who commissioned the Invalides. Moreover, we owe special thanks to the Military Governor of the Invalides, Lieutenant General Hervé Charpentier, who kindly made his "salons du gouverneur militaire" available as well. Logistics were coordinated by Major Daniel Raty. We are also fortunate that many of the most senior french officials with responsibilities and interest in cyber security were able to address the workshop: Vice Admiral Arnaud Coustillière; Ms. Isabelle Valentini; Mr. Guillaume Poupard; Ambassador David Martinon; Mr. Christian Gravel, Prefect; Mr. Jean-Yves Latournerie, Prefect; General Marc Watin-Augouard, Mr. Eduardo Rihan Cypel, Deputy; Senator Jean-Marie Bockel; Mr. Henri Serres; and Ms. Pascale Trimbach.

NATO. We appreciate the opening keynote address by Lieutenant General Heinrich Brauss, Assistant Secretary General for Defense Policy and Planning, as well as the continued support of Deputy Secretary General Alexander Vershbow. Assistant Secretary General Sorin Ducaru and Mr. Koen Gijsbers, General Manager, NATO Communications and Information Agency, led NATO's important contributions to the discussion of cyber security, together with Ambassador Lauri Lepik, Estonia's Permanent Representative on the North Atlantic Council. At the NATO Public Affairs Division, we would like to thank both Ms. Angélique Burnet-Thomsen and Ms. Marie-Line Boricaud for their valued support through a NATO grant that was awarded to the workshop this year for the second time and for coordinating the participation of Ms. Radoslava Stefanova, Head of Russian-Ukrainian Relations, NATO Political Affairs and Security Policy.

United States Department of Defense. We appreciate the continued support for over three decades of the Office of Net Assessment and the contributions this year of its Deputy Director Dr. Andrew May. The workshop would not have been possible in its present form without the support for so many years of its Director, Mr. Andrew Marshall and Ms. Rebecca Bash, both of whom retired last year. Dr. Lin Wells III was a valued advisor and reviewed a portion of this book.

Major Sponsors

Lockheed Martin. We would like to warmly thank Mr. Steve Williams, Regional Executive for Europe/Americas at Lockheed Martin International, Mr. Luigi Piantadosi, Director International Business Development, as well as Mr. Haden Land, who strongly supported the workshop until his retirement last year.

McAfee|Intel. Addressing the workshop on behalf of McAfee|Intel were Mr. Maurice Cashman and Mr. Raj Samani. We are also grateful for the support of Ms. Patricia Murphy, Vice President Sales for Southern Europe, and Mr. Thomas Gann who was the chief organizer of McAfee's workshop participation again this year.

MITRE. Beginning with our first workshop thirty-two years ago, MITRE Corporation has made important contributions. We are grateful for the contributions this year by Mr. Gary Gagnon, Senior Vice President; Major General David Senty; and Mr. Kevin Scheid, Special Advisor to the President and CEO.

Tiversa. For the third time, Tiversa sponsored the workshop with the participation of Mr. Robert Boback, CEO; Mr. Tim Hall; Mr. Gary Woods, and Dr. Jack Wheeler.

Area S.p.A. Thanks to Mr. Andrea Formenti, CEO, and Mr. Marco Braccioli, Senior Vice President, Area S.p.A. was an important sponsor for the fourth time.

FireEye. Mr. Adam Palmer, Director, International Government Affairs, was a much appreciated participant, thanks to Ms. Alexa King, FireEye General Counsel. We would also like to thank FireEye Board Member, Mr. Robert Lentz, former U.S. Deputy Assistant Secretary of Defense (Cyber Security), for his enthusiastic support of the workshop.

Associate Sponsors

Kaspersky Lab. We would like to thank Mr. Anton Shingarev, Head of the CEO Office and Director of Global Government Relations, Kaspersky Lab and Mr. Evgeny Grigorenko, Senior Public Affairs Manager, CEO Office, for joining the workshop.

AECOM. Mr. David Swindle, Group Executive Vice President, was an important sponsor again this year, and Sir Kevin Tebbit, KCM, CMG, former Permanent Secretary of Defense of the United Kingdom, met with us to help plan the workshop agenda.

Special Thanks

General Patrick de Rousiers, Chairman of the European Union Military Committee and Military Advisor to the High Representative of the European Union for Foreign Affairs, as well as Vice Admiral Marc Ectors were extremely generous with their advice and played important roles in the development of the workshop agenda. General George Joulwan has given us invaluable advice and support since the beginning of his tenure as NATO's Supreme Allied Commander, Europe (SACEUR) and participated actively in our workshops for fifteen years.

Workshop Staff

Our principal staff members were Jean Lee, a graphic designer and professional photographer; Dr. Ania Garlitski, a board-certified cardiologist, who was until recently Assistant Professor of Medicine at Tufts University: and Ms. Caroline

Baylon, a graduate of Stanford and Oxford universities who is now the lead cyber security researcher at AXA, a large international insurance group based in Paris. All three have frequently supported the workshop since their graduation from Stanford University. Joining us for the first time this year were Mr. Antoun Meroueh and Mr. Clement Arminjon. Antoun prepared the English translations of several of the chapters published in this report.

Menlo Park, California and Paris, France
April, 2016

New Challenges and Threats to Europe's Security: *A Nato Perspective*

Lieutenant General Heinrich Brauss
NATO Assistant Secretary General for Defence Policy and Planning

It is a pleasure to be here in Paris today to address this year's International Workshop on Global Security. And it is a real honour to kick off this conference. "Facing the emerging security challenges—from Crimea to Cyber Security" means addressing current and future risks and threats in terms of both geopolitical and technological challenges. Indeed, the unifying element of 'Crimea' and 'Cyber Security' is the new, non-traditional and hybrid character of threats. Therefore, I am glad to have the opportunity to set out the overall political-strategic context for the ensuing discussions, and I am doing that from a NATO perspective.

The 2014 Change in Euro-Atlantic Security and the Ensuing Security Challenges

The year 2014 saw a sea change in Euro-Atlantic security. Since then, we have faced two strategic challenges at the same time, to the east and to the south. Both challenges are different, but both affect the security of our nations and the stability of Europe and therefore need to be tackled simultaneously.

> **"Russia's strategy of...hybrid warfare focuses on intimidation and coercion while staying below the threshold of an open military aggression."**

To the east, we are confronted with a newly assertive Russia. Through its aggressive rhetoric and actions, the Kremlin has demonstrated that it doesn't share our vision of a Europe whole and free, where all countries, big and small alike, share the same respect, integrity and security and work together as partners. The Russian leadership seems to think that it can only be secure if its neighbours are unstable or even divided and under Moscow's direct or indirect control. It appears that Russia has revitalised a strategy of competition about zones of influence. Geopolitics is back on the international agenda. Of particular concern is Russia's strategy of non-linear warfare, as demonstrated in Ukraine—a sophisticated model of state warfare using political, diplomatic, economic, overt and subversive means, with cyber attacks and large-scale no-notice military exercises on our borders, and all of this combined with a huge propaganda and disinformation campaign. Hybrid warfare focuses on intimidation and coercion while staying below the threshold of an open military aggression and thus creating ambiguity and uncertainty to undermine a timely and effective response. It is clear that this strategy is a particular challenge for an Alliance of 28 democracies.

To the south, from Afghanistan through the Middle East and across North Africa, we are confronted with a pattern of growing violence and instability; a complex combination of multidimensional challenges and threats, with many different causes, from widespread poverty and corruption, through insurgencies and religious extremism to collapsing states and interference of regional actors. All of this has led to untold human suffering, generated the unimaginably brutal terror organisation ISIL/DAESH and prompted the largest flow of refugees since the Second World War. Many countries from the region and all NATO nations are taking part in the US-led mission against ISIL. NATO Allies believe that Russia's military intervention in Syria has further complicated the situation. Russia should help destroy ISIL and end the war in Syria. Supporting the Assad regime, however, is prolonging the conflict and aggravating the suffering of the people. What is needed is a political solution. NATO Allies support and encourage the efforts undertaken by the UN, the EU and a number of nations from the region and beyond to negotiate a settlement to the war in Syria.

The challenges from the east and from the south demonstrate the continued importance of NATO's fundamental and enduring purpose: to safeguard the freedom and security of all its members by political and military means—Turkey just as

our eastern Allies. At the Summit in Wales last year our political leaders took far-reaching decisions, which, taken together, mean the greatest increase in our collective defence since the end of the Cold War. Its centrepiece is the Readiness Action Plan (RAP). This is about making sure that we have the right forces in the right place at the right time, mainly through three strands of adaptation: First, we have increased our (rotational) multinational military presence in the east—on the ground, in the air and at sea. Second, we are significantly enhancing the readiness of our forces, i.e. through doubling the size of the NATO Response Force, making it more capable; establishing the Very High Readiness Joint Task Force able to deploy within a few days; enhancing the number and quality of our exercises; and developing a range of highly capable forces for reinforcement. And third, we are significantly improving our political and military responsiveness through enhancing our situational awareness, creating a system of indications and warnings, developing a new form of detailed advance planning and drastically accelerating our political decision-making.

NATO's New Long-Term Strategic Adaptation

That said, the changed security environment has not only fundamentally affected Euro-Atlantic security, it has also created a new strategic reality of a long-term nature. Therefore, NATO has to adapt its posture also to the long-term. The NATO Summit in Warsaw next year will be an important milestone on our way towards our comprehensive long-term adaptation. There are mainly three key areas we are considering:

1) We will strengthen NATO's deterrence and defence posture to provide for modern, full-spectrum deterrence. Deterrence is about preventing war, preserving stability and safeguarding freedom of decision and action against all forms of aggression. The implementation of the Readiness Action Plan provides the foundation. It will be complemented by a strategy to counter hybrid warfare, improving NATO's and Allies' resilience and developing enhanced, active cyber defence. Of note is that we are working with the EU on a coordinated and coherent response to hybrid threats. We are also helping our 'partners in between—Ukraine, Moldova and Georgia—to improve their resilience against Russia's interference and intimidation. And we are analysing Russia's growing conventional and nuclear capabilities, including her Area Access Denial capabilities in the Arctic, in Kaliningrad, in Crimea and now the Eastern Mediterranean, and we will adapt our posture accordingly.

2) We are assessing the long-term implications of the current crisis on our relationship with Russia. The world of today has become integrated and interdependent. The question is not whether we have a relationship with Russia, but what kind of relationship we have. We believe it is in the security interest of both sides to engage in a dialogue to avoid misunderstandings and accidents where our forces might come into contact; ensure that tensions are not needlessly heightened; and seek to achieve transparency and predictability of military activities. Our Allies support a negotiated solution in Ukraine and feel encouraged that the ceasefire in eastern Ukraine is now holding, but the situation remains fragile. Russia has a special responsibility as it continues to support the separatists. And there is no doubt: engagement is not the same as accepting a new status quo or returning to business as usual. Strong deterrence and defence form the basis for a constructive relationship.

> **"The question is not whether we have a relationship with Russia, but what kind of relationship we have."**

3) NATO's long-term adaptation also needs to address the growing challenges and threats from the south. The Readiness Action Plan constitutes a 360-degree approach to enhancing readiness and responsiveness. NATO's rapid response forces are fully capable of deploying to the south just as to the east. But the complex challenges in the south require a comprehensive political, economic and humanitarian response from the entire international community. NATO has a role to play as a contributor to this wider effort. We continue to be ready to deploy forces when and where needed. But we believe it is better to help project stability rather than project large combat forces. NATO has therefore set up an ambitious programme to help partner countries build their own defence and related security capacity to be able to defend themselves and contribute to regional stability. And also in this regard, we would like to coordinate our efforts with other actors, particularly with the EU. The EU has a wide range of political, economic and civilian means; NATO's comparative strength lies in the military field. We are complementary by default. By building up the capacity of partners abroad, countries like Tunisia and Jordan and helping Iraq and, at some point, Libya to become more stable, we will strengthen our own security at home.

Le Combat Digital au Cœur des Opérations Militaires

Vice-amiral Arnaud Coustillière
Officier général Cyberdéfense, Ministère de la Défense

Je suis l'Amiral Coustillière, l'officier général de la cyberdéfense du Ministère de la Défense depuis un peu plus de 5 ans. Donc je travaille avec mon camarade Guillaume Poupard, directeur de l'ANSSI, depuis 2009 et nous avons été acteurs de la montée en puissance des capacités françaises dans ce domaine. J'ai deux responsabilités, une responsabilité ministérielle de coordination d'un certain nombre d'actions politiques, de relations internationales, et de formation ; je suis aussi totalement intégré dans la chaîne militaire de conduite des opérations et en charge de la planification et de la conduite des opérations de cyberdéfense, qu'elles soient défensives ou en accompagnement de nos opérations militaires. Aujourd'hui, ma chaîne a environ cinq ans de recul et de maturité et notre défi actuel est bien de placer le combat numérique au coeur des opérations et d'apprendre à le combiner avec les autres formes de combat.

Engagement International et National de la France contre le Terrorisme

La France est très engagée dans son combat contre le terrorisme, à la fois au Levant et en Syrie, mais surtout très engagée en première ligne en Afrique, face aussi à Daesh qui commence à s'implanter dans ces régions de façon très claire. Nous sommes très inquiets de l'évolution de la frontière sud de l'OTAN, du chaos qui est en train de s'installer en Libye et qui aura des conséquences extrêmement directes sur les nations Européennes—on le voit bien déjà avec la crise des migrants.

> **« La France est très engagée car elle a...été touchée profondément dans sa structure par des attaques informatiques. »**

La France est très engagée car elle a aussi été touchée profondément dans sa structure par des attaques informatiques. Deux éléments représentent les deux extrémités du spectre : en janvier, des attaques de très basse intensité en petit nombre provenant du mouvement hacktiviste se revendiquant de l'Etat Islamique; plus gênante, une attaque beaucoup plus importante et sophistiquée au mois d'avril qui a clairement visé le dispositif politico-médiatique français avec des répercussions plus profondes; cette attaque est plus intéressante puisqu'elle a été masquée par une certaine forme de brouillard, revendiquée par l'Etat Islamique, mais tout montre que derrière l'Etat Islamique, on remonte vers des mafias, des groupes Russophones. Qui sont-ils? Est-ce que ce sont de pures mafias? Est-ce que ce sont des groupes de mercenaires? Est-ce que ce sont des corsaires ou est-ce que ce sont des services déguisés? Je vous laisse répondre à cette question mais ce sont bien les interrogations qui sont devant nous et qu'il appartient aux étatiques, aux services de renseignement, de répondre face à nos autorités politiques.

Le décor est donc planté et nous l'avons vécu au plus profond de notre système Parisien de la cyberdéfense. Guillaume Poupard pourra s'exprimer là-dessus lui aussi puisqu'il était davantage au coeur de ces affaires que nous. Ce qu'il est intéressant de retenir, c'est que l'espace numérique n'est qu'une dimension supplémentaire essentielle, un multiplicateur de force et un atout de conflit dans les espaces normaux. Il peut y avoir des actions pures dans l'espace numérique mais le plus souvent les tensions que l'on ressent actuellement avec la crispation en Europe du fait des positions Russes et, de l'autre côté, d'une émergence galopante d'un Islamisme qui a besoin de sa propagande pour exister, envahissent l'espace numérique. Pour nous nations, cela veut dire qu'il faut être capable de maintenir la sécurité et la paix dans ce nouvel espace et, pour nous militaires, c'est un défi parce qu'il faut apprendre à combiner ces nouvelles formes de combat. C'est aussi un défi puisque le flanc sud de l'OTAN est directement menacé et pour la première fois depuis bien longtemps, nos territoires nationaux sont aussi directement menacés. Les armées françaises sont très fortement engagées sur le territoire national en soutien et en appui des forces de sécurité intérieures. Nous avons aujourd'hui autant de militaires engagés en uniforme et en armes sur le territoire national qu'en opérations de combat de haute intensité à l'extérieur. Donc les réponses que nous devons donner et que nos autorités politiques attendent ne sont pas des réponses à moyen terme ou à long terme; ce sont des réponses quasi immédiates dans les jours et les semaines qui viennent. Je pense que cette dimension de temps est extrêmement importante et elle concerne chacune des nations engagées aujourd'hui dans les combats.

Rétablir la Confiance entre Nations face à des Menaces Communes

Devant ces enjeux, les nations qui ont de plus en plus des valeurs communes, font face à des combats qui sont bien des combats de valeur en présence du retour d'un nationalisme galopant et, de l'autre côté, d'une idéologie comparable à celles en son temps du communisme Stalinien ou d'Hitler. Dans ce combat, il faut que les nations apprennent à faire front commun. Mais on sait bien que, dans l'espace numérique, nous n'avons pas d'amis. Cet espace est fortement marqué par des activités d'espionnage et les meilleurs espionnages se font entre amis et parfois entre amis extrêmement proches. Donc c'est bien pour cela qu'il faut rétablir la confiance et cette confiance ne se fait pas de façon naïve. Elle se fait entre partenaires responsables, elle se fait au sein de coalitions probablement ad hoc, et surtout face à des menaces communes. Il est plus facile de rebâtir ou de bâtir une confiance dans un domaine militaire quand on sait qui est notre ennemi, quand on sait quelles sont les valeurs qui sont menacées, plutôt que dans d'autres domaines plus généraux où les intérêts politiques, économiques, et diplomatiques peuvent être beaucoup plus complexes à décrypter.

« ...dans l'espace numérique, nous n'avons pas d'amis. »

Qu'avons nous fait au Ministère de la Défense? Notre ministre a souhaité que l'on organise un grand évènement au mois de septembre dernier. Au-delà du côté débat stratégique, qui avait pour but de recentrer une partie du débat sur le combat, sur le volet militaire, cet événement avait aussi pour but de créer de façon très concrète un « cluster » de cyber commandeurs entre nations qui on une certaine maturité dans leur chaîne de commandement cyber. C'est pour cela que nous l'avons lancé à ce moment-là avec le plein soutien de nos camarades Britanniques et Américains. Très simplement, ce cluster de cyber commandeurs, c'est apprendre à se connaître, apprendre à bâtir, à coopérer, à avoir des liens de haut niveau, et faire en sorte que nos adjoints ne se voient pas simplement dans les instances très formelles de l'Union Européenne et de l'OTAN, mais qu'il y ait bien au dessus de cela des rapports de confiance où l'on puisse s'exprimer librement et surtout où l'on puisse se voir de façon très régulière. L'idée derrière ce cluster des cyber commandeurs né en septembre est qu'il se réunisse deux fois par an, en profitant du grand forum annuel qui se tient à Tallinn autour du Centre d'Excellence de l'OTAN, où se rendent toutes les nations dont les capacités militaires sont intéressantes. L'an prochain, l'édition de ce forum sera reprise par nos camarades Britanniques—je vous renvoie aux déclarations conjointes des deux ministres de la Défense français et britannique. Donc il s'agit de mesures concrètes, de bâtir la confiance dans des cercles de coopérants.

Nous avions « pour but de créer...un « cluster » de cyber commandeurs entre nations. »

La Cyberdéfense Française face aux Grandes Aggressions Informatiques

Au niveau du Ministère de la Défense français, la dynamique lancée en 2008 par le livre blanc et la programmation militaire 2008 s'est poursuivie. Nous avons écrit un livre blanc en 2013-2014. Ce livre blanc, qui est traduit en Anglais, comporte plus de 13 pages consacrées à la cyberdéfense et à la cybersécurité et il annonce extrêmement clairement une doctrine française de réponse face à des grandes agressions informatiques. Cette doctrine n'est pas une doctrine de dissuasion comparable à la doctrine nucléaire qui est une arme de non-emploi. Le cyber est une arme de prolifération, une arme d'emploi, et une arme qui est marquée par le brouillard. Donc, face à cette doctrine, on adopte quelque chose d'assez classique que l'on retrouve d'ailleurs pratiquement chez toutes les autres grandes nations, qui est de renforcer très fortement notre position défensive sous l'autorité de notre Premier Ministre. Le responsable de ce volet, c'est Guillaume Poupard, et de l'autre côté, face à ces attaques de grande ampleur, nous pourrions répondre par tous les moyens à notre disposition—politiques, policiers et diplomatiques, dans un premier temps de façon progressive, sans nous interdire le recours aux moyens coercitifs qui relèvent du Ministère de la Défense. Mais une attaque informatique ne requiert pas nécessairement une réponse informatique mécanique: on ne répond pas forcément à une attaque par missile par un renvoi de missile. Lorsqu'une attaque informatique prend place dans un contexte général, la réponse doit correspondre aux valeurs éthiques et morales de la nation qui est attaquée. Nous sommes des nations occidentales, donc nous ne répondons pas forcément à des attaques informatiques par des choses brouillardeuses du même genre, ou encore nous ne répondons pas à de la propagande par de la propagande de même niveau. Tous ces débats sont devant nous.

Ces différents documents se sont traduits par des lois de programmation militaire qui nous accordent des budgets. Dans les quatre à six années à venir, nous aurons au sein du ministère de la Défense plus d'un milliard d'euros à consacrer à cette fonction, et surtout plus de mille postes nouveaux qui seront créés avec de hautes fonctions de cybersécurité et cyberdéfense. Ensuite, nous avons réuni un ensemble d'outils, une sorte de plan stratégique, qui nous permet de mobiliser l'ensemble des énergies de notre ministère dont toutes les actions de 2014 à 2016 ont été prévues. Ce plan est suivi directement par Monsieur Jean-Yves le Drian et nous lui rendons compte environ tous les six mois, ce qui nous oblige à aller vite. Nous avons également pris une initiative assez originale parce que nous nous sommes aperçus extrêmement rapidement que l'élément le plus important pour créer une capacité de cyberdéfense est avant tout ses ressources humaines. Pour créer ces ressources humaines, il faut d'abord gérer leurs carrières et les concentrer en deux endroits en France pour ne pas les disperser partout au sein des différentes armées. Nous avons créé pour cela ce que nous appelons dans notre jargon le pôle d'Excellence Bretagne qui est centré principalement sur la bonne gestion de nos capacités et la concentration de nos ressources humaines. Ce pôle d'Excellence Bretagne comporte deux volets. Il y a un volet de partenariat public/privé avec l'industrie et surtout avec tout le tissu intellectuel et éducatif de cette région. Il y a également un grand volet de ces ressources humaines, avec l'accent mis sur la formation et l'entraînement et une relation publique/privée entre l'état et une des grandes régions françaises. C'est un engagement pris par le Premier Ministre qui est inscrit dans le Pacte d'avenir pour cette région.

> **« Ce plan est suivi directement par Monsieur Jean-Yves le Drian et nous lui rendons compte environ tous les six mois »**

Vis-à-vis de l'Union Européenne et de l'OTAN, la France est très active et continuera à être très engagée dans ce domaine. Nous participons à l'ensemble de ces deux groupes. Nous allons beaucoup insister sur la communalité de projets concrets et sur le rapprochement entre ce que fait l'OTAN et ce que doit faire l'Union Européenne dans le domaine militaire. Nous avons un remarquable outil aujourd'hui autour du Centre d'Excellence de Tallinn auquel un très grand nombre de nations se sont ralliées. Ce centre est comme le coeur de l'entraînement de l'OTAN et de l'Union Européenne auquel chaque nation peut venir accorder son propre système d'entraînement. Chaque nation aura besoin d'entraîner ses forces et de développer ses propres capacités de formation et d'entraînement, à l'identique de ce qui est fait pour les autres capacités militaires—qu'elles soient terre, mer, ou air.

Une Chaine de Commandement Militaire Préparée pour une Attaque de Grande Ampleur

Pour conclure, je vais revenir rapidement sur ma chaîne de commandement. Cette chaîne de commandement militaire a aujourd'hui environ cinq ans d'ancienneté. Nous commençons à avoir une relative maturité, qui reste cependant extrêmement modeste. En effet, l'espace numérique doit nous imposer de rester extrêmement modestes et la question qu'il faut se poser n'est pas: « Est-ce que je suis capable de résister à une attaque? » C'est « Quel sera l'état de préparation de ma chaîne, quel sera l'état de préparation de mes spécialistes ? » quand je prendrai conscience que j'ai été pénétré et que je suis confronté à une attaque de très grande ampleur. Actuellement, les réseaux du ministère de la Défense ont peut-être été pénétrés depuis quelque temps; je suis incapable d'en mettre ma main au feu. Je pense que quelques grandes nations ont eu aussi ce genre d'expérience et qu'il faut rester extrêmement modeste face à des attaques informatiques. Quand un service de renseignement veut y mettre les moyens, il peut rentrer dans le réseau de n'importe quel partenaire ou de n'importe quel adversaire. Après, il est plus compliqué d'y rester, mais la première chose, même si on a des moyens, c'est d'avoir une très grande modestie dans ce domaine.

> **« ...les réseaux du ministère de la Défense ont peut-être été pénétrés depuis quelque temps; je suis incapable d'en mettre ma main au feu. »**

Nous devons aussi apprendre à combiner des actions de lutte informatique défensive. Qu'est-ce que cela veut dire? Cela veut dire que, face à une attaque, vous agissez de façon réactive, vous ne laissez pas un attaquant rentrer complètement chez vous. Je vous renvoie en France à l'article 21 de la Loi de Programmation Militaire qui protège légalement nos propres agents et les autorise à rentrer en interaction avec un attaquant qui viendrait menacer fortement nos capacités militaires, économiques et industrielles—donc les intérêts stratégiques de la France—afin de neutraliser les effets de son action sur nos propres réseaux. Comme vous le voyez, la défense active, vue du côté français, est pour l'instant une évolution de notre

droit qui nous permet de faire des contre-mesures. Cela ne nous permet en aucun cas de mener des opérations offensives mais simplement de prendre les mesures qu'il faut aux endroits où il faut, en collaboration avec les partenaires qu'il faut, pour que les effets de cette attaque sur nos réseaux cessent. Donc, nous sommes bien dans une logique de mise en place de contre-mesures variées, organisationnelles ou autres. La loi est écrite, les modalités pratiques autour de cette forme de défense active sont beaucoup plus compliquées, mais je pense que la loi Française aujourd'hui est une des lois au monde parmi les plus achevées, du moins sur le plan juridique.

Qu'est-ce que la lutte informatique offensive? Pour nous militaires, ce sont deux choses. Cela peut être une forme de frappe en profondeur : lorsqu'on lance aujourd'hui des missiles de croisière pour frapper le coeur d'un dispositif ennemi, c'est cela la lutte informatique offensive. Mais c'est également une forme de combat tactique en soutien de la manœuvre terrestre, maritime ou aérienne, pour permettre aux forces conventionnelles de se déployer, de mener leurs propres actions et de perturber nos ennemis. Pour faire tout cela, nous avons besoin bien sûr de renseignements, et nous avons donc développé le Conseil de renseignement d'intérêt de cyberdéfense qui est le renseignement qui sert aux acteurs de la chaîne militaire de cyberdéfense. Tout cela se conçoit bien sûr dans les trois couches : la couche physique, la couche logique puis, de plus en plus, la couche sémantique. L'arme informatique pour nous est devenu un nouvel outil, ou plutôt qu'outil, je préfère le terme « nouvelle capacité » qui doit apporter un appui et surtout se combiner aux autres capacités militaires des forces armées et capacités de frappe de l'affronteur ou alors servir d'appui tactique à la manœuvre.

Les Valeurs Communes face à la Propagande Propagée sur les Réseaux Sociaux

Enfin, un défi qui me paraît aujourd'hui extrêmement important pour l'ensemble des nations démocratiques que nous représentons ici, est que l'espace numérique a explosé depuis la fin des années 90. Nous avons dressé un constat officiel fin 2010 de l'explosion des opérations d'espionnage chinoises, de celles de nos camarades américains avec les révélations Snowden, et d'autres affaires que les spécialistes connaissent mieux, qui montrent qu'en matière d'espionnage, il n'y a pas d'amis. On voit également apparaître des attaques de profondeur à des fins de sabotage avec de plus en plus de prises d'otages informatiques par les mafias qui montrent que ces domaines ne sont pas des surprises stratégiques. Ce qui est particulièrement choquant, c'est l'emploi massif actuel dans les grands conflits d'une propagande parfaitement outillée et orchestrée à travers l'ensemble de réseaux sociaux—pas seulement Facebook et Twitter, mais aussi les réseaux de type Instagram vers lesquels les Islamistes se déplacent très rapidement. Ce jeu du chat et de la souris qui est d'appréhender et de connaître techniquement les nouveaux réseaux sociaux qui apparaissent alors qu'ils n'existaient pas trois mois auparavant est extrêmement compliqué à maîtriser pour les états et pour les acteurs de la cyberdéfense car chaque réseau social représente une nouvelle topographie et de nouveaux modelés de fonctionnement. C'est comme si on prenait une compagnie tactique de l'armée de terre qui s'entraîne pour attaquer dans une vallée et que, cinq minutes avant la fin de son opération, on change les cartes et les objectifs; le lieu est toujours le même mais au lieu de passer par la vallée de gauche, il faut passer par la vallée de droite. Ces groupes de propagande sont extrêmement habiles pour exploiter les failles juridiques de nos pays, nos dispositifs pour préserver la liberté de nos citoyens et pour aller se nicher, tel des coucous, dans des endroits où il est juridiquement extrêmement compliqué pour nos services de police de les atteindre. Cet élément là me paraît très important, à la fois pour la conduite des opérations cybernétiques et aussi pour les discours qu'il faut mettre en place face à eux. Ce que l'on voit apparaître, c'est un discours nationaliste russe sans complexe fait par un groupe de hackers que les spécialistes appellent ATP28 et qui travaille derrière des pare-feux. Qui est ce groupe de hackers? Quel est son lien? Est-ce vraiment un groupe de hackers? Pourquoi ce groupe de hackers vient-il s'intéresser au conflit du Levant, au conflit en Syrie? Les discours que portent ces hackers ou ceux que portent les Islamistes sont des discours qu'il va falloir être capable de contrer sur le domaine des valeurs. Cela demande une réponse globale, pas seulement militaire, pas seulement des services techniques de cyberdéfense que nous représentons, mais un discours vraiment global sur l'ensemble de nos valeurs qui mette en première ligne nos diplomaties, nos services du Premier Ministre, nos services d'éducation. Etablir ce discours, c'est proposer des valeurs qui permettent d'aller contre celles d'un certain nombre de nos adversaires qui n'ont pas les mêmes valeurs démocratiques que nous.

> **« On voit également apparaître des attaques de profondeur à des fins de sabotage avec de plus en plus de prises d'otages informatiques par les mafias »**

Cyber Conflict at the Core of Military Operations

Vice Admiral Arnaud Coustillière[1]
General Officer for cyberdefense, Ministry of Defense

I am Admiral Coustillière and have been the general officer for cyberdefense at the Ministry of Defense for slightly more than five years. With my colleague Guillaume Poupard, director of the ANSSI since 2009, we have been actors in the development of French capabilities in this field. My responsibilities are dual. The first one is a ministerial responsibility to coordinate a number of political actions, international relations, and training. I am also fully integrated in the military chain of conduct of operations and in charge of planning and conducting cyberdefense operations, whether defensive or in support of our military operations. Today, my chain has reached five years of maturity and our current challenge is to put cyber conflict at the core of operations and learn how to combine it with the other forms of combat.

France's International and National Commitment against Terrorism

France is highly committed to fighting terrorism, both in the Levant and in Syria, and is especially in the frontline in Africa, where it is also fighting the Islamic State—a clearly growing presence in this region. We are truly concerned about the evolution of NATO's southern border and about the chaos that is settling in Libya, which will have extremely direct consequences for European countries as already illustrated by the migrants' crisis.

France is also highly committed because it was deeply impacted in its structure by cyber attacks. Two elements illustrate the two ends of the spectrum: in January, there were a small number of very low intensity attacks by a hacktivist movement claiming to be part of the Islamic State. More disruptive, an important and sophisticated attack took place in April that clearly targeted the French politico-media institutions, with major repercussions. This attack is more interesting because it was nebulous and was claimed by the Islamic State, but behind the Islamic State, the evidence pointed in the direction of Russian-speaking mafia groups. Who are they? Are they pure mafias? Are they groups of mercenaries? Are they pirates? Or are they disguised intelligence services? I will let you answer these questions, but these are the issues that our political authorities are expecting public officials and intelligence services to resolve.

> **"France is also highly committed because it was deeply impacted in its structure by cyber attacks."**

The stage has now been set by these attacks at the very core of our Paris cyberdefense system. It is worth noting that, normally, cyberspace is only one essential extra dimension, a force multiplier and an asset in conflict. Actions can be purely in cyberspace but usually tensions—like those we currently experience in Europe as a result of the Russian positions and the rapid ascent of an Islamism that needs its propaganda to exist—invade the cyberspace. As nations, we must be able to maintain security and peace in this new space and, as a military force, our challenge is to learn how to combine these new forms of combat. It is also a challenge, because the southern side of NATO is directly threatened, and for the first in a long time, our national territories are directly threatened. On the national territory, the French army has a strong commitment to support the interior security forces. Today, we have as many soldiers engaged in uniform and arms on the national territory as abroad in high intensity combat operations. Consequently, the answers we must give—and that our political authorities are expecting — are not medium-term or long-term answers; they must be practically immediate answers to be given in the next few days and weeks. This time dimension is crucial and concerns all countries that are engaged today in such combats.

Restoring Trust between Countries against Common Threats

Against these challenges, countries that share common values are fighting for these values in a context of a rising nationalism and, on the other side, of an ideology that is comparable to Stalinist communism or Hitler's ideology. In this fight, it

1 Translated by Mr. Antoun Meroueh, Institut d'Etudes Politiques de Paris.

is critical for nations to learn how to stand together. However, it is well known that there are no friends in cyberspace. This space is strongly marked by espionage activities and the best espionage activities happen between friends and sometimes between extremely close friends. This is why we need to restore trust, and this trust cannot be naive. It is built between responsible partners, probably within *ad hoc* coalitions, and especially against common threats. It is easier to build or rebuild trust in military matters when the enemy and the threatened values are identified, rather than in broader matters where the political, economic, and diplomatic interests can be much more complex to analyze.

"It is well known that there are no friends in cyberspace.

What have we done at the Ministry of Defense? Our minister called for the organization of a major event last September. Beyond the strategic debate, whose purpose was to focus part of the debate on combat and military aspects, this event's aim was to create a cluster of cyber commanders among countries whose cyber chain of command is relatively mature. This is why we launched it on this occasion, with the full support of our British and American friends. To put it simply, the cyber commanders cluster is about learning how to know each other, how to build, how to cooperate and have high-level relations. Instead of only meeting in formal bodies like the European Union and NATO, the goal is to establish trusting relationships that make it possible to speak freely and, more importantly, to meet on a regular basis. The cluster of cyber commanders will meet twice a year and will take advantage of the large annual forum in Tallinn at the NATO Center of Excellence, which gathers all countries with worthwhile military capabilities. For the next edition of this forum, which will be organized by our British counterparts, I refer you to the joint statements of the French and British Ministries of Defense. These are concrete measures intended to build trust within circles of cooperators.

"Our aim was to create a cluster of cyber commanders between countries whose cyber command is relatively mature."

French Cyberdefense against Large-scale Cyber Attacks

At the level of the French Ministry of Defense, the momentum created by the 2008 White Paper and the 2008 Military Planning law has continued. We wrote a White paper in 2013-2014. This White Paper, which has been translated into English, devotes more than thirteen pages to cyberdefense and cybersecurity and clearly sets out the French doctrine of response to large-scale cyberattacks. This is not a deterrence doctrine akin to the nuclear doctrine that advocates the non-use of nuclear weapons. Cyber is a weapon of proliferation, a weapon to be used, and a weapon that is nebulous. Therefore, like in almost all major countries, we have adopted rather traditional measures that seek to strongly reinforce our defensive position under the authority of our Prime Minister. Guillaume Poupard is in charge of this aspect. On the other side, when faced with large-scale attacks, we may respond with all necessary political, police and diplomatic measures—gradually at first, but without ruling out the use of coercive measures falling under the competence of the Ministry of Defense. Nevertheless, just as one does not inevitably respond to a missile strike with another missile strike, a cyberattack does not necessarily warrant a cyber response. When a cyberattack takes place in a general context, the response must fit the ethical and moral values of the targeted country. Western countries do not necessarily respond to cyberattacks with attacks of the same kind and, similarly, they do not respond to propaganda with a similar propaganda. All these debates are in front of us.

These various documents resulted in Military Planning laws that grant us a budget. In the next four to six years, the Ministry of Defense will have at its disposal over one billion euros and more than a thousand new positions will be created with high responsibilities in matters of cybersecurity and cyberdefense. We have also put together a set of tools, a kind of strategic plan, which allows us to mobilize all the resources of our ministry for the period 2014 to 2016. Minister Jean-Yves Le Drian follows this plan personally and, since we report to him approximately every six months, we must progress quickly. We have also taken a rather original initiative after we realized early on that human resources are a key element in the creation of cyberdefense capabilities. In order to build these human resources, it is necessary to manage their careers and concentrate their location in France to prevent their dispersion within the various army corps. That is why

"Minister Jean-Yves Le Drian follows this plan personally...so we must progress quickly"

we created the so-called « Brittany pole of excellence » which is mainly centered on the good management of our capabilities and centralization of our human resources. This Brittany pole of excellence features two major aspects. First, there is a public/private partnership with industry and especially with all the intellectual and educational fabric of this region. There is also a large part dedicated to these human resources, with an emphasis on training and practice, and a public/private relationship between the State and one of France 's large regions. This commitment, which was made by the Prime Minister, is written in the region's "Pact for the future."

With respect to the European Union and NATO, France is very active and will continue to be extremely active since we take part in these two groups. We will insist on a commonality of concrete projects and a convergence between what NATO is doing and what the European Union should be doing in the military domain. The Center of Excellence in Tallinn is a remarkable tool that a very a large number of nations has joined. It is the heart of the NATO and EU training, to which each nation can adjust its own training system. Each nation will need to train its own forces and develop its own capabilities along the lines of what is being done in the other ground, sea, or air military capabilities.

A Military Chain of Command Prepared for a Large-scale Attack

I will quickly come back to my chain of command. This military chain of command is now about five years old. Although we are becoming mature, our maturity remains extremely modest. In cyberspace, we must always remain extremely modest. If we become aware that we have been penetrated and that we are confronted to a large-scale attack, our question should not be "Are we able to resist an attack?" but rather "What will be the readiness of our chain, what will be the readiness of our specialists?" Our Defense Ministry's networks may have been penetrated for some time now; I would not bet on it, but I believe that some large nations may have experienced cyberattacks and that we must remain extremely modest in this situation. If an intelligence service decides to enter the network of a partner or adversary, it has the means to do so. Afterwards, it is more complicated for them to stay inside, but, even when means are available, it is important to remain modest.

"Our Defense Ministry's networks may have been penetrated for some time now; I would not bet on it."

We must also learn how to combine cyberdefense actions. What does that mean? When you are faced with an attack, you act in a reactive way and do not let your attacker in completely. In France, Article 21 of the Military Planning Law legally protects our own agents and authorizes them to interact with an attacker that could significantly threaten our military, economic and industrial capabilities—in other words France's strategic interests—in order to neutralize the effects of his action on our networks. At the moment, active defense in a French perspective is a legal evolution that allows us to counteract. It does not allow us in any way to conduct offensive operations but rather to take the right measures, in the right places, in cooperation with the right partners, to end the effects of the attack on our networks. Therefore, our strategy is to put together organizational countermeasures. The law exists and, although the practical modalities related to this form of active defense are much more complicated, I believe that this French law is one of the most complete in the world today, at least on the legal level.

What constitutes an offensive cyber operation? For us in the military, it is two things. It can be a kind of in-depth strike: when cruise missiles are launched to strike at the heart of an enemy position, it is an offensive cyberattack. But it is also a kind of tactical combat in support of terrestrial, maritime or air operations to allow conventional forces to be deployed, carry out their own operations and unsettle our enemies. In order to do all that, we obviously need intelligence and, consequently, we have developed the Intelligence Council on Cyberdefense which provides the intelligence used by the actors of the cyberdefense military chain. All of that is of course addressed in the three physical, logical, and increasingly semantic layers. The cyber weapon has become a new tool for us, or rather than a tool, a new capability that brings support and can especially be combined with other military and strike capabilities of the armed forces, or even be used as tactical support during an operation.

Our Common Values against the Propaganda Disseminated on the Social Networks

Finally, the cyberspace explosion that started at the end of the nineties is an extremely important challenge today for all the democratic countries that we represent here. At the end of 2010, we prepared an official report on the explosion of Chinese spying operations, on those of our American counterparts following the Snowden revelations, and on other operations that are well known to specialists. The report showed that, in matters of espionage, there are no friends. At the same time, in-depth sabotage attacks started to appear with an increasing number of cyber "hostage-taking" by mafias that show that these fields are not strategic surprises. What is particularly shocking is the current massive use in large conflicts of a perfectly equipped and orchestrated propaganda through social networks—not only Facebook and Twitter, but also networks like Instagram that Islamists are moving to very quickly. This cat and mouse situation of technically understanding new social networks that did not exist three months before is extremely complicated for states and cyberdefense actors to control, because each social network represents a new topography and a new operating model. It is as if a tactical army division were training for an attack in a valley, and five minutes before the operation, the maps and objectives had changed; the location is still the same, but instead of going through the left valley, the division is now required to go through the right valley. These propaganda groups are extremely skilled at exploiting the legal loopholes in our countries, the measures that protect our citizens' freedom, and they go and nest like cuckoos in places where it is legally very complicated for our police services to reach them. This element is very important, both for the control of cyber operations and for our counterspeech. What we now see appearing is an assertive Russian nationalist discourse by a group of hackers working behind firewalls that specialists call ATP28. What is this group of hackers? What are their links? Is this really a group of hackers? Why is this group of hackers interested in the conflict in the Levant, in the conflict in Syria? We need to counter their discourse or the Islamist discourse on ethical grounds. This will require a global response—not only military, not only coming from the cyberdefense technical services that we represent, but a truly global discourse on our set of values with, in the front line our diplomats, the Prime Minister services, and our education services. Constructing this discourse is proposing values that make it possible to counter those of a number of our adversaries who do not share the same democratic principles.

We are seeing "an assertive Russian nationalist discourse by a group of hackers working behind firewalls that specialists call ATP28."

La Stratégie de la France en matière de Cybersécurité

Mr. Guillaume Poupard
Directeur Général, Agence nationale de la sécurité des systèmes d'information (ANSSI)

Je vais m'inscrire dans la continuité des propos tenus par l'Amiral Coustillière. Comme il l'a dit, nous travaillons main dans la main depuis maintenant un bon nombre d'années pour construire une réponse française aux problématiques posées par les cybermenaces. Bien évidemment, les questions de cybersécurité sont traitées depuis longtemps; elles étaient même traitées avant que le mot cyber ne soit devenu un « buzzword », un mot à la mode que l'on entend partout. La France fait depuis longtemps de la sécurité des systèmes d'information comme dans tous les pays. Ce qui a changé, c'est le périmètre d'action, les systèmes à protéger, l'intensité de la menace, la motivation des attaquants, et les possibilités techniques offertes à ces attaquants. Quand je regarde simplement vingt ans en arrière lorsque j'ai commencé à travailler dans ce domaine, comparé à aujourd'hui, les problèmes à l'époque étaient simples, même si nous n'en étions pas conscients, et vraiment limités à de très petits périmètres.

Création de l'Agence Nationale de la Sécurité des Systèmes d'Information

Aujourd'hui, la question est extrêmement vaste et a nécessité une évolution très rapide de nos doctrines, de notre organisation, et une agilité permanente de la part de beaucoup d'acteurs là où auparavant la cybersécurité était le domaine réservé de quelques experts. Historiquement donc, c'est une histoire très récente. La prise de conscience officielle en France est apparue en 2008 avec le Livre blanc de la défense et la sécurité nationale qui a fait apparaître, aux côtés des autres menaces qui ne sont pas pour autant réduites—menaces militaires, menaces civiles et endémies, toutes les menaces qui peuvent peser sur une nation—la menace cyber comme étant une menace en très forte croissance et un sujet à traiter d'urgence au niveau français. Mais ce travail stratégique n'en disait pas beaucoup plus si ce n'est qu'il fallait créer une agence, celle que je dirige aujourd'hui, avec deux caractéristiques liées à la doctrine française. Une première caractéristique est de clairement séparer les activités défensives des activités offensives. L'autre caractéristique permise par notre système politique a été de positionner cette agence nationale au niveau du Premier Ministre. L'idée était que le sujet cyber n'était plus dorénavant uniquement un sujet restreint, militaire ou diplomatique, mais qu'il allait toucher l'ensemble des domaines à des niveaux évidemment variés. Il était donc difficile de confier ce sujet cyber à une seule branche de notre organisation au risque de laisser de côté beaucoup d'autres aspects.

> **Pour ANSSI, « ...une première caractéristique est de clairement séparer les activités défensives des activités offensives. »**

Donc, cette agence a été créée en 2009, avec depuis un taux de croissance qui est assez original dans le contexte budgétaire actuel que nous connaissons en France et que d'autres pays connaissent également, qui est celui de contraintes fortes. Notre taux de croissance est limité uniquement aujourd'hui par notre capacité à recruter, à former, et à intégrer des experts de très haut niveau de manière à répondre à la menace. Dans le contexte actuel, cela est très original et traduit la prise de conscience extrêmement forte, jusqu'au plus haut niveau de l'état, du fait que le sujet cyber doit être traité en y mettant tous les moyens nécessaires. Si cette agence est interministérielle, c'est bien parce que justement, une partie de ce travail doit être mutualisée. Donc, nous avons un rôle de prévention, un rôle opérationnel de traitement des attaques, et aussi un rôle de coordination car une part importante du travail doit également être faite dans les différents ministères. L'Amiral Coustillière est revenu sur ce que fait le ministère de la Défense qui est énorme dans son domaine. De même, nous avons une coopération extrêmement forte et qui continue à se développer avec le ministère des Affaires Etrangères. L'Ambassadeur David Martinon, qui parlera ce matin, vient de prendre en charge la question de la cybersécurité pour le ministère des Affaires Etrangères à la suite de l'Ambassadeur Florence Mangin. Les questions de cyber comportent évidemment un important côté diplomatique qui ne fait que se confirmer.

Au sein du ministère de l'Intérieur, nous avons depuis quelques mois un coordinateur cyber, le Préfet Jean-Yves Latournerie, qui interviendra également dans un panel aujourd'hui. Il coordonne les nombreuses actions qui relèvent du ministère de l'Intérieur, de la Police, et de la Sécurité intérieure. Là encore, le rôle d'une agence interministérielle comme celle que je dirige n'est certainement pas de faire ce travail à la place du ministère de l'Intérieur. Dans le domaine économique, le ministère de l'Economie et le secrétaire d'Etat au Numérique ont une implication très forte. La cybersécurité est essentielle aujourd'hui au développement de nos entreprises, ne serait-ce que pour éviter d'empêcher leur développement. Elle est également une opportunité en termes de développement économique puisqu'elle devient une activité industrielle à proprement parler qu'il faut développer parce que nous en avons besoin. C'est peut-être un mal nécessaire pour les plus négatifs d'entre nous mais je suis beaucoup plus positif. Je considère que les états ne seront jamais en mesure de couvrir l'ensemble de la menace cyber, quels que soient les moyens investis. Nous avons besoin d'un relais privé fort, compétent, de confiance, capable d'apporter des solutions à tous ceux qui en ont besoin et aujourd'hui il n'y pas grand monde qui n'ait pas besoin de se protéger face à cette menace. Je pourrais citer bien d'autres ministères, la Justice bien évidemment, pour qui le traitement du cyber va devenir une tâche de plus en plus importante, et puis l'enseignement supérieur, la recherche, le ministère du Travail. La plupart des branches ministérielles sont concernées, d'où l'importance d'avoir une coordination forte au niveau interministériel.

Définition d'une Stratégie Nationale autour de Cinq Axes

Afin de fixer un cadre à cette action d'acteurs extrêmement variés et multiples, nous avons fait depuis un an un travail de définition d'une stratégie nationale visant justement à canaliser les énergies de chacun, à se fixer des objectifs communs, pour ensuite être capables de les décliner de manière précise et en fonction des missions et des compétences de chacun au sein de chaque département ministériel. Ce travail de stratégie a abouti il y a seulement trois semaines avec la présentation par notre Premier Ministre d'un document de Stratégie nationale qui est public—vous pouvez le trouver sur le site internet traduit en anglais, en allemand, et en espagnol, de manière justement à avoir une ouverture vis-à-vis de nos partenaires. Ce document trace les grands axes, forcément à un niveau relativement macroscopique, de ce que va être notre action dans les années à venir, j'ai envie de dire dans les quelques années à venir puisque, là encore, il faut être très modeste. Quand on voit à quelle vitesse les choses évoluent, il est évident qu'avoir une stratégie à trente ans n'a probablement aucun sens dans un domaine comme le cyber. Ce document s'articule autour de cinq axes qui reprennent les thématiques majeures qui sont soit déjà développées, soit a développer impérativement dans les mois et les années à venir. Je vais rapidement les parcourir.

La Cybersécurité relève de la Souveraineté Nationale. Le premier de ces axes, qui est déjà largement traité mais où il reste énormément de travail à faire, consiste à dire que la cybersécurité est une question de souveraineté nationale. C'est quelque chose d'assumé en France que la cybersécurité doit impérativement être prise en compte au plus haut niveau, avec un niveau maximal de priorité, car la souveraineté de la nation est en jeu. Quand on parle de souveraineté, on pense bien entendu aux activités de l'état, aux activités militaires, mais également à toutes les infrastructures critiques qui sont essentielles à la sécurité de la nation. Je sais que cette préoccupation est partagée par tous nos alliés, y compris tous ici dans cette salle. C'est une préoccupation complexe car le nombre d'acteurs est important et beaucoup sont des acteurs privés; les préoccupations de chacun sont extrêmement variées; les contextes techniques, opérationnels, financiers, sont extrêmement variables d'un domaine à l'autre; et il est difficile d'avoir une réponse unique commune dans des domaines aussi différents que la finance, l'énergie, l'industrie de l'armement, les transports, les télécommunications—autant de domaines dont le disfonctionnement peut être extrêmement grave pour la nation et qui sont aujourd'hui directement visés par la menace cyber.

«...la souveraineté de la nation est en jeu. »

En deux mots, l'approche française consiste, non pas à conseiller et à pousser les gens à sécuriser, mais à imposer la sécurité aux opérateurs critiques, ceux que l'on appelle en France les opérateurs d'importance vitale. Donc, nous sommes en train de mettre en place un dispositif porté par la Loi de programmation militaire votée en décembre 2013 qui consiste à imposer quatre règles de sécurité aux opérateurs d'importance vitale. Je dis bien imposer, et pas simplement conseiller—nous ne sommes pas au niveau des «

« l'approche française consiste... à imposer la sécurité aux... opérateurs d'importance vitale. »

best practices »—nous sommes au niveau d'imposer des règles, d'imposer la notification d'incidents, et également de venir voir mon agence pour indiquer les attaques. Tout ceci n'est plus optionnel car imposer des contrôles de sécurité au sein de ces opérateurs va devenir obligatoire. Enfin, en cas de crises majeures, qui ne se sont pas vraiment produites en France pour le moment mais je ne peux malheureusement pas imaginer que cela ne se produise pas un jour, il y a la possibilité pour le Premier Ministre de donner des instructions extrêmement strictes à ces opérateurs d'importance vitale. Il s'agit d'éviter le risque de contagion, le risque systémique propre au cyber qui, par une attaque sur un secteur donné, peut très rapidement toucher l'ensemble des secteurs d'importance vitale. Cette approche par la loi est possible en France, elle est soutenue politiquement, et elle est comprise par les opérateurs avec qui nous avons énormément de dialogues. Le côté très obligatoire de tout cela est compensé par un travail en coopération extrêmement fort avec les différents ministères, mais surtout avec les opérateurs eux mêmes et c'est cela la clé du succès. Chercher à imposer des choses qui vont coûter de l'argent mais qui ne sont pas comprises est une garantie d'échec. Nous avons fait avec les opérateurs un travail passionnant d'explications, de compréhension mutuelle des contraintes de chacun et des objectifs, et aujourd'hui nous sommes en train d'aboutir sur ces travaux avec la publication des règles techniques qui vont s'appliquer dans les différents domaines. Cela va nous permettre d'avoir la démarche la plus efficace possible face aux menaces, le but étant non pas d'empêcher la menace, non pas de la supprimer car on ne sait pas le faire, non pas non plus d'apporter une sécurité absolue à nos opérateurs car personne n'y croit, mais bien de gagner du temps et d'éviter que chaque opérateur ne réagisse après que des attaques graves aient été commises. On veut anticiper ces attaques et limiter leur impact au maximum.

> **« ...imposer des choses qui vont coûter de l'argent mais qui ne sont pas comprises est une garantie d'échec. »**

Protection de l'Economie et des Citoyens. Le deuxième point concerne tous les autres puisque il n'y a pas que les opérateurs critiques. Il faut protéger l'ensemble de l'économie et il faut protéger nos citoyens. Aujourd'hui ce niveau de protection est très inférieur à ce qu'il devrait être. Il faut apporter des solutions qui ne sont pas celles de tout le monde, qui ne sont pas celles que l'on peut apporter aux opérateurs d'importance vitale. C'est extrêmement varié et va bien au-delà de la sécurité des systèmes d'information, un domaine qui reste assez technique, jusqu'à la sécurité de l'information, qui embrasse beaucoup plus de choses. Aujourd'hui, c'est cela qu'il faut bien prendre en compte, y compris pour des questions de sécurité nationale. Prenons l'exemple des données personnelles: quand un citoyen se fait voler ses données personnelles ou se fait voler son identité, c'est triste pour lui mais cela n'a pas d'impact national; quand massivement les citoyens français se voient, en étant d'ailleurs plus ou moins complices, voler et utiliser leurs données personnelles à leur insu, nous avons la conviction que dorénavant, c'est potentiellement une question de sécurité nationale et donc cela concerne en priorité l'action de l'état.

> **« Il faut protéger l'ensemble de l'économie et il faut protéger nos citoyens. »**

Information à Tous les Niveaux. Le troisième point concerne l'information à tous les niveaux. Nous sommes aujourd'hui dans une situation critique car nous manquons d'experts pour faire de la cybersécurité dans le domaine public tout comme dans le domaine privé. Il faut impérativement amplifier la formation. Nous manquons également de capacités de sensibilisation de chacun au juste niveau. Sans transformer tout le monde en experts en cybersécurité, ce qui serait invivable, nous avons besoin que chacun connaisse un minimum nécessaire pour être acteur de la sécurité de ses propres données et de son environnement.

Protection de l'Industrie et Qualification des Prestataires de Service. Le quatrième point dont j'ai déjà parlé rapidement, concerne les questions industrielles. Il faut à la fois protéger l'industrie mais en même temps disposer de solutions de services de confiance. Pour ce faire, nous mettons tout un dispositif en place pour qualifier des prestataires de service afin que l'on puisse se retourner pour se sécuriser vers des acteurs compétents et de confiance.

Une Coopération Internationale qui n'est pas Naïve mais Indispensable. Le dernier point, qui sera ma conclusion, concerne l'approche internationale, la coopération. Comme l'Amiral l'a dit, je pense que nous tomberons rapidement d'accord sur cette question. Il est absolument indispensable de coopérer dans les bons cercles et à différents niveaux car la menace est

bien souvent commune; de coopérer de manière non naïve; et surtout de ne pas s'arrêter au fait que à la suite de révélations possibles, la confiance n'est pas forcément absolue. La coopération passe également par ce que l'on appelle le « capacity building ». Il faut impérativement que les nations qui ont commencé un peu plus tôt aident celles qui sont plus en retard à monter en gamme en terme de cybersécurité. C'est une démarche qui n'est pas philanthropique, elle est purement égoïste puisque comme cela a déjà été dit, les réseaux ne s'arrêtent pas aux frontières. Il est hors de question de cloisonner les réseaux informatiques, les réseaux de nos industriels étant déjà largement multinationaux. Pour nous protéger, même si le but est uniquement de protéger nos propres intérêts, il faut également aider les autres à se protéger.

Cette coopération non naïve est essentielle si nous voulons être capable de nous protéger face à cette menace.

France's Cybersecurity Strategy

Mr. Guillaume Poupard[1]
Managing Director, National Agency for information systems security (ANSSI)

As Admiral Coustillière mentioned earlier, we have been working together for many years to build a French response to cyberthreats. Obviously, cybersecurity issues have been a concern for a long time, even before the word cyber became a "buzzword" that we hear everywhere. Like all countries, France has been working on the security of its information systems. What has changed is the perimeter of action, the systems to be protected, the intensity of the threat, the motivation of the perpetrators, and the technical capabilities available to these perpetrators. When I started working in this field twenty years ago, the issues at the time were simple compared to today's and they were confined to well-defined areas.

Creation of the French Network and Information Security Agency (ANSSI)

Today, cybersecurity is an extremely broad domain that has required a fast-paced evolution of our doctrines and organization and a constant agility from many actors while it used to be the reserved area of a few experts. Official awareness in France emerged in 2008 with the White Paper on defense and national security that, along with other threats to the nation—military, civil and epidemic—mentioned cyberthreat as a steadily growing issue that France needed to address urgently. However, the White Paper did not say much more except that it was necessary to create an agency, the one I am heading, with two specific characteristics linked to the French doctrine. The first characteristic is to clearly separate defensive from offensive activities. The other, which our political system permits, has been to put this national agency under the authority of the Prime Minister. The idea was that the cyber issue was no longer a sole military or diplomatic subject but would extend to all domains, although to varying degrees. It was therefore difficult to entrust the cyber issue to only one branch of our administration at the risk of leaving many other aspects aside.

> **For ANSSI…"a first characteristic is to clearly separate defensive from offensive activities."**

Hence, this agency was created in 2009 and it has maintained a very strong growth despite the current context of budgetary constraints that France and other countries are experiencing. Currently, the sole limitation to our growth is our ability to recruit, train and integrate top-level experts to address this threat. This is quite unique and it reflects the extremely strong conviction, up to the highest level of the State, that the cyber issue should be addressed by all necessary means. If this agency is interministerial, it is precisely because a part of this work must be shared. We have a preventive role, an operational role in handling the attacks as well as a coordinating role, since an important part of the work must also be done in different ministries. Admiral Coustillière commented on the hard work the Ministry of Defense is doing in its field. Likewise, we have an extremely strong and steadily growing cooperation with our Ministry of Foreign Affairs. In replacement of Ambassador Florence Mangin, Ambassador David Martinon, who will intervene this morning, has just taken over the cybersecurity responsibility for the Foreign Ministry. Cyber issues obviously have a significant diplomatic side that is being confirmed every day.

Within the Ministry of the Interior, we now have a cyber coordinator, the Prefect Jean-Yves Latournerie, who will also intervene on a panel at this workshop. He coordinates the many actions that fall within the competence of the Interior Ministry, the Police department and the DGSI (General Directorate for Internal Security). There again, the role of an inter-agency organization like the one I am heading, is certainly not to do the job for Ministry of the Interior. In the economic sphere, the Ministry of Economy and the State Secretary for the digital economy are closely involved. Cybersecurity is now essential to the development of our businesses, if only to prevent attacks on their development. Since it is becoming an industrial activity in itself, it is also an opportunity that we must develop because we need it. The most pessimistic among us may view this as a necessary evil, but I am much more positive. I consider that states will never be able to cover

1 Translation by Mr. Antoun Meroueh, Institut d'Etudes Politiques de Paris.

all of the cyberthreats, no matter how many resources they invest in cybersecurity. We need the private sector to be a strong, competent and trustworthy relay, capable of providing solutions to all those who need them, and today virtually everyone requires protection against this threat. I could mention other Ministries, Justice of course, where dealing with cyber issues will become an increasingly important task, and also the Ministries of Higher Education and Research, and Labor. Since most ministerial departments are concerned, it is important to have a strong coordination at the inter-ministerial level.

A National Strategy Based on Five Pillars

In order to provide a framework for these multiple and extremely diverse actors, we have been working for the past year on the definition of a national strategy. Its goal is to channel the energies of all and set common objectives in order to be able to use them efficiently based on the missions and individual skills within each ministerial department. This work on strategy, which was completed just three weeks ago, led to the presentation of a National Strategy paper by our Prime Minister. The document is public and may be found on the website translated into English, German, and Spanish, in a spirit of openness towards our partners. It outlines the main pillars of our action in the years to come—I want to say in the next few years, because once again, you have to be very modest. When we see how fast things are changing, it is clear that having a strategy for the next thirty years probably does not make sense in an area like cyber. Five pillars cover the major themes that are either already developed or must be developed urgently in the coming months and years. I will go through them quickly.

Cybersecurity is a Matter of National Sovereignty. The first pillar, which has already been widely addressed but still requires much more work, is to make cybersecurity a matter of national sovereignty. In France, it is taken for granted that cybersecurity shall always be dealt with at the highest level and with the greatest priority because the sovereignty of the nation is at stake. When we talk about sovereignty, we are obviously thinking of state and military activities but also of the critical infrastructure that is essential to our nation's security. I know that all our allies share this concern, including those in this room. This is a complex situation which involves a large number of actors, many of which are private organizations, whose concerns are extremely diverse; the technical, operational and financial contexts are significantly different from one sector to another; and it is difficult to have one common response for sectors that are as diverse as finance, energy, defense, transportation, telecommunications—all sectors in which any disruption may prove extremely serious for our nation and are today directly targeted by cyberthreats.

> **"...the sovereignty of the nation is at stake."**

Simply put, the French approach is not to advise or incite people to get more security, but rather to impose security on critical operators, those we call in France the critical infrastructure operators. We are therefore putting in place a measure that is part of the Military Planning Law adopted in December 2013. It imposes four security rules to operators of vital importance, I mean imposes, not simply advises—this is not a matter of "best practices"—we are at a stage of imposing rules, imposing the notification of incidents and a requirement to come to my agency to report the attacks. All this is no longer optional, because enforcing security controls within these operators will become mandatory. Finally, in the event of major crises, which have not quite occurred in France yet, but I cannot imagine they will not happen one day, the Prime Minister will have the option of giving extremely strict instructions to these operators of vital importance. The goal is to prevent the risk of contagion, the systemic risk inherent to cyber issues, where an attack on a targeted area can quickly spread to all the sectors of vital importance. This law-based approach is possible in France, it is politically supported and understood by the operators that we are in contact with on a regular basis. The mandatory side of all this is compensated by a strong cooperation with different ministries and with the operators themselves, which is the key to success. Seeking to impose measures that would cost money but would not be understood is a guarantee of failure. We have achieved with these operators a fascinating explanatory work, a mutual understanding of each other's constraints and goals, and today we are about to complete these efforts with the publication of technical rules that will apply to these different domains. This will allow us to have the most efficient approach to threats, the goal being not to prevent the threat, not to suppress it because we would not know how to do it, not to provide an absolute security to our operators because nobody would believe it, but rather to gain time. We

> **"The French approach is...to impose security on critical operators, those we call in France the critical infrastructure operators.**

seeking to anticipate these attacks and minimize their impact.

Protecting the Economy and our Citizens. The second pillar concerns all the other actors because critical operators are not the only ones that matter. We must protect the entire economy and we must protect our citizens. Today this level of protection is lower than it should be and we must find unique solutions that are not those we are offering to operators of vital importance. The problem is extremely varied and goes beyond computer security—an area that remains quite technical—to information security, which has a broader sense. Today, this is what must be taken into account, including for reasons of national security. Let's take the example of personal data. When a citizen is a victim of personal data or identity theft, it is unfortunate for him but it has no national impact. However, when French citizens have their personal data massively stolen and used without their knowledge, we now believe that it is potentially a matter of national security and therefore a state response becomes required.

Information at All Levels. The third pillar relates to information at all levels. We are now in a critical situation because we lack as many cybersecurity experts in the public as in the private sectors. We must imperatively reinforce training. People must also have some level of awareness. Without turning everyone into a cyber security expert, which would be unbearable, everyone must know the minimum required to be an actor in protecting the security of his own data and environment.

Industry Protection and Service Providers Certification. The fourth pillar, which I have already mentioned briefly, relates to industry issues. We must both protect the industry and be able to provide trustworthy services solutions. In order to do so, we have set up a certification process for service providers so that those who wish to secure themselves can rely on competent and trustworthy actors for help.

A Genuine and Fundamental International Cooperation. The last pillar, which will be my conclusion, relates to the international perspective, i.e., to cooperation. As Admiral Coustilliere said earlier, I think that we shall quickly agree on this issue. It is absolutely essential to cooperate with the right people and at different levels because the threat is often common; to cooperate genuinely; and especially not to stop at the fact that, as a result of possible revelations, trust may not necessarily be total. This genuine cooperation is essential if we are seeking to protect ourselves against this cyberthreat. Cooperation also involves the so-called "capacity building:" nations that have had an earlier start must help those that are lagging behind so that they can catch up in terms of cybersecurity. This is not a matter of philanthropy, this approach is purely selfish because, as has already been said, networks do not stop at borders. There is no way we can keep our computer networks separate, because those that belong to our industry are already widely transnational. To protect ourselves, even if the goal is only to protect our own interests, we must also help others to protect themselves.

Responsible Behavior of States and Conflict Prevention In Cyberspace: *An Overview of the New UN Group of Government Experts (GGE) report*

Ambassador David Martinon
Ambassador for Cyber Diplomacy and the Digital Economy, French Ministry of Foreign Affairs

I will talk about the last two reports of the UN Group of Government Experts (GGE) and will make the most of other people's efforts and achievements since I was not part of the GGE at the time. My appointment in this position, in replacement of Ambassador Florence Mangin, is quite recent. For years, I have been the French representative at the ICAAN and ITU conferences and I will soon lead the French delegation at the next Internet Governance Forum (IGF). So I have mostly been in the civil part of cyber issues.

The New 2015 GGE Report Establishes Norms for the Protection of the Critical National Infrastructure

As diplomats, our job is to try to put an end to a conflict or to try to prevent it. This is certainly why France welcomes the new GGE report. We contributed a great deal to it, and we see real substantial progress in the new 2015 GGE report. What strikes me about that report is the difference that experts were able to make with regards to peacetime norms. Two years ago, almost everyone thought that the new GGE would maybe deal with the law of armed conflict and, on the contrary, there was a sort of general reluctance to tackle this grey area, which is below the threshold of armed conflict. In fact, this is the area where most of the attacks are likely to take place in the future, thereby threatening our national security. It seems that the law of armed conflict with its already very rich legal corpus was considered a more comfortable zone to begin with. That is why I view the last GGE report as a major success because it was able to frame this grey area with a symbolic threshold, which is the attack on Critical National Infrastructure (CNI). While not necessarily amounting to the level of an armed attack, attacks against the critical national infrastructure are the most likely to escalate into conflict and therefore, the new report contains various norms related to the protection of the critical national infrastructure.

> **"...attacks against the critical national infrastructure are the most likely to escalate into conflict"**

In the course of these negotiations, the French delegation proposed a two-fold normative ensemble: the first goal was to reinforce the critical infrastructure protection at the national level and we think that the outcome is excellent. I will quote it to make things really clear:

> "States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account, inter alia, General Assembly resolution 58/199 (2003) 'Creation of a global culture of cybersecurity and the protection of critical information infrastructure'."

This is a key step for us and, as Guillaume Poupard said earlier, France has established its own CNI cybersecurity scheming in 2013 through our Military Programming Act. We are now in the middle of implementing it. We are also due to take into account the future (hopefully soon) adoption of the Network and Information Security Directive (NISD) by the European Union.

States Need to Cooperate Better in order to Increase the Level of Protection of the Critical Infrastructure

The second goal is to increase the level of cooperation with regard to CNI protection. From the start, France supported a new principle that we could call "responsibility of the proxy." This principle helps to solve the attribution problem. It is very difficult to characterize an aggression in the cyberspace and it is even more difficult to characterize or to determine who the aggressor is. With this principle, the idea is less to put efforts on finding the attackers than to make every link of the chain more secure by inviting states to comply with their due diligence obligations. This is reflected in the report through two new norms of behavior and I will quote them:

"France supported a new principle that we could call 'responsibility of the proxy.'"

- States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.
- States should also respond to appropriate requests to mitigate malicious ICT activity aimed at another state's critical infrastructure emanating from their territory, taking into account due regard for sovereignty.

At the end of their work, the group had spent more time figuring out how to prevent armed conflict than focusing on how to manage it. Again, we think that this is an excellent achievement and we welcome this result.

Can the GGE Report Be Implemented Successfully?

How do we see the implementation process of the new GGE report? Of course, the whole credibility of the process will rely on the ability to implement the report and make it enforceable. For us, the two key words are transparency and capacity building.

Transparency. Transparency is key because the report establishes a lot of norms about CERTS and CNI and countries need to be more transparent about those norms. On CERTS, there should be no doubts about the actual mandate of governmental CERTS and points of contacts should systematically be made available. On CNI, countries should share information on their definition and on the selected critical sectors. They should also be transparent on their protective framework for CNI if any. This is another reason why we welcome the current work at the OSCE where a new set of confidence-building measures might entail such guidelines about CNI protection.

Capacity Building. It is hard to say whether any single country today would have the sufficient technical and institutional capacity to ensure a full implementation of the report, and when we talk about assistance, we know that assistance takes a lot of time and resources. In the future, we might need entire services dedicated to it. We know that it is necessary and that it will be resource-consuming. This is why, for some countries, the mere idea of a duty to assist can seem pretty far-fetched since they do not even have the capacity to protect their own networks, but it is a beginning and we have to go that way anyway.

"...for some countries, the mere idea of a duty to assist can seem pretty far-fetched since they do not even have the capacity to protect their own networks..."

What could be the next steps regarding the GGE process? Again, the work on norms is very satisfactory but we can do better and we will try. There is still a lot to do on the applicability of international law in peacetime and in the context of armed conflicts. What about state responsibility for example? It has unfortunately been left aside in the discussions, but it is difficult to envisage sovereignty without responsibility. So we will probably have to work on that. There will also be the question of the GGE format, which is a tricky question but what we are sure of is that it is being effective, it is legitimate, and its scope has to be broader.

Toward Long-Term International Stability in Cyberspace

Mr. Chris Painter
Coordinator for Cyber Issues, US Department of State

The Creation of a Stability Framework

The 2013 and 2015 UN Group of Governmental Experts (GGE) reports were fairly remarkable achievements. For the first time, there was agreement among fifteen then twenty countries, including China and Russia, that international law applies in cyberspace just like it does in the physical world. How it applies and what these terms mean specifically is still being worked out, but there was no backtracking and the report clearly said that the UN Charter international law applies.

> **The goal is "...to create long-term international stability in cyberspace so that no one has an incentive to disrupt that stability."**

Even so, there was some reticence on the part of our Chinese colleagues who argue that even talking about the applicability of international law in conflict somehow condones conflict in cyber space. This does not make a lot of sense and we need to press more on this issue, but the report is still a success because it was unclear whether we could get an agreement.

Finding Common Ground and Reaching Consensus

In my mind, this stability framework has three components. One, which is the foundation element, is that international law applies. It is not just the international law above the very high threshold of armed conflict, but state responsibility, sovereignty and human rights: obligations apply in cyberspace.

Peacetime Norms and States' Responsibilities. The second component is an articulation of "peacetime norms." As Ambassador David Martinon said, getting consensus on these core peacetime norms was remarkable because these norms are truly new and they are real stability measures. We hear a lot about what we can do to protect our networks or what kind of capabilities can be brought to investigating and sharing information. This is more of a long-term game and about how to create long-term international stability in cyberspace so that no one has an incentive to disrupt that stability. When people say that there are no rules in cyberspace, it is particularly important to have these norms, these rules of the road, and the fact that international law applies. David mentioned two of them: "States should take appropriate measures to protect their critical infrastructure" and "increase the level of cooperation with regard to critical national infrastructure protection." A third significant norm is that states should not attack the Computer Emergency Response Team (CERT) of another state because it would be destabilizing; and thus States should use their CERTS for defensive purposes, not offensive ones. Consistent with that is the norm of the expectation that a state will assist a victim state if malicious code is coming from within its borders. We are also promoting a fourth norm that is not in the GGE framework because it is more of a trade versus a political-military norm. It is that states should not condone or promote the theft of IP and trade secrets for the commercial gain of their countries. If you take all these norms together, they will have a real long-term stability effect.

> **"...states should not attack the Computer Emergency Response Team (CERT) of another state because it would be destabilizing."**

Confidence-Building Measures. The third component is confidence-building measures, which can be transparency measures, cooperative norms or stability measures—designed to build better understanding and confidence between countries. David mentioned that the OSCE has done a lot of work in this area. We have a foundation group of eleven measures and are building new groups; we have had a CBM workshop for the ASEAN regional forum in Singapore that we co-sponsored

with Singapore and we are taking that work forward. These are practical transparency measures such as having hot lines, codes of conduct, and cooperative measures against third party threats. All together, they lead to a more secure environment. A question that often comes up is, how do you get wider acceptance? This is our next step. We have some really good norms in this report with twenty countries versus fifteen previously, and as everyone knows, it is harder to reach consensus with more countries, but we were able to reach consensus anyway. The next GGE will probably be expanded again, and it will be still harder to get everyone up to speed, but this is an important vehicle for moving things forward.

Peacetime Norms have a Long-Term Stability Effect

The next step is to take these norms that were agreed to and give them a wider application. This is a priority for the President who talked about these issues during the press conference with president Xi of China and would like to see them reflected in all our international meetings or bilateral and multilateral discourses. In almost every meeting the President has had with one of his counterparts, there is something in the communiqué about the applicability of norms. This was the case with South Korea recently, with Pakistan, and with Japan. Our long-term strategy here is to get like-minded countries to come together during incidents so that they can act as a group against disruptors. We also want to broaden the cyber norms discussion because not every country and not every stakeholder can be a GGE member. For example, we are sponsoring in Geneva a series of UNIDIR conferences that will widen the conversation over this coming year and we have other activities as well.

Finally, there has been a lot of friction for a while between the US and China, and also between China and many other countries due to China's unchecked activity, what we call the wholesale targeting in the commercial sector and the theft of trade secrets and other information. We think that it is actually bad for China but it is certainly bad for the lifeblood of all our economies and is something that our President has said is unacceptable. The Chinese never really accepted responsibility besides saying that they did not do it. They also did not agree that it was unacceptable, but because of negotiations in advance of President Xi's visit, they agreed with the statement that they will not promote or engage in the theft of intellectual property for commercial purposes. President Xi also welcomed the GGE report. A mechanism has been set up to talk further about norms bilaterally and, for international law, another mechanism has been set up at the ministerial level to track cooperation investigations. This is a significant advance. Does that solve all our problems with China? No. It does not come close to it because there are many other issues with China. Will China abide by this agreement? We hope so, but, as the President said, we will be watching very closely. I do think it is significant that President Xi himself clearly made this commitment and at least it will set metrics of accountability that we can hold him to. In the UK, the same commitment was agreed to during President Xi's visit with Prime Minister David Cameron and it also came up during his German visit as well. So these norms have been getting wider and wider acceptance just in these past few weeks.

> **"Will China abide by this agreement? We hope so."**

This is actually pretty remarkable when you think about how long it normally takes to get agreements in international relations while we only started thinking about some of these peacetime norms four years ago. Such a quick and wide acceptance is important because it reflects the fact that these norms are of universal interest. They are generally applicable and attractive to all countries. No country wants a critical infrastructure attack; therefore it is in everyone's interest to achieve this agreement. If China or Russia were to propose a norm that there is absolute sovereignty in cyberspace and that they need to control everything in their borders, we would not agree to that because this does not have universal applicability or attraction. So, it is important to find a common ground. A lot of good work is being done, and there is more to do. This area has been transformed from a technical issue to a national security, economic and foreign policy issue and this whole movement of attention to norms, international law and confidence-building measures is illustrative of that.

> **"No country wants a critical infrastructure attack; therefore it is in everyone's interest to achieve this agreement."**

The Evolving Cyber Threat Landscape: NATO's Cyber Adaptation Priorities

Ambassador Sorin Ducaru
NATO Assistant Secretary General for Emerging Security Challenges

I will focus on the cyber defense highlights that are based on the requirements and mandate that NATO allies received at the last Summit in Wales, also involving the threat landscape. The three key axes of focus for cyber defense at the Wales summit have been on the conceptual level.

NATO's Three Axes of Focus for Cyber Defense

First, there was a recognition that cyber defense is part of NATO's core task of collective defense and a link with its raison d'être. At the same time, it was recognized that international law applies in cyber space and, although the Alliance does not have the lead for the development of international law, it was mandated to support the development of norms, confidence-building measures, and international law because this space should not be an ungoverned space and a space of confrontation. The next axis has focused attention and resources on capability development and capacity building for both NATO's own networks and national networks. The third axis concerns new ways of doing business within and across the NATO enterprise through a streamlined governance mechanism and the main streaming of cyber defense across all NATO's tasks, planning process, and exercises. Even more so, it is a new way of doing business with the outside world through close cooperation with international organizations—the European Union, the UN, the Council of Europe, OSCE, and with partner nations on a case by case basis based on mutual interest. Another initiative is to develop a distinct NATO-industry cyber partnership which recognizes that speed and information exchange are of the essence and would strengthen NATO cyber defenses.

> **"...a distinct NATO-industry cyber partnership" initiative was launched at the Summit**

Professionalization of Cyber Crime and the Cyber Aspect of Hybrid Warfare

In view of these three axes of attention and developments in the threat landscape, it is important to note one or two qualitative evaluations that are relevant. This year, the NATO Cyber Threat Assessment Cell (CTAC) has been entering an operational phase through the development of regular threat assessments based on information on cyber attacks against NATO networks, access to information from industry about the threat landscape, and also the fusion with Human Intelligence (HUMINT). There are a number of main threat developments. First, there is the professionalization and industrialization of cyber attacks and cyber crime—an aspect of "cyber crime as a service" that includes attackers or actors whose motives may be more strategic than merely theft. Analyses from public sources have recognized this cyber pirateering in a number of articles. So the potential use of cyber crime by actors such as terrorists or even state actors is one dimension. The other dimension is the use of cyber in sync with a military operation—the cyber dimension of hybrid warfare, and the concern about the potential nexus between cyber and terrorism. These are very worrying trends, which are combined with an increase in the intensity and sophistication of cyber attacks.

> **"cyber crime by actors such as terrorists or even a state actor" is now a serious concern**

Developing New Cyber Defense Capabilities, including Training, Education and Exercises

Against this background, the priorities and way ahead to the next Summit and the next phase for strengthening our cyber defenses would focus first on developing new capabilities for NATO's own networks and also national networks. We are focusing on quantitative and qualitative elements to strengthen NATO's defenses. Quantitatively, we have a centralized

protection over 53 sites across the NATO enterprise and a decision has already been made to add ten more sites. The plan is also to link this to the NATO Force Integration Units that have been developed under the readiness action plan, and to link deployable networks to the centralized protection. The qualitative element is the introduction of modern cyber analytics and the possibility of having an automated decision support system—the Cyber Defense Decision Support System (CDDSS)—in case of cyber attacks, especially during operations.

For nations, the way ahead is to develop a new generation of cyber defense capability targets. Introduced in 2013 in the NATO defense planning process, these cyber defense capability targets were referring to the "fundamentals"— each nation is to have a cyber strategy, legal framework, institutional construct, national CERTS, training and education, a supply chain, and security mechanisms. This year, the implementation of the commitments by each ally in this field will be reviewed and we are already preparing the next generation of more evolved cyber defense capability targets. After the Wales Summit, we established minimum requirements for national networks—not for all networks because the responsibility of nations to develop cyber defense is still a key element of state sovereignty. For those nations that are linked to NATO nations and upon which NATO depends for fulfilling core tasks, however, there has been a consensual process for agreeing to minimum requirements. They are not standards, but they have to be implemented.

The other level—the skills level—concerns training, education, and exercises. There is now a cyber scenario in every single NATO exercise. This is not just a cyber coalition, a cyber-focused exercise that we have had for many years already; we are developing the full operational capability of the NATO cyber range based on the offer by the Estonian defense ministry to put the Estonian cyber range at the disposal of NATO, with extra capabilities to have it fully operational, that is, to exercise at a high level of classification.

"There is now a cyber scenario in every single NATO exercise."

Partnerships as a Rapidly Evolving Trend

There are multinational smart defense projects: in one of them, the Training Education Exercise, we pull resources together from different nations and from NATO's own institutions to provide a more convergent training and education for specialists, mainly those who focus on critical infrastructure and the defense sector systems. Partnerships are the fastest evolving trend. We are looking forward to conclude with the European Union an MOU, or a technical agreement for information exchange between the NATO Computer Incident Response Center (NCIRC) and CERT EU. We have a structure of staff to staff dialogue and within the hybrid warfare context, collaboration there would be an extra element. We are also in close contact with the EU, the UN and the OSCE in developing confidence building measures and norms and, on a somewhat regular basis, we meet with those responsible in every state. At the government level, we have briefings in the cyber defense committee. We included cyber defense capacity building, for example for Ukraine, Jordan and the Republic of Moldova.

As to the development of partnerships with industry, it can bring huge value and we succeeded in doing a couple of things last year. First, we succeeded in mapping existing cyber engagements with industry in a coherent matrix. We then intensified the information exchange on a number of levels, such as actionable information through MOUs between the NATO Communication Information Agency (NCI) and those industries that benefit from big data. This would make it easier to study trends through our CTAC capability and through the invitation of industry representatives in the cyber defense committee. This would help determine the best practices from industry that could be used also by NATO for training, education, and exercises. Last year, industry participated for the first time in a cyber coalition exercise. This year, we will have another exercise with higher participation. There have been situations where industry was able to inform NATO about vulnerabilities or attacks that systems from allied nations were encountering, and the link with industry has been extremely useful in getting the right information and mitigating such attacks. We have established a portal, a single entry point for interactive virtual space between industry and NATO. Before the coming ministerial meeting in February, we will include the basis for a malware information-sharing platform.We still have a challenge in getting more engaged with industry in terms of innovation. Here, it is extremely important to be able to have access to innovation in the cyber domain but the rules of the procurement process and the rules of the competitions create obstacles. This is something that we are struggling with, and I hope that we will be able to report much more progress on this domain at a later stage.

The EU's International Cyber Policy
Priorities and Perspectives

Ms. Heli Tiirmaa-Klaar
Head of Cyber Policy Coordination, Conflict Prevention and Security Policy Directorate, EEAS

At the European External Action Service, which is the Foreign Policy branch of the EU, we are working heavily on cyber diplomacy and international cyber policy. I believe that the European Union formulated the term "cyber diplomacy" on an official document for the first time after we adopted early this year the Council Conclusions, which are the highest-level EU policy document possible. These Council Conclusions on cyber diplomacy contain several elements. First, there is a strong element of international norms and we just had very extensive discussions here about norms and how important these norms are. Second, the principle that International Law applies in cyberspace is very important for us because, as stated in the EU Cyber Security Strategy in 2013, cyberspace should not be a lawless area where the laws, norms and social responsibilities that we have offline would not apply. Third, the Council Conclusions on Cyber Diplomacy strongly emphasize human rights online. We have recently adopted guidelines for protecting human rights online and offline and this has been an important part of what the EU has been doing.

Investment in Capacity Building both within and outside Europe

We are one of the international entities that are investing heavily in capacity building outside of the developed world. This capacity building topic has come up already several times today and everyone understands how important it is. It is important internally here in Europe in our advanced economies, and it is even more important that minimum capacities be set up outside in third countries because, as we have recently discussed with them, we now have a few global agreements on norms and peacetime activities that all countries have agreed to. We really need to make sure that there are entities in third countries that are able to uphold these agreements and right now, as far as we know, out of 54 African countries only about 15 of them have minimum cybercrime legislation. This might not seem important in this small defense-oriented audience, but those who are dealing with cyber issues know that you must have somebody to contact if a cyber attack is affecting you and there are too many of those lawless territories and lawless spaces in the world.

> **"...out of 54 African countries only about 15 have minimum cybercrime legislation."**

> **"...there is another category of countries where the criminals are under the direct protection of state actors"**

Of course, there is another category of countries where the criminals are under the direct protection of state actors—this is another issue, and we also have to deal with the safe havens. So, raising these capacities externally and also internally is an important part of the EU work.

Harmonization and Implementation of EU legislations on Cybercrime

Within the European Union, we have recently made a significant effort to step up our work on addressing cyber crime. The European Union Cybercrime Center is up and running and acts as a focal point for all global partners. It is next to Europol in The Hague and is one of our success stories that show how well we have been able to deal with the cybercrime portfolio. The legislation of all 28 countries has been harmonized and several directives have been adopted to make sure that all countries have the minimum legislation on cybercrime. It significantly deters criminal actors from hitting the EU countries, but of course it might also push these criminal actors to move outside of the EU countries and then we would have to deal with the same issues anyway.

On the network and information security, which is the technical side of cybersecurity, there is now a new piece of legislation on the table since the strategy was adopted in 2013. It is called the Network and Information Security Directive. Steve Purser will talk more about the internal work that the EU is doing on capacity building in this area. The good news is that the current Luxembourg presidency is strongly driven to adopt the directive by the end of this year and we really hope it will happen since it has been dragging on for two years. The adoption of this directive will provide the first very significant piece of cyber law that imposes on national governments minimum IT risk standards and minimum responsibilities to set up computer emergency response teams and have a cyber policy and cyber strategy in the large EU trading block. It will also have a normative effect on other countries around the European Union and, hopefully, will significantly enhance the resilience of the EU-owned infrastructure companies and public administration. Once this directive is adopted, EU member states will have two years to implement it in their national laws. However, since some member states are already more advanced and have made similar efforts in parallel, they will not need to implement the EU directive which only sets a minimum standard there. Finally, we hope that the normative dimension that the EU is imposing on this new cyber domain will equally have a more commercial and economic effect.

The directive "will provide the first significant piece of cyber law that imposes on national governments minimum IT risk standards and minimum responsibilities"

EU Global Efforts to Develop Cyber Confidence-Building Measures

The EU is also supporting global efforts to develop cyber confidence-building measures. There are cyber confidence-building workshops in the context of the ASEAN regional forum. In the Euro-Atlantic security community, which includes European countries, the United States, and Canada, state agreements on confidence-building measures in an OSCE style of discussions have become our traditional way of doing things. It is not necessarily the same in Asia where countries would not have the same culture of agreements on security issues because Asian partners may be more pragmatic and there is more sensitivity between countries. So, it will be an interesting task and a challenge to see whether we can help the Asian countries to come to some agreements between themselves on confidence-building measures and cyber norms. In March 2016, the EU will co-host a seminar with Malaysia, which is part of a series of seminars that have taken place in the US, Singapore and several other countries. These norms and confidence-building measures are key and we are supporting the efforts of all our member states concerning the UN GGE (Group of Government Experts) process. Five EU member states are always part of this process and help raise the awareness of the other EU member states. Our Council working groups have had internal discussions recently on cyber norms and international security and our twenty-eight EU countries are very supportive of this process.

"The EU also supports global efforts to develop cyber confidence-building measures."

EU/NATO Cyber Cooperation

Since today's audience is more defense-oriented, I will say a few words about EU/NATO cooperation. For several years now, we have had a very structured and ongoing dialogue with NATO. These EU and NATO parts of the defense capability development should be complementary and I believe they are. In defense terms, the EU has been concentrating on the Common Security and Defense Policy (CSDP) missions and operations because this is our defense posture; we do not have the collective defense posture that NATO has. Nevertheless, we have the European Defense Agency capability development program and cyber is now a part of it. All our member states are doing long-term capability development within the European Defense Agency. Quite importantly, we are also trying to set up an information sharing agreement between the NCIRC (NATO Computer Incident Response Capability) and CERT-EU, which are the incident response entities of both organizations, and we hope to be successful at it. Finally, we have an excellent staff that is able to handle informal contacts and stay away from political discussions. So there is definitely progress on the EU/NATO front. This morning, I was very happy to see some good progress in our EU's hybrid threat strategy in which NATO has a very important part and we are hoping to establish our EU CSDP-oriented large hybrid threat strategy by early 2016. This will also hopefully serve as another mechanism for more cooperation with NATO.

Governance Issues in Cyber Security

Dr. Steve Purser
Head of Core Operation Department,
ENISA (European Union Agency for Network and Information Security)

What is ENISA?

Enisa is the European agency for cybersecurity—we are a regulatory agency and we describe ourselves as a center of competence. Although that may sound very pompous, we are not in an ivory tower. In fact, we do all our work together with and through our stakeholder communities. So our philosophy in approaching cybersecurity is that the expertise is really outside the agency and we try to leverage the member states' expertise to bring results for Europe. That approach has two advantages: it brings scalability because the agency is rather small—my team is only fifty people, and it also brings buy-in because working together with communities brings a sense of ownership that carries on long after our projects are finished. For those who know Eurospeak, we are a "pillar one organization," which means that we are based on the internal market law. You will notice that the vocabulary I use in this presentation is very different from the vocabulary that my colleagues have been using here, which is normal because we are internal-market-oriented. This is actually significant because we believe at ENISA that bringing communities together is at least as important, if not more important, than bringing member states together. When I go to cybersecurity conferences, I am interested in listening to the kinds of dialogues that go on. They are very different and, although I have been in this field for twenty years, I sometimes have difficulties following. So we need to put a lot of effort into aligning the way we speak, the kind of things we speak about, and making sure that the information does flow between the different communities that deal with cybersecurity.

> **"At ENISA, we believe that bringing communities together is at least as important ... as bringing member states together.**

Bringing Consistency across Communities and across Countries

This brings me onto the subject of mandates. In the EU, mandates in cybersecurity are problematic because they have been around for a long time but cybersecurity is a fast moving subject. We are not at all in the same space as we were ten years ago, for instance when ENISA was created. So from our perspective, we see a lot of redundancy and overlap while synergies are not being exploited; it is a major challenge for the EU to bring the right people to address a problem at the right time. And, of course, the bad guys do not need to respect mandates—they just do what they want. So this is part of the goal of becoming more dynamic and more flexible in the future. To a certain extent, this comment is also valid on the international scene. There are many actors—ITU, OECD, the UN, the EC, the IGF etc.—and sometimes I feel that we risk contradicting each other, or that some people will try to take the lead without having a clear vision of the direction we need to follow. Unfortunately I cannot offer a solution for this but I can at least point out that ENISA sees this as being part of the problem. And a major problem we have in cybersecurity is to achieve consistency across communities and across countries, which leads me to ask, What is cybersecurity anyway? It is quite interesting that in this room, we are discussing things like cyber defense, cyber warfare, maybe cyber intelligence, cyber sabotage, whereas ENISA looks at things much more from an economic perspective. All these things are valuable but getting the language right, understanding exactly what we are, in what forum, and what our goals are is very important.

> **"ENISA looks at cyber security much more from an economic perspective."**

How Can ENISA Help Concretely?

What can we offer to this debate keeping in mind that we are a UN institution with an EU mandate and that we are only here to support institutions such as the External Action Service, the Commission etc.? Perhaps I can bring to your attention some key issues that we have noticed and give you our perspective on them in the hope that they will help you conduct a broader dialogue in the global environment.

'Actionable information' depends on understanding what 'actionable' means and what information is needed to conduct the action.

Information Exchange. At the conferences I attend, I often hear that we need to exchange more information. I totally disagree with this: we do not need to exchange more information. We actually need to exchange less information but the information we exchange needs to be targeted to solving the problem. At least in the communities I have been attending, the big problem is to define the chain of action between the information and what we need to do to have an impact. Much of the time, we do not even really understand what kind of information is useful and what is not, and we must be very careful about how we talk about information exchange. It is nice to hear the words "Actionable information" as long as we understand what actionable means and what information is needed to conduct the action. So information action impact is really important.

Critical Information Infrastructure. We talked about critical information infrastructure. Half of their budget is in this area. My background in the banking community has taught me that infrastructure can be secure only if the services that are run on top of it are also secure. Of course, we need secure information and infrastructure, but we also need to remember in that dialogue that we must go one step further than infrastructure. Ironically enough, when I was in the financial sector, our key assumption was that the infrastructure was not secure and we designed all our applications to put security on top. So it is a small distinction but sometimes it is worth bearing in mind. I will also point out that, at least in Europe, critical information infrastructure is not well defined. Different countries define it in different ways and according to different methods. Some countries use an asset-based approach, some use the procedural-based approach and some use a combination of the two. Trying to put the picture together is very complex, which explains why it takes us a long time to move forward in these discussions. In addition, some infrastructure elements are not national if you think of deep-sea cables etc., which are international problems.

"In defining what is critical infrastructure, "some countries use an asset-based approach, some use the procedural-based approach and some use a combination of the two."

It is also intriguing to see perceptions in this area. At ENISA, we implemented the Article 13A telecom regulation that makes it obligatory for telecommunication companies to report significant incidents. At first, people thought that this was horrific, it could not be done, it would be too expensive, etc. I am happy to say that, four years down the line, it is working very smoothly, it is economically viable and the data has been tremendously interesting. I use it a conferences with professionals to surprise them because almost everybody gets it wrong. The question I ask security professionals is, What is the biggest risk affecting your networks? It is not cyber attacks or malware or anything similar but 50% of the time, it is badly configured software or poorly written software. So, I am not saying that cybersecurity is not important—it certainly is—but it only accounts for about 10% of the problems that we see at the moment.

I will make two more remarks on critical information infrastructure. Of course ENISA facilitates the pan-European exercises. They have come a long way: five years ago, we had nothing to test, there were no procedures at cross-border level. Today, we have quite a sophisticated set of standard operating procedures between member states, we use these in an operational environment during the test, and people play from behind their desk using real machines and real scenarios. This is a great way of feeding experience into future policy-making.

- *CERTs are our first line of defense.* ENISA has helped set up national governmental CERTs that plug into the decision-making hierarchy and therefore can do things that other CERTs cannot. We moved on after that because we found that the problem with CERTs, at least within Europe, was their different sizes. The U.K. CERT has about 70

people whereas the smallest member states may have only five people. Getting these organizations to talk to each other in a sensible way was difficult. Hence we launched the idea of baseline services, in which you define a service level agreement (SLA) and this worked very well. However, we run the risk of overloading CERTs because we are asking them to do everything, police reports, statistics, etc. when they are not really there for that. They are a front line defense mechanism and we might want to think of complementary organizations to do some of the things we are asking CERTS to do.

CERTs vary greatly in size: the UK's has approximately 70 people while the smallest member states may have only five.

- *Aligning Cybersecurity with EU Economic and Industrial Policies.* We strongly believe that cybersecurity should be aligned with EU economic and industrial policies. After discussing with McKinsey recently, we identified a possible value creation of 640 billion euros, which is a huge amount, if we use the cybersecurity market correctly. We are in a supply push market where the suppliers come up with things and people buy them, at least in Europe, whereas we could get sectors to come together, agree on common requirements, and drive the market. ENISA will certainly look into this possibility with its partners to try to make sure that this happens.

With McKinsey, we have identified a potential to create value of 640 billion euros if we use the cybersecurity market correctly.

Collaboration. My last remark will concern collaboration. What has ENISA learned about collaboration? There is a real need for effective collaboration and we get hundreds of collaboration requests, but they rarely succeed because it is very difficult to collaborate effectively. What we think collaboration requires are very favorable conditions, clear goals and impacts, enormous amounts of perseverance and good will, and a need to drop the leadership attitude. We cannot all lead in everything. ENISA does not want to be a leader; we want to be a good supporter to make sure that we can carry plans all the way through to fruition.

Quelles Priorités pour la Cyberdéfense ?

Sénateur Jean-Marie Bockel
Sénat français, Membre de la commission des affaires étrangères, de la défense et des forces armées
Ancien Sécretaire d'Etat

Je voudrais faire trois remarques sur cette menace cyber grandissante—la première sur la situation de la France aujourd'hui; la deuxième sur l'enjeu industriel sur lequel nous sommes en train de nous mobiliser; et la troisième sur les coopérations internationales avec leurs progrès et leurs difficultés.

La Situation de la France Aujourd'hui

Lorsque j'ai fait un rapport sur la cyberdéfense au Sénat il y a trois ans, c'était à un moment où la France était à la croisée des chemins. Nous avions pris conscience d'un retard important face à un risque qui, déjà à l'époque, montait en puissance. Comme on sait bien le faire en France, nous avions mis en place quelques outils comme l'ANSSI, notre agence nationale des systèmes d'information ou notre état-major cyber, mais ces outils étaient cruellement dépourvus de moyens. La prise de conscience du monde politique, administratif, économique, et même dans une certaine mesure militaire, était encore très insuffisante. Je dis cela, non pas pour mettre en valeur mon travail qui avait été un travail collectif, mais parce qu'il y a eu un tournant en France dans un contexte budgétaire extrêmement tendu où nous étions plutôt dans l'idée de couper des budgets que de les augmenter. Là, les efforts ont été faits, tant au niveau militaire, civil, interministériel, qu'au niveau de l'organisation. Nous avons fait des efforts de recherche développement considérables avec la Direction générale de l'armement qui ont porté leurs fruits. Au fond, le seul domaine à l'époque sur lequel la France n'avait pas un retard important était celui des capacités offensives où nous avons toujours eu un bon niveau. Nous sommes en effet un des rares pays occidentaux ayant un outil de défense qui nous permet d'être en capacité aujourd'hui de faire la guerre. Les déclarations faites il y a quelques semaines par le Premier Ministre, Manuel Valls, que « la France est prête » en matière de cybersécurité correspondent à une nouvelle donne. Le seul point de désaccord que j'ai avec ces déclarations, c'est que nous ne sommes jamais prêts par définition puisqu'il s'agit d'un domaine qui évolue tout le temps.

Nous sommes un des rares pays occidentaux ayant un outil de défense qui nous permet d'être en capacité aujourd'hui de faire la guerre.

Aujourd'hui, nous avons renforcé la capacité matérielle de l'ANSSI en nombre de personnes et aussi grâce à des lois qui ont permis d'améliorer cette capacité au niveau des règles du jeu. Je vous donne un exemple: nous avons depuis peu une obligation de déclaration d'incident pour les opérateurs d'importance vitale. Etonnamment, cette obligation n'existait pas encore en France et c'est un point important parce qu'il est psychologique. Pendant longtemps, au niveau des entreprises ou de certaines administrations, la règle était de ne pas dire ou de dire le plus tard possible qu'on était attaqué parce que le dire était un aveu de faiblesse. Pour les entreprises c'était éventuellement perdre des marchés, notamment dans le domaine de la défense. Le bon état d'esprit, au contraire, est de dire, « nous sommes attaqués parce que nous avons de la valeur». Reconnaître que l'on est attaqué, c'est un signe de force parce que cela veut dire que, plus tôt nous nous faisons aider—et les outils pour nous aider existent aujourd'hui—plus nous serons fiables et crédibles. Ce qui compte n'est pas de ne pas être attaqué, c'est notre capacité de résilience, et ces obligations sont en train, lentement mais sûrement, de changer la donne.

nous avons depuis peu une obligation de déclaration d'incident pour les opérateurs d'importance vitale.

Au niveau militaire, nous avons également fait des progrès considérables avec les moyens humains qui ont été mis en œuvre, et sur ces questions, les coopérations et partenariats avec un certain nombre de grands alliés, les Etats-Unis, la Grande Bretagne, et dans une moindre mesure l'Allemagne, aujourd'hui se sont renforcés. Je reviendrai sur les partenariats dans un instant.

J'évoquais tout à l'heure la recherche développement. Tous les pays ont des domaines d'excellence, et même si nous sommes petits par rapport aux Etats-Unis par exemple, nous sommes reconnus comme étant en pointe dans certains domaines comme la cryptologie. Dans d'autres domaines également, nous avons développé avec notre Direction générale de l'armement un centre de recherche près de Rennes qui existe depuis longtemps mais qui s'est renforcé sur ces sujets et est assez impressionnant. Nous avons donc fait des progrès considérables. Il est vrai qu'aujourd'hui, à un moment où la France est engagée sur le plan militaire et sécuritaire dans bien des continents, nous sommes plus que par le passé une cible, et notre outil cyber doit être à l'échelle de notre outil militaire et sécuritaire.

L'enjeu Industriel

Ensuite, je dirai un mot sur l'enjeu industriel. En France nous avons à la fois un atout et une difficulté. L'atout, c'est que nous avons un certain nombre de très grandes entreprises comme Thales qui sont connues mondialement dans le domaine de la défense et qui sont également présentes dans le domaine aéronautique et industriel. Elles sont engagées depuis le début dans les développements cyber. Ces entreprises, et de manière générale notre ensemble industriel, ont besoin en matière de créativité, de souplesse et d'inventivité, d'un réseau de petites entreprises qui existent en France. Mais dans le domaine cyber, la petite entreprise en France aujourd'hui a trop souvent vocation soit à disparaître au bout d'un certain temps, soit à se faire racheter. Se faire racheter est très bien, c'est la preuve du succès, mais il faut quand même qu'un certain nombre de ces petites entreprises puissent durer, en tout cas ne pas échouer trop vite par rapport au produit qu'elles développent. Nous travaillons actuellement dans notre pays à faciliter le soutien, ou plus exactement les conditions de survie de ces petites entreprises à travers des réseaux et aussi à travers la prise en compte de cette dimension cyber dans toutes les démarches de soutien à l'industrie qui peuvent exister. Il faut simplement que ces soutiens soient à bon escient et produisent les résultats espérés; dans le domaine de la politique industrielle, nous sommes encore loin du compte mais nous avons fait quelques progrès.

dans le domaine cyber, la petite entreprise en France aujourd'hui a trop souvent vocation soit à disparaître au bout d'un certain temps soit à se faire racheter.

Les Coopérations Internationales

Ma dernière remarque concerne nos partenariats. Je vois ici la représentante de l'Union Européenne et des personnalités de l'OTAN. Je suis moi-même, en tant que parlementaire français, rapporteur général de la Commission de l'économie et de la sécurité à l'Assemblée parlementaire de l'OTAN. Lorsque je préparais mon rapport sur la cyberdéfense il y a trois ans, j'étais allé à Bruxelles à l'Union Européenne et à l'OTAN et à l'époque j'avais été sidéré par la faiblesse de ces grandes entités en matière de cybersécurité. J'avais rencontré les gens de la direction concernée à l'Union Européenne qui avaient l'esquisse d'une stratégie tout en ayant le sentiment quand même d'avoir quelques maillons forts et beaucoup de maillons faibles. Avoir une politique Européenne lorsque nombre de pays n'ont pas encore pris conscience de l'importance de ce sujet est très difficile. Ce n'est pas forcément d'ailleurs un problème de grand pays et de petit pays. L'Estonie est un pays en pointe puisqu'ils ont peut-être été les premiers à être attaqués en 2007 par leur grand voisin Russe et cela leur a donné un coup de fouet. Il faut dire que depuis trois ou quatre ans, l'Union Européenne a fait des progrès très importants pour déterminer une stratégie et travailler à une règle du jeu. Je terminerai mon propos sur la règle du jeu d'une manière générale.

Avoir une politique Européenne lorsque nombre de pays n'ont pas encore pris conscience de l'importance de ce sujet est très difficile.

On peut imaginer que la vocation première de l'Union Européenne n'est pas encore aujourd'hui les enjeux de défense, même si je fais partie de ceux qui espèrent que cela viendra rapidement, mais c'est quand même un peu la vocation première de l'OTAN. A l'époque où je me trouvais à Bruxelles, l'ordinateur personnel du Secrétaire Général de l'OTAN venait d'être piraté, on peinait à mettre en place une stratégie et on avait le sentiment que l'OTAN en était au tout début. Aujourd'hui, tout a considérablement progressé et nous entrons peu à peu dans un monde où les partenariats entre les pays très engagés sur ces questions et certaines organisations comme l'Union Européenne et l'OTAN peuvent se renforcer

avec tout de même, sur une question qui est un enjeu de souveraineté d'abord, le risque du maillon faible. Il est toujours préférable et plus simple de traiter avec un interlocuteur. On peut choisir de ce sur quoi on coopère et avec qui on le fait. Dès qu'on est plusieurs, c'est plus compliqué mais nécessaire en matière d'enjeux sécuritaires.

Enfin j'ai évoqué surtout la dimension sécuritaire parce que le risque d'une cyber guerre, en tout cas d'un conflit où la dimension cyber sera très importante et pourra déstabiliser un pays, même un grand pays, à travers ses services publics, ses transports, son système de santé, et son économie, reste une question majeure. Mais sans aller jusqu'au conflit, il y a aussi évidemment le développement du cybercrime. Nous venons d'entendre citer des chiffres des pertes dues à l'espionnage massif et nous restons donc sur un enjeu économique sur lequel, là aussi, des partenariats sont devenus nécessaires. Plus que jamais, nous avons besoin d'une règle du jeu au niveau mondial. Il y a déjà des conventions internationales mais pour le moment elles sont signées par très peu d'états et ne sont pas respectées. Quand je dis cela, je ne suis pas naïf. Une règle du jeu sous l'égide des Nations Unies n'empêchera pas certains pays de considérer que, lorsque l'intérêt supérieur de leur nation est en jeu, il n'est pas nécessaire de respecter les règles. Mais dans ce monde multilatéral, les règles du jeu vont monter en puissance et cela a déjà commencé sur l'internet. Lorsque ces règles existeront, chaque fois qu'une règle ne sera pas respectée, cela se saura. Et à partir du moment où il y aura cette prise de conscience, même dans des pays non démocratiques ou pas encore démocratiques—je pense à la Chine—les dirigeants sauront qu'ils ne peuvent pas faire n'importe quoi. Ne pas respecter la règle commune que tout le monde appelle de ses vœux par ailleurs, c'est prendre un risque politique majeur. Cela ne veut pas dire que cela n'arrivera pas mais il faudra y réfléchir à deux fois et ce sera un progrès.

Ne pas respecter la règle commune que tout le monde appelle de ses vœux par ailleurs, c'est prendre un risque politique majeur.

Which Priorities for Cyber Defense?

Senator Jean-Marie Bockel[1]
French Senate, Former Secretary of State for Defense

I would like to make three comments on the growing cyber threat—first, on the current position of France; second, on the industrial challenge we are currently addressing; and third, on international cooperation with its advances and challenges.

The Current Position of France

When I wrote a report on cyber defense for the Senate three years ago, France was at a crossroads. We were aware that we significantly lagged behind in the fight against what was already at that time a growing threat. We had put in place some tools like ANSSI, our national agency for information systems or our cyber military staff, but these tools severely lacked resources. There was still little awareness of the threat among political, administrative, economic, and even—to a certain extent—military spheres. I am saying this not to emphasize the significance of my work, which was a collective effort, but rather because there was a turning point in France in a context of budgetary restraint where the idea was to cut rather than increase budgets. Efforts were made at the military, civil, inter-ministerial levels, and at the organizational level as well. The substantial efforts in research and development that we made with the Defense Procurement Agency (DGA) proved to be successful. In fact, the only sector where France was not significantly behind was in our offensive capacities where we always had a good level. We are indeed among the few Western countries with a military structure that allows us today to go to war. The declarations made a few weeks ago by our Prime Minister, Manuel, Valls, stating that "France is ready" in matters of cybersecurity reflect this new situation. The only point of contention I may have with such declarations is that by definition we could never be ready since it is an area in constant evolution.

> **France is "among the few Western countries with a military structure that allows us today to go to war."**

Today, we have reinforced the physical capacity of ANSSI in the number of people employed and through laws that improved this capacity in terms of ground rules. For example, an obligation to report incidents was recently imposed on critical infrastructure operators. Remarkably, such an obligation did not yet exist in France, and this is an important point because it is psychological. For a long time, the rule for private companies or some public entities was to avoid disclosing, or disclose as late as possible, that an attack had occurred, because a disclosure was perceived as a sign of weakness. For private companies, it potentially meant losing markets, especially in the defense sector. On the contrary, the proper state of mind is to say "we are attacked because we are valuable." Acknowledging that you are attacked is a sign of strength because the sooner you seek help—and the tools to help do exist now—the more you are reliable and trustworthy. What matters is our capacity of resilience, and these reporting obligations are, slowly but surely, making a difference.

> **"an obligation to report incidents was recently imposed on critical infrastructure operators"**

At the military level, we have made some significant improvements with the human resources that have been implemented. Cooperation and partnerships with a number of our great allies, the United States, the United Kingdom, and to a certain extent Germany are now reinforced. I will come back on these partnerships in a moment. Earlier, I mentioned research and development. All countries have areas of excellence, and even if we are smaller compared to the United States for instance, we are recognized as leaders in some areas such as cryptology. In other areas, we have developed a research facility near Rennes with our Defense Procurement Agency (DGA). This research facility was established long ago, but its new focus on these issues is quite impressive. Hence, we have made some significant progress. It is true that, at a time when France is involved at both the military and security levels on different continents, we are more of a target than in the past, and our cyber tools must balance our military and security tools.

1 Translation by Mr. Antoun Meroueh, Institut d'Etudes Politiques de Paris.

The Industrial Challenge

Next, I will say a word about the industrial challenge. In France, we have both assets and drawbacks. Our asset is that we have a number of very large companies, like Thales, which are internationally renowned in the defense sector and also operate in the aeronautical and industrial sectors. They have been involved in cyber developments from the start. These companies, and our industrial complex in general, need a network of small French companies for creativity, flexibility and ingenuity. In the cyber domain, however, the fate of a small French company is often either to disappear after a period of time or to be taken over. The latter is a good thing, it is a proof of success, but a number of these small companies need to last long enough, or at least cannot fail too quickly for the purpose of the product they are developing. We are currently working to facilitate the support, or more precisely the survival, of these small companies through networks and by taking into consideration this cyber element in all possible measures of support to the industry. These supports must be used properly and produce the desired outcomes; in matters of industrial policies we still have a long way to go, but we have made progress.

> **"We are currently working to facilitate the support, or more precisely the survival, of small cyber companies"**

International Cooperation

At this workshop, we have representatives of the European Union and officials from NATO. I am myself, as a French Senator, the reporter of the Economics and Security Committee of the NATO Parliamentary Assembly. When I was working on my cyber defense report three years ago, I went to the EU and NATO headquarters in Brussels and, at that time I had been stunned by the weaknesses in matters of cybersecurity. I met with people from the concerned department at the European Union; although they had the beginnings of a strategy, they felt it had few strong links and many weak links. Making a EU policy while a number of countries have not yet realized the importance of the issue is very difficult. Furthermore, it is not necessarily a matter of large and small countries. Estonia is a leading country, because they were perhaps the first to be attacked in 2007 by their large Russian neighbor, and that gave them a boost. It should be noted that for the past three or four years, the European Union has made some significant progress in defining a strategy and setting out some ground rules. I will conclude my remarks on the ground rules in a broader sense. You may think that defense issues are not yet the primary purpose of the European Union—although I am among those who are hoping that they will soon be—but it is still NATO's primary vocation. At the time when I was in Brussels, the personal computer of the Secretary General had just been hacked, we were struggling to implement a strategy, and we had the feeling that NATO efforts were just at the beginning. Today, everything has significantly improved. Step by step, we are entering into a world where partnerships between countries that are highly committed to this issue and organizations like the EU and NATO can be strengthened, although there is always the risk of the weak link on an issue that is a sovereign matter. It is always preferable and easier to deal with one partner. We can choose on what and with whom we cooperate. When several partners are involved, it is more complicated but necessary for security issues.

Finally, I have mainly discussed the security dimension because of the risk that a cyber war—or at least a conflict where the cyber dimension would be very important—could unsettle even a large country through its public services, its transportation network, its social system, or its economy. But without going as far as a conflict, the growth of cybercrime is obviously a concern. In earlier presentations at this workshop, we heard figures concerning losses due to massive espionage, and we are still facing an economic challenge where again, partnerships have become necessary. More than ever, we need ground rules at the international level. There have already been some international agreements but, as of now, only a few countries have signed them, and they are not respected. In saying this, I am not being naive. Ground rules set up under the umbrella of the United Nations will not prevent some countries to consider that, when the highest interests of their nation are at stake, it is not necessary to follow the rules. In this multilateral world though, ground rules will be established and this has already started for the internet. Once these rules exist, every time a rule is not respected, it will be known. And as soon as countries will become aware of this, even countries that are undemocratic or not yet democratic—I am thinking about China—their leaders will know that they cannot act as they please. It would be taking a serious political risk not to respect a common rule that the world calls all countries to observe. It does not mean that rules will not be broken, but you might think twice about doing it, and that would be progress.

Cybersecurity and Collaboration Imperatives: Towards Increased Complexity?

Mr. Luigi Piantadosi
Director International Business Development, Lockheed Martin

In the next ten minutes, about fifteen thousand people will be victims of a cybercrime—18 cybercrimes per second—and roughly seven thousand identities will be stolen. This is in a ten-minute period only. We all know that not a day goes by without a cyber front-page story in the international press, or some serious government or corporate network security breach being exposed. Recently, both the New York Stock Exchange and United Airlines suspended operations for several hours due to mysterious computing problems, while the Wall Street Journal's website temporarily went down. Last week, the press reported that the British giant TalkTalk Telecom Group suffered a cyber attack, apparently exposing thousands of personal data and twenty-one thousand bank accounts. The Vodafone Group was also attacked just after Talk Talk. From 2013 to 2014, cyber attacks have gone up by 48%, representing 40 million cyber attacks and roughly 100,000 per day. Clearly, we can no longer accept that this situation is someone else's problem.

> **"When the British giant TalkTalk Telecom Group suffered a cyber attack, it exposed thousands of personal data and 21,000 bank accounts."**

Large Corporations are at the Frontline of the Cyber Battlefield

To make matters worse, many government or industry networks may already be compromised without the knowledge of the intellectual property administrators. For our cyber experts like ANSSI, the French cyber agency that operates in this beautiful and historical Invalides monument, it is old news, but for many in the public or even in large corporate and government offices, it continues to be an inexplicable and misunderstood phenomenon. The hard truth is that, in the meantime, the sophistication of our foes is growing exponentially. Large corporations like Lockheed Martin, with operations in over seventy countries, are on the front line of the cyber battlefield. High-value corporate environments such as the aerospace and defense industry are attractive attack destinations. These aggressive attacks try to breach their systems, dissimulate the objective, retrieve and extract valuable corporate IP, and persist in their theft by retaining the ability to monitor and access at will. You can easily figure out the scale of our challenge at Lockheed Martin, a high-tech defense industry enterprise with 122,000 employees and 30 million emails being exchanged every day. It is one of the great paradoxes of our time, I believe, that the very state-of-the-art information technology that empowers us to do a lot of good can also be used to undermine us and inflict great harm.

This threat makes no distinction between military and civil environments or between the public and private sector. All information and communication systems, no matter where or what they are designed for, are a natural conduit for aggression. Aggressors range from the young geek who wants to make a name for himself in the dark market—as was the case in the Talk Talk attack in which two teenagers were arrested in the UK—to sophisticated criminals ready to hit at the very heart of our systems, either to test our critical infrastructures or to steal the intellectual property and the knowledge base of all our society. Industry does not claim to have the solution to the problem, never did and does not intend to, but we are security sensitive, not only by choice but also by necessity, and we do understand how to deal with complex problems. We supply the departments of Defense and Homeland Security with the most advanced systems, like the F-35 for instance, and have a robust understanding of the customer community. We are a top provider of IT solutions around the world and we have critical defense IP. It is therefore no surprise that we are targeted by sophisticated attacks, which require a high-end capability to counter. That is

> **"Industry does not claim to have the solution to the problem... but we are security sensitive by both choice and necessity."**

why, in the last decade, we have invested heavily to establish our CERT teams and we have set up four state-of-the art security intelligence centers that are internationally located. We know how to produce intelligence that can mitigate the risk and anticipate the next move. We have acquired over time an in-depth understanding of the intricacies of this environment and, more importantly, of the diversity and complexity of our customers' needs.

Public and Private Partnerships, National and International, will Play a Key Role in Acting against Cyber Threats

What lessons have we learned? No governments or corporate entities, whether they are the custodians of a major infrastructure or a commercial IP, can ignore the clear present danger of cyber attacks. Our enemies are demonstrating a keen ability to counter in real time and we must acquire the awareness, the knowledge, the understanding, to escalate our defenses in order to adapt to environments and develop solutions that can meet the challenge. How can we do that? How can we pull together an understanding of the problem, how do we identify the approach to resolve it? Can we plan for continuity during deployment, select the technologies and the tool sets that are required? And how do we execute closely with the user and transfer the knowledge to enable a successful implementation?

For me, the answer is partnerships. As in nature and in military strategy, alliances play a key role in acting against a common enemy.

- First, this has to be a common and joint mission. The private sector owns and controls many of the critical systems that need to be protected, which means that the public sector cannot deal with this alone. Likewise, the private sector cannot do this alone either because it is governments that often have the latest information and intelligence on new threats.

- Second, we have to focus on our unique strengths. While the private sector has crucial insights, expertise and resources, the public sector is uniquely positioned to investigate, to arrest and to prosecute cybercriminals. We need to be smart, focus on what each sector does best, and then do it together.

- Third, we need to constantly be on alert. The first computer viruses penetrated PCs in the early 80s and we have been in a cyber arms race ever since. We design new defenses and then, the hackers and criminals design new ways to penetrate them. Whether it is phishing or botnets, spyware or malware, these attacks are getting more and more sophisticated everyday. So we have got to be just as fast, as flexible and agile and constantly evolve our defense. However agility and evolution do not work if there is just a single team, no matter how extensive and experienced it is. This is why the policy discussion has to be debated internationally in order to arrive at possible models for interaction between communities of interest, between the public and private ones. To be fair, we already have collaborations in place. The first one that comes to my mind is our collaboration with NATO—the NATO Industry Cyber Partnership. NATO is on the front line of all these challenges and, at Lockheed Martin, we are cooperating with them. In many countries, Lockheed Martin is working with governments and with companies on the mechanics of a hub and node model to enable better protection of the national IT infrastructure and, with it, the economic environment in the country.

> **"...policy discussion must be debated internationally to arrive at models for interaction between communities of interest, between the public and private ones."**

Removing Barriers to Effective Cooperation

This brings me to my final point. There are unfortunately barriers to effective cooperation. These barriers can be legal, pragmatic, cultural, or competitive and can lead to refraining from extensive collaboration. I will give you a few examples of obstacles to cooperation: trust and control of incident response; reluctance to disclose information; restrictions on cross-border data transfer between public and private sectors that impede companies' swift response to incidents. There is

also a significant concern that information sharing is often a one-way relationship. Governments accept information that companies share but are constrained by secrecy obligations regarding national security. Although time does not allow me to expand on these issues, we need to resist the temptation to address the problem through regulatory frameworks. This will not work in an environment that thrives on technology advantage, low barriers to entry and high rates of change. We need pragmatic and workable solutions; we need to ensure that there is another way to awareness and understanding of the threat environment, and an appreciation for those firms that actively pursue a tight information assurance agenda; we need to make a business case for public and private sector cooperation; we need to think strategically on how to create and implement corporate governance and communication and response structures to manage cyber risks.

In conclusion, there is no silver bullet to address the diverse and persistent nature of cyber threats, but understanding the opportunities to engage in meaningful partnership efforts to prevent and respond to cyber attacks would be a very good start. While cyber represents the asymmetry of todays' battlefield, we need to embark symmetrically on a common journey, emblematic of the problems that our countries, our organizations, public and private, need to make to ensure we retain our lead and protect the success we have.

Public-Private Partnerships for Cyber Security
A View from Industry

Mr. Anton Shingarev
Chief of Staff, Kaspersky Lab

Kaspersky Lab, my company, is an international cybersecurity company with its headquarters in Moscow. We focus on endpoint security, intelligence services such as security audits, penetration tests and data reports, and our third area of expertise is industrial security. I would like to talk about our view on public-private partnership from the point of view of a private company.

> **"Without data from the cyber security industry, it is impossible for governments to build a resilient society."**

First, I would agree with my colleague from ANSSI that it is absolutely impossible to protect governments and enterprises without this partnership because the cyber world is changing very fast, cyber threats are escalating, and cybersecurity companies, which are private companies, are obviously much quicker to change than governments. We see what is going on, we see the cybersecurity landscape and without data from us, it is impossible for governments to build a state resilient society. For us, it is equally essential to build this partnership because we do not have a mandate to catch criminals, only law enforcement can do that. We do not have the power to regulate either, so we need to cooperate with states. However, we see three main problems in achieving effective cooperation.

Kaspersky's Views on the Problems of Public-Private Partnerships

First, there is a lack of legislation. I mainly speak about cyber investigations, where this lack of legislation is a huge problem for us. As a result almost all of what we do at this stage is in a grey zone and this sometimes leads to peculiar situations. For example, we actually investigated a cyber case in Europe in which European law enforcement agencies had to send information to our company and then asked us to share this information with their partners in another organization. This is because it is sometimes easier to do it this way. Concerning digital single market discussions, we are looking forward to the future announcement of a public-private partnership regulation for Europe that will hopefully change the situation. Secondly there are no working mechanisms to share data, especially about cyber incidents. Again, I am speaking about malware investigations. Steve Purser, our colleague from ENISA, said that we do not need to share a large number of data. I absolutely agree. We need pinpoint mechanisms to share data concerning investigations of the threats and incidents that we see.

Finally, a loss of trust creates big problems for private partnerships. After the Snowden allegations and given the current political situation, trust between nations and between companies and nations, is unfortunately at its lowest level. This makes it very hard sometimes to share data and information about current incidents with specific countries. I will give you an example. Earlier this year, we announced a big case, which was called Carbanak. It was a cybercriminal attack on European banks and we estimate that the attack resulted in 1 billion euros to be stolen. It took us a year to investigate this attack together with Interpol, Europol and ALA Law enforcement Agencies and the criminals were finally caught this summer. Again it was an international gang composed of Ukrainians, Russians, and some Europeans. We were simultaneously working on another case that is unfortunately going much slower because we are still working on it. We do see a resistance to share that creates a big problem for us and for our partners in law enforcement and this resistance tends to

> **"Carbanak was a cybercriminal attack on European banks: we estimate that the attack resulted in the theft of 1 billion euros."**

"Carbanak showed us that cybercrime is more and more organized. It is not just sporadic hackers as it was five years ago. Now it is organized cybercrime…Terrorists can hire the same group of hackers for terrorist attacks and it may be just a couple of years before something like that happens."

influence the whole security both in Europe and internationally. In addition, the Carbanak example showed us that cybercrime is becoming more and more organized. It is not just sporadic hackers as it was five years ago. Now it is organized cybercrime, with twenty, thirty, forty people who are working daily to try to steal money. This is very dangerous because the next step is obviously cyber terrorism. Terrorists can hire the same group of hackers for terrorist attacks and it may be just a couple of years before something like that happens. This loss of trust between nations definitely creates a big problem for the whole global security.

I also would like to add that sharing new information about reports is very important as well because one single company cannot see the whole picture. Our colleagues from Lockheed Martin have unique data, those from Intel have unique data, we also have unique data, but none of us sees the whole picture. Governments must understand that we need to ask for different sources, which is the only way you can see the whole picture and understand how to build a resilient society. And finally, partnership actually means relations of partners, of peers. In many cases, however, when we speak about partnership with governments it means "Give us some data and we will be very grateful." But it does not really work that way because, as a cybersecurity company, we need to understand what is going on and how to improve our products. We are aware that in many cases we are speaking about national security. We are not saying that we would like to know everything that is happening but, at the very least, we need to understand the current landscape in countries and regions so that we can improve our products and create better ones, which, at the end of the day, will protect the citizens of your countries. It should be a two-way street, and as Luigi Piantadosi said earlier, there is unfortunately no silver bullet in cybersecurity. It is all about building alliances, building partnerships between cybersecurity companies, between states and with everyone. Only together shall we make the world a safer place.

When we speak about partnership with governments it often means little more than, "Give us some data and we will be very grateful."

Invited Address

Ambassador Ihor Dolhov
Deputy Minister of Defense of Ukraine

Ukraine is facing a big and multifaceted problem. I will try to touch on several features that we discussed together a year ago: what has changed, in what direction, and what are the results of this change? From the outset, let me stress that I do not represent the official position of the Ministry of Defense of Ukraine here. My comments will rely on my new experience as Deputy Defense Minister and the developments that I have recently observed.

What Has Changed?

Let me start with cyber. For Ukraine and for the OSCE, cyber is not only a threat but it is in effect a cyberwar because our enemies in East Ukraine are supported by Russia. How do they operate? They jam the OSCE drones that are used to patrol the area and verify the withdrawal of weaponry. It is a very practical new tool that has come into use in this hybrid type of warfare. What has changed since last year? I will start with the military dimension. If in the summer of 2014, the Ukrainian army was ready to fight with less than 10,000 combat-ready troops, today we have more than 60,000 troops ready to fight in anti-terrorist operations. If a year ago the Ukrainian army counted 140,000 soldiers, it now counts 250,000. If last year, we had no clear vision of what was happening and in what direction we were moving, Ukraine now has developed a new strategic concept and a new military doctrine. This doctrine stipulates that the Ukrainian defense sector must implement all the necessary reforms to make the Ukrainian armed forces and defense sector compatible and interoperable with NATO. The goal set by the President of Ukraine and now confirmed by these documents is to upgrade the Ukrainian defense forces and defense sector to a level that will make our country ready to apply for NATO membership.

> **"...cyber is not only a threat, but it is in effect a cyberwar because our enemies in East Ukraine are supported by Russia.**

This military doctrine is a new phenomenon in Ukrainian political life. After more than twenty years of independence, we can call things by their names and the new military doctrine has openly stated that, at this stage, the Russian Federation is an enemy of Ukraine. Along with this declaration, we have started first to implement the doctrine and change the armed forces and second to change the institutional grounds of the Ukrainian defense sector. We are very thankful to all the governments from NATO member states and partners that made it possible for us to get instructors from Canada, the United States, Sweden, Poland and Lithuania. Our new military units are now being trained according to the NATO standards and these units are 100% ready to cooperate and fight along with any army of NATO member states. We are in the process of creating a new type of forces—special operation forces—and we will start training them this month. Our capacity and capability in terms of arms and armament has been increased. Instead of only repairing our arms and artillery systems, we are upgrading them and, even more, we have restarted research programs that had been frozen by the previous government because at that time there was no need to develop these technologies. We have also stopped all defense cooperation with Russia and, of course, this creates a number of problems for our defense industry since many Ukrainian enterprises were kept fully employed by the orders from the Russian Federation. So, how can we use Western technologies and produce the equipment we need? When the war started, we ran into immediate difficulties, one of which was communications. Thanks to the assistance of the United States and NATO, we somehow managed to solve this problem but in the long run, we must produce our

> **"The new military doctrine has openly stated that, at this stage, the Russian Federation is an enemy of Ukraine."**

> **"...we must produce our own communication system and we need partners to produce in Ukraine. We must...make our own drones."**

own communication system and we need partners to produce it in Ukraine. We must also counterbalance electronic means of identification and positioning and make our own drones. We have started to plan for this and other things that were not necessary several years ago but are badly needed now.

In What Direction are the Changes Going?

We fully enjoy our increasing cooperation with NATO. NATO has made decisions that are very important for the Ukrainian defense sectors and we have already implemented several projects in the framework of the new five Trust Funds NATO has established. We also resumed a very close strategic cooperation with the United States and the US Congress recently voted a bill to allocate $300 million of military technical assistance to Ukraine. Americans are increasingly involved in the training and reorganization of the Ukrainian armed forces and other nations, including France, are also ready to contribute.

> **"We thank the governments of France and Germany and NATO, for creating a trust fund for humanitarian demining."**

A problem of a military nature relates to the huge number of unexploded shells, munitions, and land mines on the ground. Unfortunately, our internal reports inform us every day about new casualties, mostly among the civilian population. So this is a top priority and again we are very thankful to the governments of France and Germany and to NATO, which is going to create an additional trust fund for this humanitarian demining. The territory to demine is very large and mostly agricultural, and we only have several weeks before the snow covers the land and makes it even more difficult to conduct a demining work.

Militarily again, we have more than sixty thousand troops in the conflict area. On the other side, there are four to six thousand combat-ready troops including ten to eleven thousand regular Russian army officers. We know them by names and we know where they are. In the Donetsk and Luhansk occupied regions, they strictly control the whole chain of command from top to bottom, down to the level of platoon. And officially we all continue to play the same game: Moscow informs us that there are no Russian troops there but everybody knows that they are present. We continue to pretend that there is no confirmation that the MH17 plane was downed by a Russian missile and was targeted intentionally and, in many other respects, the situation continues to be very strange. Why is it strange?

> **"Moscow informs us that there are no Russian troops, but everybody knows that they are present."**

Let me talk about the political set of measures and their implications. The Minsk process, signed by representatives from Ukraine, Russia and the OSCE in September 2014 sought to implement an immediate ceasefire but failed to stop the fighting in the Donbass region. Our thanks go again to President Hollande and Chancellor Merkel for trying to find at least interim solutions to solve the issue. After a recent meeting that took place here in Paris at the beginning of October, the situation has changed. Finally there is a sort of real ceasefire but it is not fully respected because separatists using small arms recently wounded five Ukrainian soldiers. An exchange of prisoners has started very slowly and six soldiers have now been released but 169 remain in prison and more than 500 are missing. Under OSCE monitoring and verification, we have also implemented additional security measures by continuing to withdraw battle tanks and light artillery 15 kms away from the contact line but, of course, we would like to see a stronger OSCE presence in the area. We still lack control over more than 300 kms of the Ukrainian-Russian border, which means that we cannot talk about a solution unless the border is open because satellite images show a daily supply of fuel, money, people, artillery and munitions on the other side. One of the provisional Minsk arrangements was to conduct local elections in the separatist-controlled territory but the separatists strongly refused to conduct their elections on the same day as the Ukrainian local elections. After the early October Paris meeting and under instructions from President Putin, the separatists finally recalled their self-proclaimed election dates in their territories.

What is next? The Minsk arrangements were to be implemented by the end of 2015 but it is already clear that it will not be possible to conduct local elections on the occupied territories by the end of the year. It is also clear that two other important

provisions of the Minsk arrangements cannot be fulfilled now. Why? The first provision calls for all foreign troops to be withdrawn from the area but Moscow continues to falsely claim that they do not have troops there, so there is nothing to withdraw. The second provision restores full Ukrainian government control over the state border throughout the conflict zone but we cannot control the border. So we cannot talk seriously about any local elections and without local elections, the Ukrainian government would not have a partner to negotiate further steps to settle the situation.

"...without local elections, the Ukrainian government would not have a partner to negotiate further steps."

Where Are We Now?

When I checked the news yesterday, Mr. Putin was stating that the annexation of Crimea is "Russian world." We know in Ukraine what "Russian world" means. We know that we have more than 1.5 million internally displaced persons, more than in Syria, and this is the result of the Russian aggression into Ukrainian territory. In Donetsk and Luhansk, which are more or less controlled by separatists, the local civilian population of over 2.5 million continues to be suppressed by the separatists and Russians. These 40,000 people control a huge territory and cannot envisage the possibility that the civilian population would be free to select their own way of life. So this is the result on the ground.

We are looking forward to start implementing the free trade agreement with the European Union on 1 January 2016 and are in the process of reforming our defense sector and our economy. This week, the Ukrainian parliament will vote on a new taxation code and pieces of legislation that we need to adopt before implementing the European Union trade agreement. Although the trade with Russia has drastically dropped down, we managed to survive and increase the trade volume with the EU and other countries. At last year's workshop, I was asked about the gas situation and its transit. Ukraine fulfilled its commitment and paid every single dollar for any cubic meters of Russian gas. In addition, we concluded an agreement with the European Commission and Ukraine's Naftagas was credited 300 million euros to secure gas supplies to Europe through the winter. What is very important is to note the price difference that Ukraine paid for gas: two years ago, it was $456, this year it is $264.

As a result of Russian aggression, "we have more than 1.5 million internally displaced people, more than in Syria"

Conclusion

So this is our future, but I would now like to come back to the threats and challenges. We were discussing hybrid warfare, a notion which I accepted a year ago. Now we have to to look forward to not just hybrid warfare but a new kind of hybrid politics. We once had *realpolitik*, but the future with which we will have to live will be hybrid politics. Whether it is a question of Syria or Montenegro or the support for political parties in France or in other countries, all of their characteristics are in my view a manifestation of the hybrid politics.

A New Paradigm for Relations with Russia versus a Return to Business as Usual

Ambassador Oleh Shamshur
Ambassador of Ukraine to France

Murphy's law says, never be too happy to see the light at the end of the tunnel, it might be the light of the approaching train. This is exactly what we faced after 2008. I will try to follow the guidelines the workshop chairman gave me and look at the situation from a conceptual point of view. First, let me say that it is never too early to think about the future of your interaction with your current opponent or adversary but you should decide that for yourself. Would you want to be involved in an ad hoc job or you would really like to change the whole design so that all the pieces would fit together? This is the dilemma being faced by the West right now. Even before looking at possible areas of cooperation with Russia, I believe that under the present circumstances there is only one area where cooperation can work, which is the implementation of the already concluded arms control treaties since this implementation is actually needed by both sides.

"There is only one area where cooperation with Russia can work, which is the implementation of the arms control treaties that have already been concluded."

Does the West "finally realize the need to work out a new paradigm for its interactions with Russia?"

So we have to define the conceptual base of this exercise. By that, I mean looking at the areas of possible cooperation or how the future would look like. Otherwise, this exercise might turn out to be an exercise in futility or, even worse, create a misleading and potentially dangerous and deceptive reality, a "tromperie" as the French would call it. In this context, I would like to pose a question. Is the West trying to get over its rough relations with Russia and return to a more business as usual relationship or does it finally realize the need to work out a new paradigm for its interactions with Russia?

The System of European Security Has Been Destroyed

The paradigm should be based on the real facts on the ground, including absolutely unacceptable behavior and annexation, further division, interests and principles, flagrant violations of international law, etc. When I spoke for the first time at the German Marshall Fund in Washington, D.C. in March 2014 in the midst of the Crimean crisis, several people in the audience actually addressed the issue of possibly revising the paradigm of this relationship. Unfortunately, the more I look at the discussion now, the more I see a lack of desire to think in those terms and even an inclination to go back to business as usual. And maybe business as usual is missing the understanding that a return to the status quo *ante bellum* is simply not possible. It is definitely not possible for one very simple reason: there is one man in the world, Vladimir Putin, who does not want a return to the status quo. He wants much more than that and that is the reality. In that sense, the business as usual approach is not simply useless, it is very dangerous. If the West wants to really build a new paradigm for its relationship with Russia, it should acknowledge the enormous difficulty of the task and if it does acknowledge it, it should face an inconvenient truth that a majority of politicians in the West are still denying. The truth is that the system of European security is not simply compromised or in danger, it has been totally destroyed. We have to reconstruct a new system of security: it may incorporate some elements of the existing system but it must be a new

"A return to the status quo *ante bellum* is simply impossible ... for one simple reason: Vladimir Putin does not want a return to the status quo. Does the West 'finally realize the need to work out a new paradigm for its interaction with Russia?'"

European security architecture that can work and provide the security that is definitely non-existent now. Of course, this new architecture should not have anything to do with the phony ideas once put forward by Mr. Medvedev.

There is one more victim of the Russian aggression and stark insufficiency of the western response—the regime of global non-proliferation has been very seriously damaged by the total collapse of the 1994 Budapest Memorandum on Security Assurances: the approaches that were a cornerstone of the Budapest Memorandum are now null and void. We are beginning to feel the consequences of the destruction of the Budapest Memorandum structure. We did not have much confidence in it before and many people in Ukraine who opposed the weak guarantees in the memorandum now feel even more deceived, although I am not in favor of returning to the nuclear option, which is not an option at all. If we allow Russia to get away with the annexation of Crimea or enforce its program in Eastern Ukraine—and Mr. Pascu talked about hard to swallow parts of the Minsk arrangements—we risk stimulating even more aggressive behavior by Russia. A new hot phase of the already existing situation would only be a matter of time. It is quite clear that the situation cannot be resolved by using force, but it cannot be resolved by using only diplomatic means either. We need synergy between diplomatic efforts, pressure on Russia—sanctions should be maintained—enhanced military and technical cooperation with Ukraine, and aid to Ukraine so that it can get over the current economic crisis and implement reforms. Only then shall we stop Russian aggression and only then can we start looking for a durable solution.

"We need to ensure a synergy between diplomatic efforts, pressure on Russia including sanctions, enhanced military and technical cooperation with Ukraine, and aid."

Russia's Attitude towards the West and the Need for Strategic Thinking

The West should not be deceived by what it would like to see. Most Russians do believe and support the current Putin regime, and this may be the most difficult part of the situation in Russia today. From above, the ideology of the "besieged fortress" is being continuously imposed on the Russian society and the majority of the Russian population supports it. I think that policy making in the West reflects a lack of knowledge concerning the underlying motives that shape the decisions made by Putin and his closest entourage. Whenever the U.S. and the West in general are hoping that Russia can be useful, it is eventually confronted with the reality that Russia is twisting the situation to its advantage. Syria is the perfect example. Many in Europe argued that the Russian presence was needed because it would alleviate the situation with the refugees. But what is happening is exactly the opposite. They are creating a new wave of refugees from areas like Aleppo, which has been attacked by Russian forces and aircrafts. And we should also recognize that, for the time being, no matter how weakened Putin may be, he is holding the strategic initiative and he will rig the game if he is allowed to do so.

"Putin is holding the strategic initiative and he will rig the game any time he will get a chance to do so."

So far the policy of the West toward Russia has showed a conspicuous absence of strategic thinking. Instead of a wishful thinking policy or a policy based on a state of denial, we need a policy that is not reactive but proactive and can prevent the emergence of new crises. If this state of denial approach continues, the West and its partners will go from one crisis to another. We should understand that resuming operations or interactions with Russia is not possible without a change in our attitude concerning the situation in Ukraine, and a Russian change of attitude toward international law. This is for the long haul since this change cannot be achieved tomorrow. So politicians need perseverance and backbone to find the right response to the aggressive actions by the Russian leadership. This is true both for the West and for Ukraine. Ukraine needs a new paradigm of its relationship with Russia, because so many notions that were imposed in Soviet times on the Ukrainian population are now dead. We have to build good relations with Russia but, this is not possible without a change of attitude toward Ukraine in the heads of the Russians and without the discontinuation of the Russian aggression. It will take time. Unfortunately this is the reality. Since we are in France, I would like to quote Nicolas Baverez, a French expert who published an opinion op-ed a couple days ago in *Le Figaro.* He wrote: "New autocrats think that they can control the time. This allows them to employ coherent long-term strategies in this chaotic and violent world. Facing them, the democracies should reform and unite to defend freedom, answering the global challenges of the 21st century."

The Increasingly Strained Relationship with Russia: Can Cooperation Function without Trust?

Mr. Ioan Mircea Pascu
Vice President of the European Parliament; Former Minister of Defense of Romania

Russia's Challenge to the post Cold War Order

Let me begin by making a few points concerning the crisis involving Russia and Ukraine.

The Ukraine crisis came as a surprise, although, after the war in Georgia of 2008, it should not have. For the first time since 1945, borders in Europe were being modified through force. One could say that what happened in both Georgia and Ukraine was a result of the decision taken by the allies at the Bucharest NATO summit in 2008. At that time, NATO withheld the Membership Action Plan (MAP) from the two candidates while offering them the certainty of membership in a distant future. In other words, they offered them light at the end of a non-existent tunnel. In order to make sure that this membership would never happen, Russia chose to cripple both countries territorially, therefore making them ineligible. By annexing Crimea and militarily destabilizing eastern Ukraine, Russia effectively challenged the very foundation of the post Cold War order, primarily in Europe, but also beyond, for example in Syria today. They also claimed the right to be treated as an equal of the US, as the Soviet Union once was, at least in the sense of recognizing Russia's special privileges within its "sphere of influence," including the former Soviet territory and, possibly, its adjacent areas.

"By annexing Crimea and militarily destabilizing eastern Ukraine, Russia effectively challenged the very foundation of the post Cold War order."

The Minsk 2 Ceasefire Agreement

Both NATO and the EU have reacted to this new situation. NATO reacted by strengthening its collective defense function based on the recognition that conventional war in Europe had again become a possibility. The EU reacted by progressively imposing sanctions against Russia, starting in March 2014, in the hope that it would alter Russia's course. These included diplomatic measures; restrictive measures targeting individuals such as asset freezes and travel restrictions; restrictive measures in response to the illegal annexation of Crimea and Sevastopol; economic sanctions including measures targeting exchanges with Russia in specific economic sectors; and measures concerning economic cooperation that were introduced in July 2014. The downing of Flight MH17 in the context of the military destabilization in Eastern Ukraine led to an enhancement of the sanctions approved previously and the formulation of a number of political requests addressed to Russia and the separatists it actively supports. However, these conditions "changed polarity" half a year later, when the Minsk 2 Ceasefire Agreement was signed on 23 February 2015.

The EU reacted by progressively imposing sanctions against Russia, starting in March 2014, in the hope that it would alter Russia's course.

The Minsk 2 Agreement stipulates that the first step should consist of a mutually agreed and viable ceasefire; the re-establishment of Ukrainian control over its border; an immediate halt to the flow of arms, material and military personnel from the Russian Federation into Ukraine; the urgent release of all hostages held by the illegally armed groups, as well as the prisoners detained by the Russian Federation."

It also stipulates that, after elections in the separatist regions of Donetsk and Lugansk, Kiev will restore control over the border with Russia; the authorities in Donetsk and Lugansk will be permitted to legally keep militias; an encompassing constitutional reform will be implemented by the end of the year, which will decentralize the Ukrainian political system and offer privileges to Donetsk and Lugansk, including self determination in relation to language; the liberty to appoint judges and prosecutors; as well as the establishment of economic relations with Russia.

Moreover, on 19–20 March 2015, "The European Council agreed that the duration of the restrictive measures against the Russian Federation, adopted on 31 July 2014 and enhanced on 8 September 2014 should be clearly linked to the complete implementation of the Minsk agreements, bearing in mind that this is only foreseen by 31 December 2015."

Russia "achieved its goals: it has Crimea...it has obtained a veto over major decisions by Ukraine, through control over Donetsk and Lugansk; and it is getting Ukrainian membership in NATO and possibly the EU off the table.

For almost six months after its signature, the Minsk 2 Agreement failed to be implemented. Then, in the context of Russia's shift of strategic focus to Syria, it started to be implemented in earnest, opening a prospect for lifting the sanctions against Russia in early 2016, with the possible exception of the sanctions that are directly related to Crimea. For all practical reasons, Russia, which could not and therefore did not want to conquer Ukraine entirely, has already achieved its goals: it has got Crimea, the most important strategic component; it has obtained a veto over any major decisions by Ukraine, through control over Donetsk and Lugansk; and it has succeeded in getting Ukrainian membership in NATO and possibly in the EU off the table.

Can There Be a Return to a Cooperative Relationship with Russia with Less Trust?

Under these circumstances, will the lifting of the sanctions following the implementation of the Minsk 2 Agreement mean a return to the happier days of "business as usual" in relations with Russia? This remains to be seen. To a large degree, it will depend on the future behavior of Russia, particularly in Europe, with regard to the NATO and EU countries on their eastern flank, a context in which Moldova could very possibly be a test case.

The real question we are supposed to answer is who most needs a return to a more cooperative phase in the relations with Russia? Is it the West—which did not initiate the actions triggering the current freeze—or is it Russia, which considered it in its direct interest to continue its collaboration with the West over Iran, for instance, in spite of the freeze mentioned above? Another crucial question would be: can one build anew a cooperative relationship, only this time with less trust than before? After all, Russia is an indispensable actor of the international system and cooperation is always better than confrontation. However, given what happened, which has not been at the "initiative" of the West, Russia lost credibility and it will be much more difficult to trust its commitment to preserving the current European and international order, against which it openly pronounced itself. As an illustration, even the technical negotiations on managing the recently appeared confrontation, both locally in Syria and regionally, at the Euro-Atlantic level would not have been necessary, had Russia not launched itself deliberately into a near-confrontation and with brinkmanship similar to that of the Cold War era. Let us not forget that Russia, a consummate "gambler" at the table of international politics, does not hesitate to "print" a new playing card, even when, or especially when, it appears to have run short of them.

"Who most needs a return to a more cooperative phase in the relations with Russia? Is it the West—or is it Russia?"

NATO-Russia Relations: Prospects and Assessment

Ms. Radoslava Stefanova, Head of Russian-Ukrainian Relations
NATO Political Affairs and Security Policy

Today, the NATO-Russia relations are at their lowest. It is certainly not business as usual and for that reason, I would like to explain what business as usual was.

The NATO-Russia Council

Our relations with Russia were channeled through a very unique institution called the NATO-Russia Council. It was devised specifically for Russia, was very far-reaching and wide-ranging, and it was not offered to any other partner. Russia was an equal partner around the table with the North Atlantic Council and it had an elaborate structure of working groups. Our cooperation, which goes back over many years since the Council was established in 2002, included many common projects of mutual benefit. Russia was taking this structure seriously because it takes the NATO organization seriously. It was a very useful institution for Russia, giving it access to our headquarters, our decision-making procedures, our capabilities and technology, things that it did not have and made use of. For example, Russia requested help from NATO when one of its submarines got in trouble in the Far East and Russia did not have the technology to extract it. It was also useful for NATO. During one of our operations in Afghanistan, for example, the Afghans did not trust the Russians directly but ended up accepting spare parts for their helicopters and air force because the Russians worked with NATO.

> **" Russia requested help from NATO when one of its submarines got in trouble in the Far East."**

The Russian Invasion of Ukraine and Annexation of Crimea

After the Russian decision to invade Ukraine and illegally annex Crimea by force last year, all practical military and civilian cooperation within the NATO Russia Council was suspended. The institution still exists but it is frozen. The political dialogue remains open and there have been two formal meetings of the NATO-Russia Council at ambassadorial level with Ambassador Alexander Grushko, Russian Permanent Representative to NATO, but they were unproductive. Two more meetings in the framework of the wider Euro-Atlantic partnership were unsuccessful as well for lack of what to say to each other. As long as Russia keeps insisting that there are no Russian troops in Ukraine and makes similar statements in Russia Today, Sputnik, or other various Russian outlets, it is not clear how discussions in the NATO-Russia Council can become more constructive.

In the meantime, high-level contacts are continuing. Both the current NATO Secretary General and his predecessor keep meeting with Foreign Minister Sergey Lavrov. Secretary General Jens Stoltenberg briefly met with President Putin in New York in the margins of the UN General Assembly meeting. Whenever Ambassador Grushko and his deputy, Mr. Yuri Gorlach, request a meeting, the NATO staff is always available but we hardly have anything in common anymore. We do not agree on their actions in Ukraine and in Syria. We still cultivate the military lines of communication, however, and insure that they work but, for the past two years, Russia has stepped up its military exercises and returned to essentially a Cold War practice of snap exercises. It regularly misreports the numbers of those exercises to the appropriate Arms Control mechanisms in Vienna and this creates a lot of unpredictability and instability on our borders. For that reason, our top military officials have tried to speak directly to Russia's chief of defense, but they have not been able to get through to him. Although we tried to install some transparency

> **"Russia has stepped up its military exercises and returned to essentially a Cold War practice of snap exercises...It regularly misreports the numbers of those exercises."**

in our relationship, there is virtually no interest on the Russian side to be transparent, especially when it concerns Russian military activity. So this is a problem and we cannot force them to the table if they do not want to be there.

NATO's Review of its Relations with Russia

At the moment, NATO is in the process of undergoing a thorough review of its relations with Russia. Next year's Warsaw Summit will examine Russia's current foreign defense policy, what it means for NATO and what kind of relationship NATO should have with Russia. NATO has also invested a lot in collective defense with the introduction last year of a readiness action plan which more than doubles its Spearhead Force, a highly flexible and mobile force that can be deployed within 48 hours if needed. Russia has demonstrated its ability to move troops very quickly from one theater to another, including when it invaded Crimea, and we must be prepared to deal with this. In addition, NATO is doing work to counter a hybrid cyberthreat and threats coming from ballistic missiles.

> **"We have been working with Ukraine to help with their defense capabilities and provide NATO advice and expertise on how Ukraine can reach the standards that it wants to reach."**

In my section especially, we have been working with Ukraine to help with their defense capabilities and provide NATO advice and expertise on how Ukraine can reach the standards that it wants to reach. We have also been working with other partners, in particular Moldova and Georgia. We consider that the Russian pattern of behavior of stationing illegal Russian troops in Moldova and Georgia is destabilizing the region and we have been providing these two countries with help and institutional capacity building that they have requested from us. This partnership outreach is an important part of our work.

I will finish with a brief assessment of why NATO has turned away from a very cooperative relationship with Russia and why this is becoming more confrontational. To illustrate this, I will point out that the NATO strategic concept document is still valid, there is no intention of changing it, and it still says that NATO is striving towards a strategic partnership with Russia. Already in 2010, however, Russia had designated NATO as its number one foreign threat and had even upgraded this threat level in their new military doctrine late last year and the naval doctrine this year. There will probably be a similar language in the new strategic concept that Mr. Putin has promised by the end of 2015. So, there is clearly a different attitude from Russia towards NATO as opposed to NATO's attitude towards Russia. We do value cooperation, but not at any cost, because we are talking about a fundamental difference of principles. It is not a problem between NATO and Russia, it is a problem of the Russian leadership's perception of NATO. On this subject, there is a group of democracies that would not be adverse to an institutional transition of power and that scares the current Russian leadership. Due to an incredible lack of soft power, Russia finds itself in a situation where it forces countries to stay in institutions that it has created, whereas these countries, like Ukraine and others in the region, are attracted by other social, political and institutional models—mostly the European Union—and wish to go in a different direction. This undermines the very construct of power of the current Russian regime and creates the problem with NATO.

> **"In 2010, however, Russia designated NATO as its number one foreign threat."**

For How Long Will Politicians Repeat their Mistakes?

Ambassador Jaromir Novotny[1]
Advisor to the Prime Minister of the Czech Republic (Foreign Policy and Defense);
Former Deputy Minister of Defense

Two years ago, I wrote an article on the situation in Syria in which I expressed some concerns over the fact that the West supports the so-called democratic opposition to Assad´s régime by supplying weapons. This so-called democratic opposition is a community of Sunni Islamic fanatics from all over the Islamic world including China, Russia (Chechnya, Dagestan), Central Asia and Western European countries. All are armed and financed by Saudi Arabia, monarchies in the Gulf, and Turkey. It requires great imagination to consider these countries as representatives of democratic regimes in the region. As to the Turkish Government and its supporters among French and British politicians who share a fierce desire for the destruction of Syria, do they want to unknowingly contribute to redrawing the map of the Middle East? It could result in an independent Kurdistan (which could begin by joining the areas inhabited by Kurds in Iraq and Syria, maybe even in Turkey), a Shiite Iraq, a Sunni Iraq, an Alawite Syria, a Sunni Syria, and no one knows what would happen with Lebanon. Do the EU politicians realize how massive an immigration wave this would start? Is the EU, where the people are already reluctant to accept other Muslim immigrants, able to absorb such a wave of immigration? How long will politicians repeat their mistakes? Indeed, are not Afghanistan, Libya, and the "Arab Spring" enough? Must Syria be destroyed as well? At the beginning of the 20th century, there was a saying among diplomats: "If the British and the French begin to contemplate over the map of the Levant with pencil in hand, it is the beginning of major problems for all."

This so-called democratic opposition is a community of Sunni Islamic fanatics from all over the Islamic world...armed and financed by Saudi Arabia, Gulf monarchies, and Turkey.

The Situation in the Middle East Today

I wrote my article in March 2013. More than two years later, what is the situation like? As a reminder, Iraq and Syria were artificial creations of British and French diplomats when the Ottoman Empire disintegrated on the eve of the World War I. Each contains communities of Sunnis, Shiites and Kurds. In Washington on 10 September, Lieutenant General Vincent Stewart, Director of the Defense Intelligence Agency, told an industry conference that he is "wrestling with the idea that the Kurds will come back to a central government of Iraq," suggesting that he believed it was unlikely. On Syria, he added "I can see a time in the future where Syria is fractured into two or three parts." Speaking on the same panel, CIA Director John Brennan noted that countries' borders remain in place, but that the governments have lost control over them. Thus, a self-declared caliphate by the Islamic State straddles the border between Iraq and Syria. "Iraqis and Syrians now identify themselves more often by tribe or religious sect, rather than by their nationality. I think the Middle East is going to be seeing change over the coming decade or two that is going to make it look unlike it did."

"Iraqis and Syrians now identify themselves more often by tribe or religious sect, rather than by their nationality."

At another conference on intelligence on 27 October in Washington, again CIA Director John Brennan stated "When I look at Libya, Syria, Iraq and Yemen, it is hard for me to envision a central government in those countries that is going to be able to exert control or authority over the territory that was carved out post World War II. A military solution is just impossible in any of these countries." Bernard Bajolet, head of France´s DGSE external intelligence agency, who also addressed the same conference, noted that the region was not likely to return to its former self following the current conflicts: "The Middle East we have known is

According to CIA Director John Brennan, "A military solution is just impossible in any of these countries."

1 These remarks are entirely my personal views. They do not reflect the positions of the prime minister or the government.

over, I doubt it will come back. We see that Syria is already divided on the ground, that the régime is controlling only a small part of the country, only one-third of the country that was established after World War II. The north is controlled by the Kurds, we have the same thing in Iraq. I doubt really that one can come back to the previous situation."

According to Henry Kissinger, "With Russia in Syria, a geopolitical structure that lasted four decades is in shambles. The U.S. needs a new strategy and priorities."

On a 26 October CNN special, American journalist Fareed Zakaria declared: "the Iraq War was a failure and a terrible mistake, causing geopolitical chaos and humanitarian tragedy. The United States replaced the régime in Iraq and gave the new one massive assistance for a decade. The result? Chaos and humanitarian tragedy. Washington toppled Muammar Gaddafi´s régime in Libya but chose not to attempt nation building in that country. The result has been chaos and humanitarian tragedy. Washington supported a negotiated removal of Ali Abdullah Saleh´s régime in Yemen and the election that followed, but generally took a back seat. The result again was chaos and humanitarian tragedy. The reality in that part of the world is that many of its regimes are fragile, presiding over weak institutions, little civil society, and often no sense of nationhood itself. In that situation, outside interventions, however well-meaning, might not make things better. Sometimes they can even make things worse." And finally, on 16 October, Henry Kissinger published an article entitled: "A Path Out of the Middle East Collapse." The main idea of the article is:" With Russia in Syria, a geopolitical structure that lasted four decades is in shambles. The U.S. needs a new strategy and priorities."

How Are the Different Middle East Actors Staking their Positions?

Here is below a short summary of how the different players in the Middle East crisis see possible solutions:

- Saudi Arabia strongly supports the Sunni fundamentalists with weapons and finance and is involved in a proxy war with Iran, particularly in the Syrian civil war.
- Turkey supports the Sunni fundamentalists and cooperates with the Islamic State. Supply routes for ISIS go through Turkey; Turkey is buying ISIS oil; ISIS fighters are treated in Turkish hospitals. Turkey is even fighting against Syrian Kurds.
- The UK and France support the so-called democratic opposition, which in fact consists of Sunni fundamentalists in Syria, and attack the Islamic State in Iraq.
- The rest of the EU (Germany, Spain and Austria) are prepared to negotiate with Assad.
- Israel discreetly supported the rebels operating near the Golan and perhaps even in areas inhabited by Druze. It is assessing the conflict in terms of its own security interests.
- Iran strongly supports Assad and is fighting a proxy war with Saudi Arabia.
- Russia also strongly supports Assad. Russia´s principal concern is that the collapse of Assad regime could reproduce the chaos of Libya, bring ISIS into power in Damascus, and turn all of Syria into a haven for terrorist operations, reaching into Muslim regions inside Russia´s southern border in the Caucasus and Central Asia.

In concluding, I would like to raise two questions in relation to the immigration crisis: First, is it fair that a country that is hosting the soccer World Cup at a cost of billions of dollars, that is constructing ski slopes in the desert, and that professes belief in Islam, is unable or unwilling to accept its fellow Muslims? Second, what is NATO's credibility when the sea borders between two member states—Turkey and Greece—and the sea border of Italy are controlled by human traffickers?

How Did ISIS Develop in Its Present Form and Achieve Rapid Gains

Ambassador Fareed Yasseen
Ambassador of Iraq to France

I need to be convinced of the wisdom of Intelligence agencies because they have been wrong more often than not. In our panel, Ambassador Novotny rightly pointed out the negative role played by certain actors —countries such as Turkey, Qatar, and Saudi Arabia, but I disagree with him on a few things. First, mistakes happened in dealing with Saddam Hussein, with Assad, with Kadhafi—who will be next?

A mistake by politicians in the West has been their wavering treatment of dictators: "first, preferential treatment, then war."

There is something shameful in this: first, preferential treatment, then war. Whom do you point the finger at for this kind of wavering? Second, the Ambassador's description of Iraq and Syria has some truth to it but it is only partial truth. The reality is very complex and cannot be apprehended using reductive methods. To my mind, not getting rid of Saddam Hussein in 1991 was the first major mistake that the United States made when it went to war in Iraq. Removing Saddam in 1991 would have resolved a lot of issues and helped make the transition to a better Iraq at a far lesser cost for the Iraqi people. The US approached Iraq in an extremely reductive fashion, dividing it into three categories (Kurds, Shia, Sunnis), but Iraq is much more multi-dimensional than that. For example, the urban Sunnis have more in common with the urban Shia than with the rural Sunnis. And right now, 40% of Daesh's fighting force is made of Iraqis who are mostly rural Sunnis. So it is really complex.

"Not getting rid of Saddam Hussein in 1991 was the first major mistake by the United States went it went to war in Iraq."

The Perfect Storm that Led to the Emergence of ISIS

Anyway, all this is about the past. I want to talk about the future because today's serious problems in the Middle East concern all of us, wherever we are. People thought that ISIS just came out of the blue and occupied Mosul in June 2014. In fact, ISIS resulted both from a number of developments that took a long time to come about and from more instantaneous events. Indeed, if we examine the root causes of the emergence of ISIS, we will find that everyone shares in the blame: the Iraqi government, with its perceived mistreatment of its Sunni minorities in Mosul and the very pervasive corruption that was engendered in 2003; the West, for the way in which they handled the Syrian crisis, during which Syria became a breeding ground for extremist Jihadists; countries from the Gulf that have helped, at least indirectly, promote extremist Jihadism, not only in Iraq and Syria, but in Europe and in places like Senegal and the United States. Because of the way these various factors strengthen each other, one can even say that ISIS resulted from a perfect storm.

"ISIS itself can be seen as the natural extension of Al Qaeda, which engendered Al Qaeda in Iraq, which morphed into the Islamic State in Iraq, then the Islamic State in Iraq and Syria, and then ... the Islamic State, period."

ISIS itself can be seen as the natural extension of Al Qaeda, which engendered Al Qaeda in Iraq, which morphed into the Islamic State in Iraq, then the Islamic State in Iraq and Syria, and then it relabeled itself the Islamic State, period. These entities essentially form a continuum whose dimensions and complexity increase with time and they are a threat to us all: 9/11; London, Madrid, Charlie Hebdo in Paris and, more recently, the Russian plane crash in the Sinai. Thus, the reach of ISIS is global, but so is their membership: we have counted approximately 80

nationalities among the foreign fighters that are present in Iraq. These new Jihadists are smart and have become extremely adaptable in the way they develop new tactics for the battlefield. They are not short of smart engineers, and we have already seen how adept they are at using information technology, so we should not be surprised by their use of suicide bombers and armored vehicles, turning them into practically unstoppable armored explosive devices, or by how they artfully booby-trap the houses they withdraw from or abandon and even in their attempts at using chemical agents.

The ISIS Ideology Carries in itself the Seeds of its Own Destruction

From our perspective, the reactions of many countries, particularly the United States, were slow in the coming. The language world leaders used to describe their response to ISIS seemed to me not to convey the urgency that the matter required. For example, the expression used until then by President Obama, "to degrade and ultimately defeat ISIS" may imply a period during which ISIS is contained before it is defeated. The problem is, you just cannot contain ISIS, certainly not in this age of the internet, easy travel, and porous borders.

I was therefore quite heartened recently to hear Secretary of Defense Ash Carter use much stronger language in connection to ISIS, explicitly using the word "destruction." This language feels far more appropriate than the standard "degrade and ultimately defeat."

Yet ISIS is not invincible. To paraphrase George Kennan, ISIS's ideological nature carries in itself the seeds of its own decay. I will give some examples of how, by getting everybody geared up to fight them, they are weakening their own position and degrading their support, even within the communities that they control. I will cite these examples of ISIS's "unforced errors" in a chronological way:

- *First Error.* ISIS occupied Mosul in June 2014 when the United States were gearing towards mid-term elections and Iraq was not a big draw in public opinion. What did ISIS do? They assassinated two Americans, a journalist, James Foley and a humanitarian worker, Peter Kassig, in a horrendous way and posted their killing on the Internet. That action placed Iraq back in the American debate, and led to one of President Obama's most moving speeches. Also, it also led the United States to conduct a review of how best to salvage the Iraqi armed forces.

- *Second Error.* This happened when ISIS attacked the Kurds. They were in full control of Mosul and the Nineveh province and could have remained there and consolidated their own Afghanistan-like chunk in Syria and Iraq. But propelled by their ideology, they attacked Iraqi Kurdistan, seriously endangering Erbil and threatening the American Consulate there. The ISIS push was stopped, thanks to hard fighting by the Iraqi PeshMerga forces and renewed support from the United States, Iran, France, and other EU countries. One important factor here was the new involvement of US air power. This saved Erbil, and turned the tide on ISIS.

> **"The ISIS push was stopped, thanks to hard fighting by the Iraqi PeshMerga forces and renewed support from the United States, Iran, France, and other EU countries"...plus "US air power."**

- *Third Error.* Who can abide by the way ISIS treats women and the people they enslave? Their treatment of women and religious minorities (in particular the Yezidis) has no place in the 21st century. More than anything else, this has united the civilized world against them. Note, though, that this ISIS-sanctioned kind of behavior is not new. It happened in 2006-2007 when Al Qaeda controlled Anbar Province, and forced young girls to marry foreign fighters against their will and that of their families. The Surge put an end to it in what should be a successful case study for the management of crises. The Surge worked in part because this kind of behavior helped drive a wedge between the local population

> **"Who can abide by the way ISIS treats women and the people they enslave? Their treatment of women and religious minorities (in particular the Yezidis) has no place in the 21st century."**

and Al Qaeda. This was one reason why the very conservative local tribes turned against them. Half a decade later, ISIS has shown that it can learn from the past: this time, instead of preying on the daughters of majority communities, they proceeded differently. Locally, they targeted a small history minority, the Yezidis, enslaving the women, and killing all the men so that they could not fight back. Beyond the regions under their control, and particularly in Europe, they used the Internet to lure young women of Muslim origin to come to Syria and serve as war brides.

- *Fourth Error.* ISIS's fourth mistake was to change their name, removing all geographic limitations, thus implying that they covet all Muslim lands, including Gulf Cooperation Council (GCC) countries and in particular Saudi Arabia, home of Islam's holiest shrines. Indeed, ISIS has hit targets in Saudi Arabia, not only Shia shrines (they consider the Shia to be heretical) but also representatives of the state. This not-so-subtle message has not been lost, and the GCC countries are now more engaged in the fight against ISIS.

- *Fifth Error.* The ideology of ISIS had support in Jordan, which was on display in the celebrations carried out by families when Jordanian fighters returned from Iraq or when they died there. This has changed after the horrible burning of a Jordanian pilot in January 2015. No one in Jordan will dare carry out such displays any more. More so, members of the Jordanian armed forces, most of whom originate from traditional communities where family honor and clan loyalties rank high, will not forget that ISIS subjected one of their own to such inhuman treatment.

- *Sixth Error.* ISIS has committed terrorist attacks against Turkey, which is the main transit country for most of their foreign recruits and support originating from outside the areas they control. Turkey has increased its controls on its borders, and an Iraqi expert who follows ISIS very carefully told me that the level of inflow of foreign fighters from Turkey into Syria and Iraq has dropped from fifty a day to five a day. If Turkey continues on this trend, then ISIS will starve.

The actions of ISIS "are increasing the forces arrayed against them...on its own, no single Iraqi community can defeat ISIS, but if we are united, we can."

What does all this mean? It means that ISIS is taking actions that are consistent with its ideology but that are increasing the forces arrayed against them and bringing these different forces together. This is illustrated by the way the various components of Iraq's society and polity have reacted: there is the realization that on its own, no single Iraqi community can defeat ISIS, but that if we are united, we can.

One characteristic of ISIS and other Jihadist groups is that they are believers in end of world Muslim scenarios. They are preparing themselves for the battle of end of times that, according to their beliefs, will take place in Syria between the forces of good and the forces of evil. In their scenarios, they are, of course, the forces of good, the forces of evil are everybody else, but most specifically those they label as "the Crusaders" and "the Jews." Some analysts have cautioned that this belief will unite these various strands. It is significant that Al-Zawahiri, who as head of al-Qaeda is opposed to ISIS, sent orders to his followers in Syria to line up behind ISIS when the Russians announced their plans to increase their involvement in Syria.

"ISIS and other Jihadist groups...are believers in end of world Muslim scenarios...preparing themselves for the battle of end of times that...will take place in Syria between the forces of good and evil. "

What the Coalition Will Need in order to Achieve the Destruction of ISIS

In order to destroy ISIS, we need to act on several levels:

Territory. We must deprive ISIS of territory and that can only be achieved by military action. Things are going well in this direction: although we suffered some surprising setbacks in Ramadi, Beiji has recently been retaken and further progress is expected. This success is due to better coordination between the various components of the Iraqi armed forces, the popular mobilizations, and coalition air power. In the next couple of weeks, we expect action on Ramadi and the famous

Sinjar mountain where the Yazidis sought refuge. Once the territory has been taken back, it needs to be stabilized. This is necessary in order for the refugees not only to return, but to stay in their homes. Iraqi authorities, together with the United Nations, have initiated a sustained effort to set up police stations and courts, to revive the infrastructure and utilities, even to provide funds for small businesses to start up. This approach seems to be working. Still, this is short term; long terms measures (including political reform) will need to be implemented.

"ISIL's local sources of revenue (oil, antiquities, smuggling, 'taxation') cannot cover their local expenses...the balance is covered by cross-border remittances, probably from Gulf Cooperation Council countries."

Resources. ISIS must be deprived of its resources and the money. Some reports indicate that ISIL's local sources of revenue (e.g., oil and antiquities, smuggling, "taxation,"…) cannot cover their local expenses, and that the balance is covered by cross-border remittances, probably from GCC countries. These remittances are, of course, illegal and there are international efforts aiming to curtail them. But more needs to be done.

Turkish Border. The overwhelming majority of foreign fighters reaching Syria and Iraq come through Turkey, but the efforts of the Turkish government to prevent this are inadequate. Turkish authorities should control the border much more comprehensively. In any case, that is in their own interest.

Ideology. We also have to combat the ideology of ISIS. This is probably the most difficult part, because the promotion of this ideology is widespread and diffuse. Much of the promotion of the ideology happens through satellite channels and the internet. But the main proponents are identifiable: they are clerics who would not be able to hold their own in a debate with a well-trained scholar. Measures like the gag order placed by the Norwegian government on one such cleric could help, as would limiting their access to printed materials, satellite, audio, video and the Internet. There are legal measures that could apply: hate speech legislation, or anti-pedophilia laws. But this would require the cooperation of internet service and content providers, and that will not happen without pressure from governments and the public. We will also have to find better ways to deradicalize returning Jihadis, and also better ways to prevent young people at risk of succumbing to the attractions of extreme messages, like creating better and more inclusive schools, or even reintroducing of whatever strengthens the national fabric, e.g., national service. In Iraq, the reintroduction of national military service is a subject of debate.

It is worth noting that variants of ISIS have happened in the past. The same ideology first appeared in the late 18th century, when Muhammad bin Abd Al-Wahhab, the founder of this ultra-conservative, fundamentalist school of thought, rose up and occupied large areas of the Arabian Peninsula, ransacking and pillaging cities outside of the Arabian peninsula and well into the South of Iraq. This rebellion was put down in the first decade of the 1800s by an expeditionary force sent by the Viceroy of Egypt on orders of the Caliph in Istanbul. The latter, it should be noted, represented Islamic legitimacy. In the same vein, the ideology of ISIS should be dealt with and addressed by Muslims who are seen to be legitimate. Just as the liberation of Iraqi territory needs to be carried out by Iraqis, so must ISIS ideology be dealt with by Muslims who are seen by Muslim communities as legitimate.

"Just as the liberation of Iraqi territory needs to be carried out by Iraqis, so must ISIS ideology be dealt with by Muslims who are seen by Muslim communities as legitimate."

Lessons Learned from Digital Info-Terrorism: A Technical Vision

Mr. Andrea Formenti
Founder and CEO, Area SpA

Since I founded AREA in 1996, I have been continuously involved in understanding the global trends concerning electronic surveillance and lawful interceptions and translating them into systems and country-specific projects. Although our company has established roots outside of our country, our leading market position in Italy gives us a unique opportunity to deal on a daily basis with all the various public authorities and their own vertical requirements.

Maria Giulia/Fatima's Story with ISIS

Last year, we talked about the Dark Web and how some Italian citizens were digitally recruited by Daesh/ISIS. A few months ago, Maria Giulia Sergio, a 27 year-old Italian woman, moved to Syria to join ISIS together with her Albanian second husband. She converted to Islam and is now accused of recruiting for ISIS. Recently, several people were arrested in Italy and Albania, mainly family members, together with a 30 year-old Canadian citizen, Haik Bushra, who had some responsibility in Fatima's recruitment.

Being able to provide technology to Italian law enforcement agencies gives us an almost unique opportunity to learn through this kind of specific domestic investigations about Daesh's appeal, both within and outside Muslim communities. In this case, Maria Giulia/Fatima was born in 1987 and grew up in a typical catholic family that was neither wealthy nor poor. In early 2000, the family moved from southern Italy to the north of the country near Milan where Maria Giulia received a good public high school education. Maria Giulia started her radicalization process in 2010 after having watched on YouTube Yusuf Estes, an American preacher from Texas who converted from Christianity to Islam in 1991.

Technical Aspects of Uncovering her Story

Italian legal prosecutors and investigators had a chance to obtain a full picture of the way DAESH works and gets recruits thanks to conversations that were conducted in Italian and fell entirely under national jurisdiction; prosecutors had asked for "all technical interception capabilities to be put in place." In the initial phase, Facebook and Skype were widely used by Fatima to communicate from Syria with her family members in Italy. The plan was to move the entire family to Syria. From the publicly available intercepted conversations, it appears that Fatima and her terrorist organisation had false information about what can be intercepted; for example Fatima stated many times over Skype that her audio channel was absolutely safe—probably this is a typical internal propaganda effect and maybe only the audio channel generated in Italy is under surveillance.

> **Fatima's terrorist organization had false information—she "stated many times over Skype that her audio channel was absolutely safe."**

Currently it is not easy for an Italian legal prosecutor with all the judicial authorization (i.e. a specific target-based warrant) to have direct access to the communication contents generated through the so called Over The Top application service providers. In fact the "Big Six" communities (Apple, Facebook, Google, Microsoft, Twitter and Yahoo) are not providing the same level of direct cooperation with Italian authorities. I was recently at a conference in Washington DC and realized that the daily life of the US Law Enforcement Agency (LEA) is not 100% complication free either; it seems like they are facing more prob-

> **(Apple, Facebook, Google, Microsoft, Twitter and Yahoo) do not provide the same level of direct cooperation with Italian authorities.**

lems than I would have expected. A specific presentation was entitled "Google, Apple, Facebook and Other Internet Giants Battle Law Enforcement over User Privacy Rights." Some of the questions were, "Why would law enforcement regard a court order, warrant or subpoena as routine while the party served with the order calls it a grave constitutional threat? How are privacy pressures influencing the debate?" Recently, the New York County District Attorney's Office stated: "We see no basis for providing Facebook with a greater right than its customers are afforded" and Apple CEO Tim Cook said "Let me be crystal clear: weakening encryption or taking it away (for example by creating an intentional backdoor for law enforcement) harms good people who are using it for the right reason."

Apple's Tim Cook has said that weakening encryption or taking it away...harms good people who are using it for the right reason.

The needs of Law Enforcement Agencies are not all strictly based on accessing contents. For example, a response to the question—"Which Skype accounts are used with a specific (Syria based) IP address?"—would be useful information for some Italian LEAs. We already have some good examples to imitate: Research in Motion (RIM), the maker of BlackBerry, has been actively cooperating with Italian national authorities for many years and has provided valuable contributions to all the judicial and national security investigations. Of course, our company's contribution remains exclusively technical and our goal here is just to highlight cases of better cooperation between countries and between public and private sectors in order to mitigate the fact that internet encrypted communications will become more widespread than ever.

Workaround Methods

What should we do in the meantime? We can work around the technical limitations of encrypted communication in several ways. Software agents or government spyware are not the "panacea" for every investigation needs in cyberspace; they are very useful but just as "ultima ratio" and in very specific cases. The hack of the Italian spyware maker Hacking Team last summer did teach us some lessons. Some years ago, Area SpA designed and finalized a Virtual Human Intelligence Platform in order to give Italian Law Enforcement Agencies an additional powerful tool. We approached the matter from a purely software engineering point of view, and, when we became technically successful, our customers gave us guidance on how to improve and enlarge the spectrum of the platform's usage, always keeping in mind that any information collected had to be usable as proper evidence in a court of law.

Future Challenges

A recent TOR statistic chart published by the Oxford Internet Institute about the anonymous internet shows that Italy was the biggest user.

A recent TOR statistic chart published by the Internet Geographies at the Oxford Internet Institute about the anonymous internet shows that, in 2014, Italy was the biggest user of such an anonymity platform. Honestly, I do not know what it means and can only speculate. Certainly, I can see a common technical field between Cyber Security Electronic Surveillance and Lawful Interception: continuous R&D, investment in national small/mid cap innovative company (mentioned by Senator Bockel), international cooperation, public/private integration, technology standardization, specific training, and global awareness are crucial factors for the future. I personally believe that going through a baby steps approach, as mentioned by ENISA panelist Dr. Steve Purser, is probably the best and most practicable approach.

Sources:
Marta Serafini – "Maria Giulia che divenne Fatima" – ISBN 9771825788817
TeleStrategies ISS World 2015 Washington, DC
Oxford Internet Institute – University of Oxford

Afghan Peace Prospects

Ambassador Omar Samad
Ambassador of Afghanistan to Belgium, former Senior Advisor to Afghanistan's Chief Executive Officer

The Afghan Security, Political and Economic Transition of 2014

The peace prospect for Afghanistan is a topic that covers a very wide region from North Africa to South Asia and includes Afghanistan. Afghanistan was supposed to be a passé issue after 2014. It is not—not only is it not passé but it is now encountering new forms of threats. A classic one, which the Afghans have seen for the past twenty years, is in the form of the Taliban. Now, small cells of ISIS or Daesh, whatever you wish to call them, are emerging in certain parts of the country. For the past eight years or so, we also have had the presence of Pakistan's Taliban (TTP). They are fighting the Pakistani government but have paid allegiance to the late Mullah Omar and roam between Pakistan and Afghanistan. They are fractured as are all the Afghan Taliban. As of today, the Afghan Taliban have pledged allegiance to two groups after the untimely death of Mullah Omar—untimely for those who had negotiated on his behalf until July of 2015 and who had duped everyone from Afghanistan to London and Washington. Now, we can see that the Taliban are not consolidated, which may be a positive blessing on the one hand, but it seems to make our efforts to combat terrorism and bring peace to the Afghan people after all these years more difficult. Afghanistan remains a focal point as much as we do not want to talk about it. This is why President Obama recently announced that his decision to end the mission in Afghanistan around 2016 is not going to happen, and he will "pass the buck" to the next American president. He plans to keep 10,000 U.S. troops and a few thousand NATO troops until the end of 2016, subsequently bringing the numbers down to 5,500 and leaving the next decisions to the new American leader.

"Afghanistan was supposed to be a passé issue after 2014...but it is encountering new threats."

What does this mean for the Afghan people and for the one-year old Afghan government after the complex and somewhat disorderly reign of Mr. Karzai who, for the last four or five years of his presidency, tried to play politics with strategic issues and almost took Afghanistan to the brink of civil war? Afghanistan would have fallen into civil war without the formation of a national unity government—the 2014 election that saw the amazing turnout of Afghan men and women embracing democracy, saying no to the Taliban, and going to vote for a transfer of power from Karzai to someone else—and without the shameful fraud that took place under Mr. Karzai's watch and involved many other players. So, there are many lessons to be learned, but what saved the day was the formation of a government headed by the two leading candidates, which is a difficult experience given the situation in Afghanistan. But the good news is that both President Ashraf Ghani and Chief Executive Abdullah are trying their best to work as a unified government and deal with the tremendous challenges that exist after the 2014 transition. If you remember, the transition was not just a security transition, the ending of a combat mission and the longest war for the United States; it was also a political transition that almost turned into a disaster; and it was an economic transition that is hurting the Afghan people and causing the exodus of hundreds of young Afghan men and families from the country because of a sense of uncertainty about the future, even though the government is trying very hard. Mr. Obama has given reassurances, NATO has given reassurances, the international community continues to help and is committed to helping Afghanistan, probably all the way until 2024. Yet we are still facing issues.

"...the good news is that both President Ashraf Ghani and Chief Executive Abdullah are trying their best to work as a unified government"

The Important Remaining Issues: Security and Debunking the Facts

Security. The biggest one, of course, is security. Security today does not look like just us versus the Taliban but it is us versus all the other elements that I mentioned earlier, including Daesh. The good news is that the Afghan forces have proven to

be resilient and very effective, especially our special forces. Afghan special forces have done an amazing job over the last few months to make sure that the Taliban cannot hold on to any territory. This includes the fall of the important province of Kunduz in October which we retook from the Taliban but turned out to be a symbol of weaknesses in the system. The fall of Kunduz should not have happened but it did happen for several reasons: One was Mr. Karzai's policies for the past four or five years of not allowing night time raids, special operation raids, aerial bombardments etc. by US or Afghan forces. Then, Mr. Karzai released thousands of Taliban—known terrorists that had been held in prison since 2011 and 2012—under the pretext that there were innocents among them. Perhaps there were a few innocents but we know for a fact that these people were predominantly caught on the battlefield. Where did they end up and who orchestrated this strategy to bring them back and create a challenge for the new Afghan government? Unfortunately, the answer lies in our neighborhood, in Pakistan, as it has for years. While we deal with the Afghan problem, we are not dealing with its source, which lies across the border with Pakistan. Pakistan hid Mullah Omar's death for two and a half years. Even American intelligence was not 100% sure about his death. Our own intelligence was 100% sure of it but Pakistan played that card, making everyone believe that peace could come under Mullah Omar's tenure to pursue their own strategic interests at the expense of Afghanistan. The plan backfired when it was revealed and peace talks were stalled. To this day, the Afghan government and people are unwilling to go back to the table until and unless Pakistan proves its credentials, its sincerity, and we are first able to build trust. We are no longer in a hurry to sit at the table with people who do not represent a significant part of the nation and who are based in Pakistan.

> **"...the answer lies in our neighborhood, in Pakistan, as it has for years"**

> **"We are no longer in a hurry to sit at the table with people who do not represent a significant part of the nation and who are based in Pakistan."**

Debunking a Few Facts. Some serious strategic assumptions and theses that were held true over the last decade have proven to be wrong today. Even by any stretch of the imagination, the thesis that the Afghan conflict is a civil war cannot have any credibility. 99.9 % of the population is on one side and the other .1% or .2% is on the other side. That is not a civil war. It is not an ethnic war either. There may be some ethnic politics involved but there is no ethnic issue in the conflict. Let us not forget that today, the Afghan constitution allows every Afghan citizen regardless of creed, ethnicity, or political persuasion, to be part of the new Afghanistan. The Taliban are welcome if they come as normal citizens. Secondly, on the thesis that the Taliban are nationalists fighting against a foreign invasion, we must remember that the Taliban have been fighting against other Afghans since 1995 and before 9/11 when they emerged from Madrasas. So it is incorrect to say that the Taliban are nationalists fighting a foreign invasion. Some people say that the Taliban are not the enemy, not terrorists, and only Al-Qaeda is the enemy. Yes, there are differences between the Taliban and Al-Qaeda but these differences are minimal and, at the end of the day, they will support each other and merge to create a bigger force when that day comes. Three weeks ago, the largest Al-Qaeda underground center of operations inside Afghanistan was detected and eliminated along Pakistan's border near Spin Boldak in the South. It was the largest center ever found in the country since 2001 and Afghan and US intelligence show that dozens of Al-Qaeda and Taliban operatives were working together in this center. The information that we captured is being analyzed now. It shows what the Al-Qaeda Taliban (LashkaTaiba), the Uzbek Islamic movement (IMU), the Chinese Islamic movement, the Tajik Islamic movement, Pakistan's TTP, are doing together and planning to destabilize Afghanistan. This could not have happened without some type of foreign facilitation and it is a real example that I am giving you just as of a few days ago. What you can see is a situation that needs to be managed differently and the hope is that we have all learned the hard lessons. We all want the Afghanistan dossier to be closed, peace to return to this country, foreign troops and advisers to go back home, but this situation is part of a much bigger scenario. As I said earlier, it stretches from North Africa to South Central Asia. We need new thinking, new strategies and new measures to combat this in all its different forms. We also need to understand that, despite their differences—they may look different, they may speak different languages—these groups share common threads.

> **"Al-Qaeda Taliban, the Uzbek Islamic movement, the Chinese Islamic movement, the Tajik Islamic movement, Pakistan's TTP, are working together to destabilize Afghanistan."**

The Importance of Countering Nuclear Proliferation

Dr. Andrew May
Associate Director, Office of Net Assessment, Office of the U.S. Secretary of Defense

Let me say first that I am really speaking for myself here. I do work in the office of Net Assessment in DOD but my views are my own and, in a lot of cases, they probably run counter to official US policy; so do not associate them with those of my friends at the State Department or even at DOD.

I would like to talk briefly about the possibilities that the future may be a much different and more nuclear future than most people tend to think. What strikes me is the long list of speakers attending this two-day workshop who are here to talk about cyber and I worry that if we wanted to assemble a similar group to talk about the nuclear future, we could not find half as many people. In my own view, nuclear weapons will continue to be a very important part of international affairs and of the nature of conflict. They cut across the three different main pillars that we discussed today. If we think about Russia and the contest with NATO, we are likely to find that nuclear weapons may be part of that. If we think about the Middle East and the prospect of increasingly powerful non-state actors and state actors, we may find that nuclear weapons are also injected into that context. And as we talk about cyber, there is a sort of loose association where people start to talk about cyber as WMD. I think that this is a line that should be gone down very carefully; we do not know yet about cyber but WMD 1.0, so to speak for you cyber people, as nuclear weapons is a very serious threat and a very serious concern.

> **"Nuclear weapons will continue to be a very important part of international affairs and of the nature of conflict."**

There is one way I see nuclear weapons coming back into prominence in our discussions and it is potentially driven by some existing nuclear powers that, for various reasons, need to make their weapons more usable. I am not talking about giant city busting weapons, I am talking about countries with relatively small populations compared to the geography they feel they need to defend that are facing potential opponents who seem to be superior in the conventional arena. They are starting to look at scenarios in which they may need to use nuclear weapons, perhaps even on their own territory. They do not want these weapons to be the end of days but they want weapons they can use, they can fight with, and that the territory on which they fight can still be useful some day. It will not be Chernobyl. I believe that such weapons are a technical possibility. You can begin to imagine scenarios in which a country uses such weapons in a military circumstance to solve their military problem, not unlike the first use of atomic weapons solved a military problem of the United States. The reaction of the world to the first use of these weapons was not condemnation, it was envy, and it is not impossible that the response to the second use will not be condemnation but envy as well. If a country is able to use those weapons in a way that is military efficacious, it is at least possible, if not likely, that other countries may say, "Look what they did, they solved their problem, which is not dissimilar to ours. We would like some of those kinds of weapons to solve problems that we may have in the future." In the wake of the next nuclear use, we may find a rapid proliferation of a very different kind of nuclear weapon, a cleaner weapon with a smaller yield that is deliberately designed to be militarily useful. We may find nuclear weapons right back on the table as a militarily attractive solution to military problems.

> **"We may find a rapid proliferation of a very different kind of nuclear weapon, a cleaner weapon with a smaller yield, deliberately designed to be militarily useful."**

> **"One thing is sure: refusing to think about this is not going to help."**

I think it is much too soon for us to start talking about what we can do to stop such a world from happening, or what we would want to do with such an environment, how we would adapt our militaries to it. It is very likely that existing nuclear powers may find that their ways of thinking about nuclear weapons and nuclear arsenals are very inappropriate for that kind of world and there is a real potential that they will find themselves flat-footed. One

thing I can be sure about is that refusing to think about this is not going to help. If we cannot think about how to stop such an environment yet and how we want to react to it, at the very least we can be spending time in circumstances like this workshop to think about what that world might look like.

As a consequence, we might think about what sorts of policies, programs, and capabilities the militaries of the West might want so that we do not lose any more ground than we have to in such a circumstance.

Cyber Propaganda and Cyber-enabled Terrorism: *Countering Online Extremism*

Ingénieur Général Daniel Argenson
Deputy Director, Institute for Higher Defense Studies (IHEDN)

Given the growing role of cyber propaganda and cyber-enabled terrorism, I would like to say a few words about countering online extremism. Anyone who has the good fortune to live in a democracy knows that whenever such issues are raised, it always comes to a debate opposing security on the one hand and privacy rights on the other. Today, the internet and social media are fully part of both our professional and private lives, and this is particularly the case for younger generations: everyone here will probably agree that trying to limit the social media access of our teenagers might cause a revolution!

Our democracies are making good use of these social media tools, including for marketing purposes, and this is generally well accepted by our public opinion. So it should be no surprise if other organizations, perhaps state or non-governmental ones, also use these tools in more or less the same way—although not necessarily with good intentions. In some cases, these tools may even be part of a hybrid war. Indeed, Daesh is now able to deliver its propaganda very professionally and recruit young foreign fighters in our democracies by using these tools in the same way that Hollywood makes movies. When it comes to defense and security, this new paradigm does away with borders. During the opening training session at IHEDN, the institute to which I belong, French Prime Minister Manuel Valls said that we are facing a new enemy who ignores borders and uses all means at his disposal. Similarly, David Thompson, a French journalist, described Jihadists as fighting with a Kalashnikov in one hand and a smart phone in the other.

"French Prime Minister Manuel Valls said, "We are facing a new enemy who ignores borders and uses all means at his disposal."

So these are the facts and other speakers on our panel will try to go deeper into this analysis and perhaps give us some pointers on the way to proceed. We must face this issue with more than traditional means—such as military operations, intelligence, or other things we are accustomed to discussing—by using the same kind of tools that Daesh are using. Of course, we will not be able to address this problem completely without also trying to understand the reasons why young people who live in peace in democracies can be radicalized. The answer requires a multi-dimensional and cross-disciplinary approach that includes defense and security, but also social analysis and a response to questions such as: "Are those young people victims or executioners?" and "Are they hostages or targets?" We need to answer such questions if we want to fully address this difficult issue

"We will not be able to address this problem completely without also trying to understand the reasons why young people who live in peace in democracies can be radicalized."

Countering Online Extremism: The Need for a Comprehensive Approach

Dr. Frederick Douzet
Castex Chair of Cyber Strategy, Institute for Higher Defense Studies (IHEDN)

Countering online extremism is definitely a very complicated issue and there is no simple answer, so I will just focus on two points. First, I would like to emphasize the need for a comprehensive approach to fight online propaganda and extremism and second, explore how research can help the discussion, how it can help get a good diagnosis of the situation and also provide good answers.

Why do we Need a Comprehensive Approach?

As a professor of geopolitics and the chairwoman of the Castex Chair of cyber strategy, my background and research are multi-disciplinary. I have done a lot of work in urban studies and cyber studies and interestingly, this issue brings together my different fields of expertise. Therefore, the timing of last month's events really struck me because, in order to fight the consequences of radicalization—meaning terrorist attacks—a decision was made in October to increase random checks by the police in public transportation. From a security perspective, this seems like an important message to send to reassure people. But this same month of October, a decision from the Court of Appeal on racial profiling condemned the French state and, again during the month, we had the 10th anniversary of the 2005 urban riots in France. I remember well teaching in a sub-urban university at the time and seeing the tensions building up month after month. I was teaching a course in American civilization and discussing segregation, discrimination, confrontation between minorities and the police and how complicated it was. Most of my students' reactions were that they could not go to Paris without having their papers checked at least four or five times. They felt a lot of resentment because the message they were receiving was that they actually did not really look French.

> **After the 2005 riots, students from the suburbs resented not being able to go to Paris "without having their papers checked at least four or five times."**

> **They resented the message that they "actually did not really look French."**

How does this relate to online propaganda and radicalization? I think that propaganda works on people who are somewhat receptive. It works both ways and we must work on both ends of the spectrum by countering the message, but also understanding why these young people are receptive to this message and what we can do about it. This is not easy because we are not talking about the same timeframe: stopping the action of terrorism is an emergency while it takes more time to work on its cause. At least we need to make sure that while we work on the consequences of this propaganda, we do not make the cause worse, and in the context of fighting online propaganda, we do need to put the emphasis on countering the message. Countering a message, however, is not just a matter of social media or doing great TV commercials. Random police checks also do send a message but if they are not done properly, they can send a terrible message. So huge efforts are required to train the workforce so that the checks are actually random.

I believe this is an important point. It is just one example among others, and I am well aware that there are many different causes as to why propaganda is effective on these young people. I am just pointing out the idea that we also need to fight the sigmatization of Muslims in public and media discourses because fighting that stigmatization will weaken the propaganda message. So we need a comprehensive approach, first to make sure that while we treat the symptoms, we do not aggravate the cause and second,

> **"We also need to fight the stigmatization of Muslims in public and media discourses."**

because countering online propaganda and extremism requires coordination of both online and offline action. We cannot solely see these issues through a security perspective.

This somewhat resonates with what Admiral Coustillière was saying about the need to fight cyber attacks by developing specific cyber actions and also integrating that dimension into all other forms of combat—in this case, all other forms of political action. He also mentioned that we must remain very modest about this. So a comprehensive approach is important as a way to identify the right targets, tools, and vehicles that will convey the message both online and offline. It is also important in order to identify where and when there should be government communication and what other actors might be involved in countering the message. Finally, it is important to involve the right set of people for support and expertise, for example, for facilitating the creation of online resources and exploiting what networks have to offer in order to deconstruct discourses. And of course, it is important to address the causes, however complex and multiple they may be. I must admit that this is easier said than done.

How Can Research Help?

Academic research can help establish a diagnosis to elaborate a strategy and provide some tools. There is a lot to be learned from communication sciences and it is very clear that Daesh is using the latest communication strategies from a broad group of fields such as psychology, sociology, or security studies. In geopolitics, we emphasize the spatial context and the actors' strategies. We have an ongoing project to understand the propagation of online propaganda. How can we map it? How can we identify the links, nodes, patterns of diffusion of the message through, for example, the analysis of a selection of tweets and twitter accounts? The idea is to understand the operational nodes and links between actors in order to be able to act upon them. If we are able to get the data from Twitter, we will have to geolocalize this information to cross it with the territorial data from geographic information systems we obtained from all the studies we have done in field work. This will help us understand the spatial organization of this propaganda diffusion.

> **"How can we map Daesh's communication strategy? How can we identify the links, nodes, patterns of diffusion of the message through the analysis of tweets and twitter accounts?"**

Another project that would be very interesting and, here, access to data is also key, is understanding the geography of radicalization through the analysis of the spatial context in which those who have left for Syria were raised. Again, this is one factor among others, but through the spatial context, we do have a lot of indicators that might help understand how we can act and where we should concentrate our forces in a context of scarce public resources. Spatial context matters and if we could get anonymized data for the young people's last residence before leaving for Syria, we could cross them with a huge number of territorial indicators and perhaps draw some lessons about what we can do. Both projects would lead to a better understanding of what places we need to target through counter-propaganda and what other kinds of actions we could take to decrease the level of receptivity to the message that Daesh is broadcasting. Again, we are in a context of shrinking public budgets in which government services are often swamped with emergencies to deal with. So it would be very easy to "bribe" academics with data they would be delighted to work with for free.

> **We should study the geography of radicalization by analyzing the spatial context in which those who have left for Syria were raised.**

Les stratégies de contre-discours sur Internet : La campagne Stop Djihadisme

Monsieur Christian Gravel
Préfet, Directeur du Service d'information du Gouvernement (Premier ministre)

Investissement de l'Etat français dans le cyberespace et les réseaux sociaux

Dans son « opus magnum », le théoricien djihadiste syrien Al Souri affirme que « le combat dans la voie de Dieu est un ensemble réunissant sur un même plan : opérations politiques, militaires et médiatiques. » L'enjeu de la domination informationnelle est aussi important que celui de la victoire par les armes létales. Elle permet de susciter des recrutements, de retourner ou d'agréger des opinions, de casser ou, au contraire, de galvaniser des troupes. L'impact de la mise en scène d'une tête décapitée est plus élevé que celui—plus classique—d'une bombe ayant causé des dizaines de morts. Sur ce nouveau théâtre opérationnel, les belligérants s'affrontent pour exercer une emprise sur les esprits et défendre leur vision du monde.

> **L'enjeu de la domination informationnelle est aussi important que celui de la victoire par les armes létales.**

Aujourd'hui, les réseaux sociaux constituent des sources majeures d'influence et le web est devenu de facto le "5ème champ de bataille" (après la terre, la mer, l'air, la stratosphère) pour reprendre l'expression de Daniel Ventre. Cette lutte d'influence s'inscrit dans un contexte marqué par la révolution numérique qui a bouleversé la capacité de conviction des États : l'explosion des flux d'information et, surtout, de désinformation; la substitution du modèle classique vertical (top down) par un modèle désormais horizontal, où chaque expression se vaut, a réduit la capacité des émetteurs légitimes traditionnels à imposer leur point de vue, surtout dans un contexte de crise politique profonde et de contestation idéologique; enfin, la croissance exponentielle de circulation des théories complotistes et conspirationnistes sur la toile nécessitait, plus que jamais, un investissement de l'Etat dans ce cyberespace qui n'a pas vocation à se laisser phagocyter par les thèses les plus extrémistes et anti-démocratiques.

La puissance publique doit devenir un acteur offensif, actif, performant sur le même terrain que celui de nos ennemis qui maîtrisent parfaitement les codes d'une communication moderne et attractive, sans parler de leur avance dans ce processus. Les organisations terroristes ont, largement, un coup d'avance. Elles ont considérablement professionnalisé leur stratégie de communication au cours des 20 dernières années. Le modèle de propagande de Daesh des années 2010 n'a rien à voir avec le modèle d'Al Qaïda des années 90. En maîtrisant les codes modernes de la communication occidentale, elles ont renforcé leur impact auprès des cibles visées en Occident et créent sur la toile le sentiment d'une communauté virtuelle qui dépasse toutes les frontières.

> **La puissance publique doit devenir un acteur offensif, actif, performant sur le même terrain que celui de nos ennemis.**

Première campagne de communication : une plateforme et une vidéo

Le gouvernement Français devait, en toute logique, investir ce terrain étant donné l'importance du phénomène des départs en Syrie et en Irak. C'est dans ce cadre qu'est né notre projet « Stop Djihadisme ». Lancée en janvier 2015, quelques jours après les tragiques attentats perpétrés en France, cette campagne de communication pose le premier jalon du contre-discours des autorités françaises. Conçue en étroite concertation entre le Service d'information du Gouvernement (SIG) et le ministère de l'Intérieur, elle repose sur deux principaux supports : une plateforme et une vidéo.

> **La campagne de communication, « Stop Djihadisme », pose le premier jalon du contre-discours.**

La plateforme « www.stop-djihadisme.gouv.fr » vise, d'abord, à informer l'ensemble de nos compatriotes sur la menace terroriste. Par des outils pédagogiques (infographies, témoignages), elle invite chacun à la mobilisation et à la vigilance. Son contenu est régulièrement actualisé : en octobre dernier, la parole y a été donnée à des familles dont les proches sont partis en Syrie ; cet hiver, elle sera également ouverte à celles de réfugiés syriens ayant fui Daech. Cette plateforme veut, aussi, être une ressource pour les parents qui s'inquiètent de la dérive de leur enfant. Un numéro vert d'appel téléphonique, géré par l'Intérieur, et des formulaires en ligne sont alors mis à leur disposition pour alerter les autorités publiques, en toute confidentialité, afin de pouvoir bénéficier, au niveau local, d'un accompagnement global de l'Etat (social, éducatif, psychologique).

Parallèlement, le clip vidéo « Stop Djihadisme » a été diffusé largement sur le web. Son parti pris est d'opposer frontalement les mystifications de la propagande aux réalités du terrorisme. Par son montage rapide et ses images violentes, il cherche à éveiller le sens critique des jeunes fascinés par la « sous-culture » djihadiste ou trompés par la rhétorique humanitaire mais, surtout, à susciter un choc auprès de l'entourage du jeune concerné pour prendre conscience des mécanismes d'embrigadement de l'organisation terroriste. Enfin, son objectif est de contrecarrer les formes soft de la propagande djihadiste qui circulent principalement sur Twitter ou Facebook. « Stop Djihadisme » a touché un large public. Le clip a été vu plus de 2 millions de fois et a surtout permis un doublement du nombre de signalements via le numéro vert.

Le clip « Stop Djihadisme » a permis un doublement du nombre de signalements via le numéro vert.

Depuis l'été dernier, le Gouvernement travaille au déploiement de la deuxième phase de sa campagne. Si le succès de la première est réel, ses limites sont, en effet, toutes aussi évidentes. Combattre la propagande djihadiste exige d'occuper le terrain numérique, chaque jour, avec de nouveaux contenus. La saturation de l'espace digital est aussi l'un des enjeux de la lutte. Il est donc, d'abord, indispensable d'augmenter considérablement le volume de notre contre-discours. Mais il ne suffit pas d'atteindre la « masse critique ». Il faut également affiner nos messages au plan qualitatif.

Deuxième phase de la campagne de communication: « Bataillons de community managers »

Pour être efficace, un contre-discours doit, en premier lieu, « coller au plus près » le discours qu'il combat. Or la propagande djihadiste est très mobile et protéiforme. Si elle utilise souvent le masque de l'engagement humanitaire, elle n'hésite plus à faire des atrocités commises des éléments de promotion.

De la même manière, le contre-discours doit toujours rester adapté au public qu'il vise. Or les profils des candidats au djihad sont très variés. Du jeune exalté en quête de rédemption au fou sanguinaire en quête d'ultra-violence, le spectre est large. Il couvre l'ensemble des pathologies sociales, religieuses et psychiques. Enrayer la radicalisation des individus exige donc, à chaque fois, de faire du « sur-mesure ». Comme le fait Daech.

Pour garantir la force de leur contre-discours, les autorités publiques doivent impérativement trouver des appuis et des relais au sein même de la société civile. Une large partie des personnes visées par la propagande djihadiste est, par définition, imperméable à toute parole officielle. Imbibées de thèses complotistes sur Internet, elles n'accordent plus aucun crédit aux messages portés par l'Etat, incarnation suprême du fameux « système » à la solde des judéo-maçons-réptiliens !...

Sur la base de ce constat, le Premier ministre, Manuel Valls, a donc annoncé sa volonté de déployer, sur Internet, des « bataillons de community managers » d'ici la fin 2015. Par leur nombre, ils seront en mesure de répondre chaque jour, coup pour coup, aux messages djihadistes. Par leur diversité, ils seront à même de toucher chaque cible. Le Service d'information du Gouvernement a reçu la mission de piloter—en lien direct avec les principaux ministères concernés—la mise en place de ces bataillons. Les community managers pourront s'appuyer sur les travaux d'un comité scientifique regroupant des experts sur le sujet, en bénéficiant de leur savoir en sociol-

Le Premier ministre a annoncé sa volonté de déployer, sur Internet, des « bataillons de community managers ».

ogie, en histoire, en psychologie et en théologie. Chaque volet de la propagande ennemie doit être démonté, décrédibilisé, vidé de sa substance.

Au-delà de l'esthétique de l'horreur produite par Daesh, du poids des images exploitées sous toutes ses formes, la force de l'organisation est de produire un récit reposant sur une vision simpliste de l'Histoire, sur une rhétorique du sens faisant appel aux aspirations naturelles de chacun, à travers leurs rêves, leurs espoirs, leurs fantasmes dans le cadre d'un projet de société idéal. Ces mots touchent d'autant plus précisément que la cible est fragile : jeune voire très jeune, en difficulté sociale et/ou psychologique. Le chemin qui leur est proposé donne un sens à leur vie. C'est la raison pour laquelle la production d'un contre-récit constitue un enjeu majeur. Permettre à l'Etat de replacer chacun dans une trajectoire collective s'inscrivant dans des valeurs fondamentales, et ne pouvant tolérer le moindre compromis avec les droits fondamentaux. Ce combat de LA civilisation contre la barbarie ne doit naturellement pas tomber dans le piège tendu par les djihadistes, ou autres salafistes, du « choc des civilisations ». Il ne s'agit surtout pas d'organiser une parole « contre » mais bien un discours « avec », permettant d'envisager une vie de la multitude se fondant dans l'unité de la République, fidèle à sa grande Histoire.

Le chemin qui leur est proposé par le djihadism donne un sens à leur vie.

Réhabiliter un système de valeurs qui transcende les différences et répond aux aspirations d'une jeunesse qui ne trouve pas sa place

Le défi auquel nous sommes confrontés n'est pas exclusivement sécuritaire. Parce qu'il est global, il est hautement politique. Puisqu'il s'agit bien de « refaire la société » à travers un projet de vie, s'appuyant sur une vision du monde lucide nécessitant de nouvelles solutions face à une partie de la jeunesse qui ne trouve pas sa place. Il s'agit de répondre à l'aspiration d'une partie de notre population en quête de sens, de reconnaissance, d'identité. Tout repose sur la réhabilitation d'un système de valeurs transcendant les différences individuelles, communautaires, culturelles. L'objectif de cette contre-narration est bien de diffuser largement des messages à caractère positif permettant d'envisager la concorde après avoir démonté, un à un, l'ensemble des leviers d'enrôlement.

Nous ne terrasserons pas le mal sans établir un diagnostic intégral et affronter toute la vérité en face.

Le Gouvernement français est pleinement mobilisé dans la lutte contre le terrorisme islamiste. Mais—aussi fort soit-il—son engagement ne suffira pas pour vaincre, si ce combat n'est pas l'occasion d'un examen de conscience général. La radicalisation djihadiste n'est pas, en effet, un épiphénomène conjoncturel. Elle est, au contraire, l'expression de crises structurelles de notre époque. Nous ne terrasserons pas le mal sans établir un diagnostic intégral et affronter toute la vérité en face. Le terrorisme islamiste nous confronte à des questions politiques et sociétales majeures : Qui sommes-nous ? Où voulons-nous aller ? Telles sont aujourd'hui les interrogations lancées à la face de l'Islam et de l'Occident.

L'Islam est une grande religion. Ses apports à la culture universelle sont précieux, au même titre que ceux des autres monothéismes. Amalgamer l'Islam à l'islamisme, assimiler la foi à la démence, chacun d'entre vous le sait bien, c'est sauter à pieds joints dans le piège tendu par les apôtres de la guerre des civilisations. Que cette dimension soit une simple couverture ou qu'elle soit un véritable ressort, en réalité, peu importe. Comme le rappelle avec force le philosophe soufi Abdennour BIDAR, une terrible question reste posée à l'Islam : « pourquoi ce monstre ignoble a-t-il choisi ce visage et pas un autre ? » Selon le même auteur, ce masque ne pourra lui tomber du visage que lorsque l'Islam reconnaîtra pleinement le « droit à la liberté vis-à-vis de la religion », en s'attaquant aux racines du mal d'une radicalité politique bien éloignée de toute forme de spiritualité authentique.

Face au péril islamiste, la responsabilité de l'Occident est toute aussi grande. Qu'ils aient choisi le modèle communautariste à l'anglo-saxonne ou le modèle républicain à la française, nos pays sont confrontés aux mêmes problèmes plus ou moins graves d'intégration ou de violence. Or le sentiment de relégation sociale est un puissant facteur de radicalisation pour les jeunes. Les pouvoirs publics et la société civile doivent donc se mobiliser, sans relâche, pour leur ouvrir un avenir sur notre

« La civilisation du supermarché » crée ainsi « le sentiment de toujours manquer la part essentielle de la vie ».

sol. Mais, en vérité, notre tâche est plus vaste encore. Elle dépasse le plan social et englobe le plan culturel. Notre modèle consumériste génère, de manière simultanée, jouissances matérielles et insatisfaction existentielle. « La civilisation du supermarché » crée ainsi, comme l'explique le philosophe Gilles Lipovetsky, « le sentiment de toujours manquer la part essentielle de la vie ». Au problème d'intégration s'ajoute donc, plus profond, un problème d'aspiration.

Engagés l'un et l'autre dans la lutte contre l'islamisme, l'Islam et l'Occident se tendent chacun un miroir. D'un côté, certains regrettent une religion sans liberté. De l'autre, certains déplorent une liberté sans horizon. D'un côté, le reproche d'une confusion entre spiritualité et soumission. De l'autre, celui d'une confusion entre plénitude et consommation. D'un côté, le trop plein de sens. De l'autre, le vide sidéral. De ces situations opposées se dégage pourtant une solution commune : celle d'une transformation culturelle de l'un et l'autre. Ou, pour dire mieux encore, celle d'une élévation spirituelle de l'un par l'autre. C'est bien là, il me semble, le véritable enjeu qui nous réunit aujourd'hui et qui devra nous animer demain.

Counter-communication Strategies on the Internet: The "Stop Djihadism" Campaign

Mr. Christian Gravel
Préfet, Director of the Government Information Office (SIG), French Prime Minister's Organization

The french investment in cyberspace and social networks

In his "opus magnum," Syrian theoretician of dijhadism Abu Musab al-Souri declares that "the combat to follow God's path combines at the same time political, military, and media operations." The stakes for "information dominance" are fully as important as achieving victory by lethal weapons. Information dominance makes it possible to facilitate recruiting, turn around or strengthen opinions, discourage—or on the contrary—galvanize troops. The media impact of a decapitated head is stronger than the more classic effects of a bomb causing dozens of deaths. In this new operational theatre of information, the fighters seek to achieve control over mindsets and to defend their vision of the world.

The stakes for "information dominance" are fully as important as achieving victory by lethal weapons.

Today, the social networks constitute major sources of influence and, to quote cyber conflict specialist Daniel Ventre, the web has become de facto the "fifth field of battle" (after land, sea, air, and space). This battle for influence is taking place within the digital revolution and has affected the credibility of states. Both the explosion of information, particularly disinformation, and the substitution of the classic vertical model (top down) of influence by a model that is now horizontal, where every expression of opinion is considered to be of equal value, have reduced the power of legitimate and traditional sources of information to impose their points of view. This is especially true in the context of profound political crises and ideological conflicts. Finally, the exponential spread over the internet of conspiracy theories requires, more than ever, an investment in cyberspace by the State, which should not be undermined by extreme and anti-democratic ideologies.

The State must become an energetic and offensive actor operating on the same terrain as that of our enemies.

The State must become an energetic and offensive actor operating on the same terrain as that of our enemies who control the codes of modern persuasive communication perfectly, and benefit from a technical advance that they have developed on their own.

The first communication campaign: a platform and a video

Logically, the French government had to invest in this area given the significance of the phenomenon of fighters and others leaving for Syria and Iraq. Our project, "Stop Djihadism," follows this logic. Launched in 2015, a few days after the tragic attacks that were perpetrated in France, this campaign is the first step in counter-communication by the French authorities. Conceived in close collaboration with the government's information service (SIG) within the Interior Ministry, it rests on two principal elements: a platform and a video.

The campaign,"Stop Djihadisme," is the first step in counter-communication by the French authorities.

The platform, "www.stop-djihadisme.gouv.fr," seeks to inform our countrymen about the terrorist threat. With its pedagogical tools (including infographics and testimonies), it encourages all of us to be prepared and vigilant. Its contents are regularly updated: last October, the spotlight was given to families whose members had left for Syria; this winter, it will

be given to refugees from Syria who fled Daesh. The platform is also a resource for parents who are concerned about the behavior of their children.

In parallel, the video clip "Stop Djihadism" has been diffused widely over the Internet. Its goal is to directly confront the mystification of propaganda with the reality of terrorism. With its compelling collection of violent images, it seeks to awaken the critical sense of the youth who may be fascinated by the "sub-culture" of Djihadism or deceived by its humanitarian rhetoric, but above all to create a shock among those who are close to the youth concerned—in order to create an awareness of the recruiting mechanisms that are used by the terrorist organization. Finally, its objective is to counterbalance the "soft" forms of Djihadist propaganda that circulate principally on Twitter, Facebook, or Youtube. "Stop Djihadism" has reached a large audience. It has been viewed more than two million times and, above all, has led to a doubling of alerts received on the Interior Ministry's special "numéro vert" (toll free) telephone line.

The "Stop Djihadisme" clip has led to a doubling of alerts received on the Interior Ministry's toll-free line.

Since last summer, the government has been rolling out the second phase of its campaign. While the success of the first phase is very real, its limits are also evident. Combating djihadist propaganda requires monitoring the digital terrain every day, with new content. The saturation of the digital space is also one of the elements of the fight. It is therefore indispensable to considerably increase the volume of our counter-communications. But it is not enough to attain a "critical mass." It is also necessary to refine the effectiveness of our messages.

Second phase of the communication campaign: battalions of "community managers"

In order to be effective the counter-message must, first of all, stay very close to the message that it must combat. However, the djihadist propaganda is very mobile and constantly shifting in form. Although it wears the mask of humanitarian engagement, it does not hesitate to use the atrocities that have been committed for promoting its message.

In the same manner, the counter-message must always be adapted to the public that it targets. From the young religious zealot on a quest for holy redemption to the raging mad man seeking extreme violence, the range of threats is wide. It covers the full gamut of social, religious, and psychiatric pathologies. Wiping out individual radicalization thus requires, in every case, a "tailor-made" approach. Just as Daesh has done.

To guarantee the effectiveness of their counter-communication, the public authorities must necessarily seek support in the very heart of civil society. A large portion of those targeted by Djihadist propaganda, by definition, is resistant to any official communication. Intoxicated by internet rumors of conspiracies, they give no credibility whatsoever to messages from the State—the supreme incarnation of the famous "system" governed by the Judeo-Masonic-reptiles!

On the basis of this observation, Prime Minister Manuel Valls has therefore announced his intention to assign "battalions of community managers" to the internet before the end of 2015. Since there will be many of them, they will be able to answer every day, blow-by-blow, the messages of the jihadists. By their diversity, they will be able to reach every target. The information system of the government (SIG) has been given the mission of planning—in direct coordination with the principal ministries that are concerned—the preparation of these battalions. The community managers will be able to utilize the research efforts of a scientific committee that will bring together experts on the subject, and benefit from their knowledge in sociology, history, psychology, and theology. Every element of the enemy propaganda must be dismantled, disproved, and emptied of its substance.

The Prime Minister has announced his intention to assign "battalions of community managers" to the internet.

Even more than the vision of horror created by Daesh and the power of the images it exploits, Daesh's strength lies in spreading a narrative based on a simplistic vision of history, based on a discourse that appeals to the natural aspirations

of everyone, through their dreams, their hopes, and their illusions in the context of an ideal society that Daesh advocates. These words are all the more effective precisely because their targets are vulnerable: those who are young and even the very young, and in social and/or psychological difficulty as well. The path Daesh offers gives a meaning to their life. This is the reason why offering a counter-message is a major challenge—allowing the State to guide everyone in a collective path based on fundamental values, and without tolerating the slightest compromise with fundamental rights. This combat of CIVILIZATION against barbarism must certainly not fall into the trap laid by the djihadists, or other salafists, of the "clash of civilizations." It is certainly not a matter of organizing a message "against" but a message "with," making it possible to imagine a life for the nation based on the unity of the Republic, faithful to its great History.

The path Daesh offers gives a meaning to their life.

Strengthening a system of values that transcends differences and responds to the aspirations of youth who cannot find their place

The challenge that confronts us is not exclusively security. Because it is global, it is highly political. It is a matter of "restructuring society" through a project to reorient lives, based on a clear vision of the world that requires new solutions for the benefit of some of our youth who cannot find their place in society. It is a matter of responding to the aspirations of a part of our populations in search of meaning, of recognition, and of identity. Everything depends on the renewal of a system of values that transcends differences among individuals, communities, and cultures. The goal of this counter-narrative is to spread positive messages as widely as possible in order to be able to foresee a conciliation after having dismantled, one by one, the mechanisms of enlistment."

The French Government is fully mobilized in its fight against Islamic terrorism. But—as strong as its efforts may be—its engagement will not be enough to achieve success, if the combat is not seen as the opportunity for a broadly based examination of conscience. The radicalization of djihadism is not a passing epiphenomenon. It is, on the contrary, the expression of structural crises of our time. We will not defeat the evil without undertaking a full diagnosis and squarely facing the truth. Islamic terrorism confronts us with fundamental political and social questions: Who are we? Where do we want to go? These are the kinds of questions that are being posed today to Islam and to the West.

We wil not defeat the evil without undertaking a full diagnosis and squarely facing the truth.

Islam is a great religion. Its contributions to universal culture are precious, at the same level as other monotheistic religions. Associating Islam with Islamism (or political Islam), confusing faith with madness—every one of us understands this—is like jumping with both feet into the trap laid by the apostles of the war of civilizations. In reality, it doesn't matter whether this dimension is simply a cover or whether it is something more powerful. As the Sufi philosopher Abdennour Bidar forcefully reminds us, Islam must address a terrible question: why has this awful monster chosen this face and not another? According to this same author, the mask can only fall from its face if Islam fully recognizes the "right to liberty of religion" by attacking at its very roots the evil of a political radicalism far removed from any form of spiritual authenticity.

In the face of the Islamist danger, the responsibility of the West is just as large. Whether one chooses the Anglo-Saxon communitarian model or the French republican model, our countries are confronted with the same problems, more or less gravely, of integration and violence. In fact, the sentiment of social rejection by the young is a powerful factor in their radicalization. For this reason, both public authorities and civil society must be mobilized energetically in order to offer young people a future on our soil.

The "civilization of the supermarket" creates "the feeling of always missing the essential part of ones life."

But in reality, our task is greater still. It must go beyond the social level in order to fully encompass the cultural dimension. Our consumerist model generates, at the same time, material pleasures and existential dissatisfaction. The "civilization of the supermarket" thereby creates, as explained by the philosopher Gilles Lipovetsky, "the feeling of always missing the essential part of ones life."

To the problem of integration, it is therefore essential to add a more profound one, the problem of aspiration. Engaged in the fight against Islamism, Islam and the Occident each hold up a mirror to the other. On one side, there are those who regret religion without liberty. On the other side, there are those who deplore liberty without limits. One side reproaches the confusion between spirituality and submission. The other side reproaches the confusion between well-being and consumption. For one side, there appears to be an overflowing of the senses. For the other side, there is the vacuum of outer space. These opposing situations, nonetheless, lead to a common solution: the cultural transformations of both Islam and the Occident. Or, to speak more clearly, there must be a spiritual elevation of one by the other. These are the forces, it seems to me, that we must bring together today and will motivate us tomorrow.

La coopération avec les acteurs de l'Internet : un élément essentiel de l'enquête en matière de cyberterrorisme

M. Jean-Yves Latournerie
Préfet, Conseiller du Gouvernement, chargé de la lutte contre les cybermenaces
Ministère français de l'Intérieur

J'ai été nommé en décembre dernier conseiller du gouvernement, chargé de la lutte contre les cybermenaces. A ce titre, il me revient de proposer et de coordonner la mise en œuvre de la stratégie du ministère de l'intérieur dans ce domaine. Celle-ci comprend bien évidemment l'ensemble des actions menées contre la criminalité numérique, mais également la défense et la protection des systèmes d'information du ministère lui-même.[1]

Aujourd'hui, je m'attacherai particulièrement à évoquer devant vous notre réponse au cyberterrorisme.

La stratégie française de lutte contre les cybermenaces

Cette stratégie de lutte contre les cybermenaces repose sur plusieurs éléments clés. Il s'agit d'abord de bien comprendre la menace, et d'adapter la réponse de nos forces aussi rapidement que possible, afin d'être en mesure de faire face aux crises majeures que connaît notre pays, et dans lesquelles la composante cyber joue un rôle croissant. Le second élément décisif est la qualité de notre coopération avec le secteur privé, de telle sorte que nous puissions : mieux prendre la mesure de la menace ; mieux protéger l'activité économique de nos entreprises, les produits et les services qu'elles délivrent, et les consommateurs ; et enfin, construire ensemble une réponse efficace à ces cybermenaces.

Depuis le début de ma mission, il y a tout juste 10 mois, notre pays a été confronté à un certain nombre d'événements graves qui ont renforcé la conviction qu'une coopération étroite avec les services de télécommunications et les fournisseurs d'accès à l'Internet était absolument nécessaire pour parvenir à identifier les suspects ou pour faire cesser la publication de contenus diffusés dans le but de terroriser la population.

Dans la lutte contre la pédopornographie, « des succès importants ont été obtenus en coopération avec les entreprises du secteur de l'Internet »

Bien entendu, cette problématique n'est pas nouvelle. Depuis de nombreuses années, nous n'avons pas ménagé nos efforts en France, en Europe et partout dans le monde pour combattre la criminalité numérique et lutter contre la diffusion de contenus illégaux, notamment les contenus pédopornographiques qui mettent en scène des victimes bien réelles dans les situations les plus horribles. Des succès importants ont été obtenus dans ce domaine grâce à la coopération avec les entreprises du secteur de l'Internet. Nous ne devons pas pour autant baisser la garde, car il existe malheureusement encore de nombreuses victimes de telles violences, et de nombreux auteurs à identifier et à interpeller. Parmi les contenus illicites, figurent également les discours de haine, qu'il s'agisse de propos ou d'images à caractère raciste, d'incitations à la discrimination, ou de publications diffusant la propagande terroriste ou faisant l'apologie du terrorisme.

S'agissant des cybermenaces dans le champ du terrorisme, le constat se précise ; il est à ce jour le suivant :

- Des signes de plus en plus nombreux indiquent que des actions cyberterroristes sont non seulement possibles, mais intégrées à la stratégie des groupes terroristes. La France est très souvent la cible de groupes favorables à DAESH - fort heureusement avec peu de résultats tangibles à ce jour, se limitant pour la plupart au défacement de sites Internet peu sensibles.

1 Un membre de la commission nationale de l'informatique et des libertés (CNIL) est désigné pour exercer le contrôle de l'application de cette procédure de blocage ou de déréférencement ; les premières procédures de blocage ont été mises en œuvre à partir d'avril 2015, et les premier déréférencements sont intervenus au mois d'août de la même année.

- Cependant, l'attaque subie par TV5 monde en avril 2015 a démontré qu'un certain nombre de nos infrastructures clés sont potentiellement vulnérables aux cyberattaques, notamment lorsque ces attaques visent la destruction des moyens de production de leur cible.

- La France est également l'une des cibles les plus importantes du cyberdjihadisme, avec des contenus spécifiquement adaptés aux communautés de langue française et aux habitudes culturelles de notre jeunesse. Ces messages sont conçus pour favoriser le recrutement, mais également pour atteindre le moral de nos populations.

La lutte contre les contenus illicites

J'en viens maintenant à la lutte contre les contenus illicites. En effet, la France a récemment renforcé significativement sa capacité de réponse à la diffusion de tels contenus :

Une législation précise. La loi de 1881 sur la liberté de la presse décrit précisément les catégories de contenus qui ne relèvent pas de la liberté d'expression et qui ne sont pas socialement acceptables. Dans les cas les plus graves, ces infractions peuvent être poursuivies comme des crimes ou délits de droit commun, y compris en ayant recours à diverses procédures telles que la comparution immédiate, et sont passibles de peines allant jusqu'à trois ans d'emprisonnement. S'agissant de la pédopornographie, mais aussi, depuis la récente loi du 13 novembre 2014, de l'apologie du terrorisme, la publication de tels contenus sur Internet constitue une circonstance aggravante, qui porte le maximum de la peine encourue à 7 ans d'emprisonnement. Lorsqu'un contenu illicite relatif au terrorisme ne peut pas être retiré, la même loi a introduit la possibilité d'en bloquer l'accès ou d'obtenir son déréférencement dans les moteurs de recherche , comme c'était déjà le cas s'agissant des contenus pédopornographiques.

« Les fournisseurs d'accès à Internet et les hébergeurs ont l'obligation de mettre en œuvre un service de réception des notifications des contenus illicites »

La responsabilité des fournisseurs d'accès à Internet. Les fournisseurs d'accès à Internet et les hébergeurs ont l'obligation de mettre en œuvre un service de réception des notifications ou des signalements des contenus illicites ; l'association nationale des fournisseurs d'accès et de services Internet (AFA[2]) fournit un tel service pour le compte de ses membres et participe au réseau INHOPE.

La plateforme nationale PHAROS. Toute personne peut également signaler en ligne des activités ou des contenus illégaux à notre plateforme nationale « PHAROS », appartenant à notre unité nationale spécialisée dans la lutte contre la cybercriminalité (l'OCLCTIC [3]) qui comprend une équipe dédiée au recoupement des signalements reçus, à leur mise en relation avec un crime ou un délit, aux premières investigations, ainsi qu'à l'envoi aux fournisseurs d'accès et de services Internet des demandes de retrait de contenus. Cette même équipe PHAROS est également chargée de préparer et de diffuser les listes de contenus illicites justifiables d'une procédure de retrait ou de déréférencement dans les moteurs de recherche.

Création d'une plateforme de coopération avec les grands acteurs de l'Internet. Pour renforcer la coopération avec les fournisseurs de services Internet, plus particulièrement dans le traitement des faits concernant le terrorisme ou d'autres crimes graves qui peuvent être commis en France, nous organisons un dialogue étroit avec les principaux fournisseurs d'accès et de services de l'Internet.

« Après une récente attaque terroriste dans un train à grande vitesse, les opérateurs ont répondu en moins d'une heure aux demandes des enquêteurs »

En février 2015, le ministre de l'Intérieur, Bernard Cazeneuve, s'est personnellement rendu aux Etats-Unis à la rencontre de plusieurs de ces acteurs, et les échanges qui ont suivi ont abouti à une plateforme de coopération rendue publique le 22 avril 2015. Parmi les dispositions arrêtées d'un commun accord au sein de ce document, figure la diffusion à tous les enquêteurs de France de formulaires spécialement

2 Devenue l'Association Française des Prestataires de l'Internet (AFPI) début 2016.

3 L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, appartenant à la direction centrale de la police judiciaire (DCPJ/SDLC).

conçus pour garantir que les réquisitions adressées aux opérateurs contiennent d'emblée l'intégralité des informations nécessaires à leur traitement. Ces formulaires sont intégrés ou directement accessibles depuis les logiciels de rédaction des procédures utilisés par les enquêteurs. La plateforme de coopération établit également un processus spécifique de validation concernant les réquisitions qui doivent être traitées en urgence – urgence vitale, terrorisme, ou autres situations particulières. Ce mode opératoire a été utilisé récemment à la suite de l'attaque terroriste perpétrée dans un train, au cours de laquelle trois citoyens américains sont intervenus de manière héroïque pour neutraliser le terroriste. Dans cette affaire, les opérateurs ont répondu en moins d'une heure aux demandes des enquêteurs.

Enfin, conformément aux dispositions arrêtées le 22 avril 2015, je réunis très régulièrement un groupe de contact permanent entre les services et les opérateurs, aux fins d'évaluer le fonctionnement des dispositions prises, mais aussi de maintenir le dialogue et d'envisager le cas échéant d'autres modalités de coopération. L'association française des fournisseurs d'accès et de services Internet a rejoint ce groupe de contact.

Pour conclure je voudrais insister sur le caractère essentiel de la coopération dans la lute contre le cyberterrorisme. Il s'agit en premier lieu de la coopération avec les acteurs de l'Internet que je viens de décrire, et qui a été étendue en juillet 2015 avec la création de l'unité européenne de référencement (EU IRU) au sein d'Europol. Cette coopération se nourrit également des relations très étroites que nous entretenons avec nos collègues des services du Premier ministre et des départements ministériels de la Défense, des Affaires étrangères et de la Justice notamment. Elle va bien au-delà de la seule répression enfin, comme l'a illustré la présentation du travail réalisé par Christian Gravel dans le domaine du contre-discours.

Facilitating Investigations of Cyber-enabled Actions of Terrorist Groups through Cooperation with Internet Communication Platforms

Mr. Jean-Yves Latournerie
Prefect, Government Special Advisor for the Fight against Cyberthreat, Ministry of the Interior

Last December, I was appointed as Government special adviser for the fight against cyberthreats, in charge of proposing and conducting the strategy of our ministry in this domain. This includes the coordination of our initiatives against cybercrime as well as the cybersecurity of the ministry itself. Today, I would like to describe our response to cyberterrorism.

The French Strategy against Cyberthreats

The French strategy against cyberthreats contains a number of key elements: understanding the threat; adapting our forces' response quickly; and being able to respond to the crises that our country is going through whenever the cyber element plays a growing role. Another key element is the quality of our cooperation with industry so that we can better measure the threats we are facing; better protect industry's economic activity, products, services and customers; and build together the solutions against those cyberthreats.

From the time when I started this new mission just 10 months ago today, our country has been confronted with a number of events that have demonstrated from the start that a strong cooperation with the telecommunications and internet service providers was necessary in order to identify suspects and stop the publication of content meant to terrorize the population. Of course, this is not a new subject. For a number of years, we have been working in France, in Europe and all around the world to fight against cybercrime and undermine the distribution of illegal content, with child abuse content representing some of the most horrendous situations portraying actual victims of abuse. Great successes have been attained in cooperation with the internet industry. We must not lower our guard, however, and sadly, there are still many victims of such abuses around the world and perpetrators to identify and arrest. Objectionable content also includes different forms of hate speech, such as the expression of racism, the incitement to discrimination and publications that support and propagate the message of terrorists.

> **For internet child abuse, "great successes have been attained in cooperation with the internet industry."**

In our understanding of cyberthreats, the concepts of cyberterrorism and cyberjihadism are becoming more precise:

- There are increasing signs that cyberterrorist actions are possible and part of the strategy of terrorist groups. France is very often the target of groups supporting the activities of Daech—hopefully with few tangible results, and mostly through the defacement of unimportant websites.

- But the attack sustained by TV5 Monde in April has demonstrated that some of our key assets are potentially vulnerable to cyberattacks, in particular if those attacks are conducted to destroy the activities of its target.

- France is also one of the major targets of cyberjihadism, with content specifically designed for the French-speaking community and the cultural habits of our youths. The messages are intended to recruit, but also to undermine the confidence of our population.

The Fight Against Objectionable Content

I will focus now on the fight against objectionable content. France has recently enhanced its arsenal in response to those contents:

Precise Legislation. We have precise legislation describing which types of expression do not constitute freedom of speech and are not socially accepted. The most serious among those unlawful publications are investigated as regular criminal offenses, including for instance a possible sentence of three years and the possibility to use all the tools in our procedure, such as immediate trials ("comparution immédiate"). This includes of course child abuse content, but more recently, since the law of November 2014 against terrorism, the "apology" for terrorism is now investigated like any other criminal offense with aggravated circumstances when those publications are done on the internet, raising the maximum penalty to 7 years of imprisonment. When content cannot be removed, the same legislation has introduced the possibility to block access to content related to terrorism or obtain its removal from search engine results,[1] (adding to previous provisions that allowed to block the distribution of child abuse content).

Responsibilities of Internet Service Providers. Internet access providers and Web hosting companies have an obligation to provide a service to receive notifications of illegal content; the national association of internet service providers (AFA) maintains such a service for its members (www.pointdecontact.net) and they are part of the INHOPE network.

The PHAROS National Platform. Illegal online activities and content can also be reported by any person on the internet to our national platform "PHAROS," part of our national cybercrime unit (the OCLCTIC) with a team dedicated to cross-referencing the reports, relating those reports to an offense, starting the investigations and sending requests to service providers for the removal of content; The PHAROS team is also in charge of preparing and distributing the lists of illegal content that should be blocked by Internet service providers or removed in search engine results.

"Internet access providers and Web hosting companies have an obligation to provide a service for receiving notifications of illegal content;"

Creation of a Cooperation Platform with the Biggest Internet Service Providers. To enhance the cooperation with internet service providers, in particular in the management of the most serious events related to terrorism or other serious crimes that can be committed in France, we are developing a closer dialogue with the biggest internet service providers. Last February, French Interior Bernard Cazeneuve personally visited a number of these actors in the United States and the discussions that followed were formalized by a cooperation platform announced on 22 April 2015 in Paris. This platform includes the distribution of specific forms to all investigators in France to ensure that their requests contain all necessary information. The forms are directly available in the software our investigators use to write police reports. The platform also includes a special validation process for requests that must be regarded as emergency—vital emergency, terrorism or other specific situations. This process was used during the last terrorist attack on a train when three American citizens heroically neutralized the terrorist. Elements were obtained in less than one hour from the operators. Finally, I have been mandated to facilitate a permanent contact group to maintain this dialogue and review the functioning of our cooperation platform. It has been extended to the French ISP association.

After a recent terrorist attack on a high-speed train, elements were obtained in less than one hour from the internet operators.

To conclude, I would like to insist on the essential cooperation aspect of the fight against terrorism online. This goes with the cooperation with the industry that I have described and it has been reinforced in July by the creation of the European Union Internet Referral Team at Europol, as well as through the cooperation with our counterparts in other departments, such as the Ministries of Defense, Foreign Affairs, and Justicex or the work presented by Christian Gravel on his counter-speech.

1 Our national Personal data protection authority (the CNIL) is in charge of controlling the application of the blocking and search engine removal provisions, by appointing one of its members; blocking of child abuse content and publications related to terrorism started last April and the first search engine removal requests were sent last August.

Protecting Critical Infrastructure from Cyber Attack

Caroline Baylon
Research Associate in Science, Technology, and Cyber Security, Chatham House

Why is Critical Infrastructure such an Attractive Target?

How can we best deal with the growing threat to our critical infrastructure from cyber attack? Whether it is from the electrical power grid to transport networks to the water supply, much of our critical infrastructure is increasingly internet connected. It is also making use of commercial off-the-shelf software that is easier to hack and, with this, come a number of vulnerabilities. The electric grid, for example, which consists of electrical power generation plants and the power distribution system, is central to nearly all aspects of modern life. Yet cyber attacks could take down significant parts of the grid in all countries around the world, from Japan to the United States to France. The consequences of a loss of electricity could be dire. Transport would be severely disrupted, as computer-controlled systems—from train signaling to air traffic control—would not function, leading to accidents and potential loss of life among the population. Communication would also be impacted as television, radio and, in many cases, phones would not work; this would hamper the ability of emergency services to respond. Business would be affected and the stock market could not operate, crippling a country's economy. All this shows why critical infrastructure is a highly attractive target for those seeking to harm a country.

> **"Cyber attacks could take down significant parts of the electrial grid in all countries around the world."**

The Potential Threat Actors

Hackers and Cybercriminals. The large number of potential threat actors is acquiring increasingly powerful capabilities. One group of actors—hackers and cybercriminals—has been using search engines like Shodan, which makes it possible and in fact quite simple to run a search for critical infrastructures that are connected to the internet. In the same way, automated exploits tool kits like the Metasploit framework are free to use and automate the process of cyber attack. As a result, it is now possible for hackers with little skills to wage attacks on critical infrastructure that are capable of causing harm.

> **"Cybercriminals have been using search engines like Shodan, which makes it simple to search for critical infrastructures connected to the internet.**

Nation States. Another group of actors is nation states. The discovery of the Stuxnet worm that was targeted against Iranian nuclear facilities in 2010 really showed other countries the true extent of a cyber weapon's destructive capabilities. Since then, countries have been rushing to develop offensive capabilities, increasingly penetrating each other's power grids and other critical infrastructure to look for vulnerabilities that they can exploit to gain tactical advantage. China and Russia are known to have installed backdoors and malware that can be activated at a later date in the U.S. power grid, while the U.S. is engaging in similar tactics. Although at present it would not be in any country's interest to attack another—they are confining themselves to laying the groundwork for possible future use—they may choose to do so in the event of an outbreak of hostilities. This was recently demonstrated in Ukraine, when an attack attributed to Russia took down the power grid in over 100 towns and cities. So, even if countries are only developing cyber weapons for defensive purposes or for deterrence, we do need to recognize that increasing capability also means an increase in the probability that this capability will be used.

> **"China and Russia are known to have installed backdoors and malware that can be activated at a later date in the U.S. power grid."**

Terrorist Groups. Finally, the last major threat comes from terrorist groups who are interested in attacking critical infrastructure and may use cyber means to do so. The Islamic State in Iraq and Syria (ISIS) is highly skilled in the use of social media for propaganda and has been actively trying to attack the U.S. power grid. At present, ISIS's efforts have proved unsuccessful, but there is a real concern that they could buy or acquire this capability in the not-so-distant future.

These challenges will be discussed more fully by my colleagues Raj Samani from the cyber security industry, General Marc Watin-Augouard from the French government's national police force—the Gendarmerie Nationale, and Jakub Boratyński of the European Commission's DG Connect.

Public Private Partnerships for Defending Critical Infrastructures

Mr. Raj Samani
Chief Technology Officer, Europe, McAfee/Intel

Is the cyberthreat to critical infrastructure over-exaggerated? If we look at the headlines, the term digital Pearl Harbor has been used more than once and the term cyberwar is kind of used interchangeably with traditional war. Despite all these headlines, we have only seen two major attacks on critical infrastructure through cyber that have had an impact on availability. I am referring to the 2010 attack in Iran against nuclear facilities and most recently in Germany where a steel mill was compromised. So the risk has perhaps been somewhat over-exaggerated, but, personally speaking, just because the threat has not been realized does not mean that we can ignore the vulnerability of our critical infrastructure.

Our Critical Infrastructure's Vulnerability

Caroline Baylon discussed Shodan earlier. Shodan was remarkable because it demonstrated the direct accessibility and connectability of our critical infrastructure to the internet. Within one or two clicks you can have access to medical devices that are directly connected online. Shodan was last year's news: what has changed since? Two weeks ago, we concluded a piece of research entitled "The Hidden Data Economy." Quite ironically, we are here in France where we identified criminals selling access into control panels of critical infrastructure installations—a hydroelectric generator—to anyone willing to pay.

> **"...we identified criminals selling access into control panels of critical infrastructure installations–a hydroelectric generator–to anyone willing to pay.**

When we talk about cybercrime or about nation state attacks, we often discuss the fact that it is quite simple to become a cyber criminal or hacker. All you need is the ability to pay and the required level of sophistication is now the lowest it has ever been. For a few bitcoins, you can purchase a username and password and you can directly start impacting the French critical infrastructure. So we are living in an environment and in a world whereby our attacker does not need to have any knowledge, skill or capability to impact our society. Although we only have two concrete examples, the potential for this happening is enormous and we need to address this challenge pretty quickly.

Making Public-Private Partnership a Reality

So where do we begin? You often hear the term public-private partnership but in most cases, it is just lip service. It is used by organizations as a marketing term to try to get more business. So we have been doing everything we can to try to make sure that public-private partnership is more than lip service. Over the past three years, we have been directly supporting and assisting the European Cybercrime Center Europol, the UK National Crime Agency as well as US agencies on identifying and taking down criminal infrastructures that are impacting our society. Just three months ago, we led a takedown against organized criminals from Eastern Europe who had been impacting our citizens. We directly led that operation and successfully dismantled that botnet. In the last twelve months, we have been engaged in about ten to twelve operations directly targeting online criminals who were attacking our infrastructure. That is the law enforcement side.

> **"We led a takedown against organized criminals from Eastern Europe who had been impacting our citizens. "**

"We are facing an environment in which the threat actor is getting access to more capability to disrupt"

Today, we have no choice but to pursue the modernization of our grids and modernize every part of our critical infrastructure. We have huge inefficiencies across the globe with regards to the consumption of our critical infrastructure and we are facing an environment in which the threat actor is getting access to more capability to disrupt this. So a key component of this is to be able to work in partnership. For example, in the European Commission, we have been aiding and assisting the Smart Grids Task Force group to develop better guidance and standards. In summary, the only way we are going to be able to combat these threats is by collaborating and working together.

La Relation entre la Protection des Infrastructures Vitales Et la Cybercriminalité

Général (Gendarmerie) Marc Watin-Augouard
Fondateur du Forum international de la Cybersécurité (FIC),
Directeur du Centre de Recherche de l'Ecole des Officiers de la Gendarmerie Nationale

Le sujet que je vais traiter—la relation entre la protection des infrastructures vitales et la cybercriminalité—a sans doute été largement évoqué hier par Guillaume Poupard, par l'Amiral Coustillière, et par d'autres intervenants. Je vais donc essayer de vous en donner une approche un peu plus personnelle.

Le Passage de la Cybersécurité Artisanale à la Cybersécurité Industrielle

> **« L'année 2007 a été une année charnière avec l'attaque cyber massive de l'Estonie. »**

En 2001, le Conseil de l'Europe a ouvert la ratification de la Convention sur la cybercriminalité. A l'époque, on ne parlait que de cybercriminalité et elle était abordée sous un angle assez artisanal. Il n'y avait que quelques hackers, on commençait à vendre de la pédopornographie sur l'internet, mais on en était au stade de l'artisanat. En 2014, les Etats de l'Union Africaine ont ratifié la convention de Malabo sur la cybersécurité, qui englobe non seulement la lutte contre la cybersécurité mais également la cyberdéfense, et même la sécurité des données à caractère personnel. Entre les deux, on est passé du stade artisanal au stade industriel et nous avons constaté que 2007 a été une année absolument charnière avec l'attaque cyber massive de l'Estonie.

La cybercriminalité n'a pas de définition universelle mais on est d'accord pour dire qu'il y a trois types d'infractions: celles qui prennent le cyberespace comme cible, c'est-à-dire toutes les atteintes au système de traitement automatisé de données; les atteintes aux données, qui sont plus particulières; et toutes les infractions qui concernent l'utilisation impropre de la cryptologie. Et puis il y a les infractions dont le cyberespace est le vecteur, qui portent des contenus comme la propagande, le terrorisme, l'apologie du terrorisme. Enfin, il y a les infractions qui sont amplifiées par le cyberespace, en fait les escroqueries. C'est une trilogie qui a ses limites parce qu'aujourd'hui, il y a souvent des cyberattaques qui ciblent les systèmes, mais qui utilisent les contenus, et aussi les escroqueries, comme des infractions du type usurpation d'identité. Donc, on ne peut pas dire qu'il y a une catégorie qui vise plutôt les personnes, une catégorie qui vise plutôt les entreprises, et une catégorie qui vise plutôt les états. Tout est assez mélangé.

En 2007, on est sorti effectivement de l'artisanat pour entrer dans la phase industrielle. A partir du 27 avril, l'Estonie est massivement bombardée, non pas avec des armes et des munitions, mais par une attaque par déni de service, c'est-à-dire un blocage du fonctionnement de plus de 85.000 ordinateurs. On a dit à ce moment là que c'était la cyberguerre et le commencement des cyber-armes. Je dis souvent qu'il faut toujours penser à la cyberguerre mais n'en parler que rarement.

> **« TV5 Monde, qui est un de nos grands medias, a été attaqué. On a dit que Daesh était responsable mais il s'agissait sans doute de hackers Soviétiques. »**

Pourquoi? Parce que le droit des conflits armés s'applique à la guerre et notamment à la cyberguerre, même s'il faut l'adapter, et que dans le droit des conflits armés, il faut d'abord identifier un ennemi qui relève d'un état, ou d'une organisation étatique ou paraétatique. Or, qui peut dire qui a attaqué l'Estonie? Il y a des doutes mais il n'y a jamais eu de preuves. Et c'est la même chose dans tous les cas—il y a des doutes mais il n'y a jamais de preuves. En France, TV5 Monde, qui est un de nos grands medias, a été attaqué. On a dit que Daesh était responsable mais il s'agissait sans doute de hackers Soviétiques. Donc, on voit bien aujourd'hui que le mot cyberguerre est difficile à employer. La guerre dans le cyber est quotidienne, notamment sur les théâtres que nous connaissons, mais

pas la cyberguerre. Tant que nous n'avons pas identifié un ennemi, nous sommes toujours dans le droit commun et il faut évoquer la cybercriminalité qui attaque nos entreprises, notamment nos entreprises critiques, sous l'angle du droit commun et non pas sous l'angle du droit des conflits armés. Lorsqu'on dit cyber-armes, il n'y a pas de cyber-armes mais peut-être des armes plus sophistiquées. STUXNET n'est pas un travail de petit hacker, c'est le travail d'une équipe construite qui dispose de moyens à long terme. Et lorsqu'il s'agit d'une attaque par déni de service, elle peut avoir un but de criminalité crapuleuse, un but terroriste, ou viser un état ou une infrastructure critique. C'est la même arme. Ce qui change, c'est l'objectif poursuivi, la finalité attendue, et la qualité des auteurs. Donc, si dans tout ce que nous faisons et observons aujourd'hui, nous partons dans la cyberguerre, nous avons tort parce que, la plupart du temps, nous traitons le problème dans un cadre de droit commun.

La différence entre une petite attaque cyber quotidienne qui ne touche qu'un individu et une grande attaque est la même que la différence entre un euro et un million d'euros que vous devez à votre banque. Un euro que vous devez à votre banque est une dette; un million d'euros, c'est toujours une dette. Un euro, la banque vous envoie l'huissier; un million d'euros, la banque vous invite à déjeuner. Cela veut dire qu'en fait, la cybercriminalité n'est pas traitée de la même manière selon l'ampleur de la cible ou selon les enjeux, mais nous sommes toujours dans la cybercriminalité. Après 2007 cependant, la France, l'ensemble des pays d'Europe ainsi que le reste du monde ont compris que quelque chose avait changé et qu'il fallait avoir une politique de cyberdéfense, notamment pour protéger les infrastructures d'importance vitale. C'est cette cyberdéfense qui a été mise en place en France avec notamment le Livre blanc sur la défense en 2008 et renforcée par le Livre blanc de 2013.

Cybercriminalité et Cyberdéfense Sont dans la Continuité l'Une de l'Autre

« ...la cyberdéfense et lutte contre la cybercriminalité s'interpénètrent. »

Il est important de noter que nous sommes désormais dans un système qui est continu. Un grand nombre de gens voient la lutte contre la cybercriminalité et la cyberdéfense comme étant deux champs différents. Ce n'est pas tout à fait faux mais ce n'est pas vrai non plus parce que cyberdéfense et lutte contre la cybercriminalité s'interpénètrent. L'une est la continuité de l'autre. Quand nous agissons pour protéger les opérateurs d'importance vitale, nous sommes dans la continuité de la lutte contre la cybercriminalité. Donc, opposer l'une et l'autre est une erreur et justement, par rapport aux opérateurs d'importance vitale, il faut agir sur tous les registres en même temps et ensemble. Quand TV5 Monde a été attaqué, nous avons vu apparaître des acteurs de la cyberdéfense ainsi que des acteurs de la lutte contre la cybercriminalité parce que le même phénomène a dû être traité à la fois sur le plan de la réparation, de la compréhension des phénomènes, sur le plan technique, et aussi sur le plan judiciaire parce qu'une enquête judiciaire a été ouverte. Donc, pour les opérateurs d'importance vitale, il faut bien comprendre que tout est mélangé, même si les acteurs ne sont pas les mêmes, et cela nous amène à développer un dialogue permanent. En France nous parlons de « la Bande des Quatre», c'est-a-dire que nous avons le pompier, Guillaume Poupard, qui arrive sur l'incendie, le soldat, l'Amiral Arnaud Coustillière, le Préfet Jean-Yves Latournerie, qui représente la partie exécutive de la lutte contre la cybercriminalité, et enfin le diplomate, l'Ambassadeur David Martinon. Ce cartel doit travailler ensemble parce que nous ne pouvons pas protéger aujourd'hui nos opérateurs d'importance vitale d'une manière dispersée. Nous devons le faire d'une manière parfaitement unitaire avec, bien sûr, l'idée que chacun doit garder son propre rôle et que chacun a sa propre logique professionnelle. Parfois, le travail dans le domaine de la cyberdéfense se fait dans le secret. Le travail dans la lutte contre la cybercriminalité se fait dans la transparence, dans le cadre normal de l'opposition à toute personne des éléments de preuve qu'on a recueillis. Donc, ce sont deux approches qui ne sont pas tout à fait les mêmes mais ces deux approches sont complémentaires.

Un Partenariat Public-Privé pour Protéger les Opérateurs d'Importance Vitale

Alors, pourquoi faut-il travailler ensemble? Aujourd'hui, nous devons mettre en commun les renseignements d'intérêt cyber ou d'origine cyber parce que la recherche-développement est aussi importante pour la cyberdéfense que pour la lutte contre la cybercriminalité ; c'est aussi parce que nous devons apporter aux opérateurs d'importance vitale une réponse totale, complète, et non pas des réponses dispersées dans lesquelles on finirait par ne pas comprendre l'intervention des autorités

« Nous ne réussirons pas à protéger nos opérateurs d'importance vitale…sans développer un partenariat public-privé. »

étatiques. Enfin, nous devons être conscients que nous ne réussirons pas à protéger nos opérateurs d'importance vitale contre les atteintes de la cybercriminalité sans développer un partenariat public-privé. Ce partenariat nous amènera sans doute à revoir un certain nombre de paradigmes sur lesquels repose la séparation publique-privée telle que nous la connaissons en France. En particulier, si nous voulons que les acteurs de la lutte contre la cybercriminalité ou de la cyberdéfense aient un niveau technique suffisant, nous allons devoir partir tous ensemble sur un marché de plus en plus restreint par rapport à l'offre et à la demande. Il va falloir que nous trouvions des solutions intelligentes avec les partenaires privés pour que les acteurs de la lutte contre la cybercriminalité puissent aller dans leurs entreprises parfaire leurs connaissances et revenir ensuite dans le système de l'état, ce qui me fait dire avec le ministre de l'Economie et des Finances français que le statut des fonctionnaires est sans doute largement compromis.

Voila pourquoi je pense qu'aujourd'hui cette lutte contre la cybercriminalité n'est pas autonome par rapport à la protection des opérateurs d'importance vitale. Nous avons besoin d'être auprès d'eux, et notamment auprès de leurs sous-traitants parce que lorsque nous parlons d'opérateurs, il faut penser aux sous-traitants et peut-être même aux sous-traitants des sous-traitants. Ceci nous amène à avoir une stratégie qui n'est pas simplement concentrée sur les entreprises mères mais peut-être aussi à descendre dans le territoire, dans l'irrigation, dans la capillarité, pour pouvoir leur apporter une réponse de proximité.

The Relationship between Critical Infrastructure, Protection, and Cybercriminality

General (Gendarmerie) Marc Watin-Augouard[1]
Founder of the International Forum on Cybersecurity (FIC)
Director, Center for Research, Officer School of the Gendarmerie Nationale

The topic I am going to discuss—the relationship between critical infrastructure protection and cybercriminality—has probably been fully addressed earlier by Guillaume Poupard, Admiral Coustillière and others. My approach will therefore try to be a little more personal.

The Transition from Artisanal to Industrial Cybersecurity

In 2001, the Council of Europe opened the Convention on Cybercrime for ratification. At the time, cybercrime was the only subject and it was approached in a fairly artisanal manner. There were a few hackers, child pornography was starting to be sold on the internet, but it was on a small scale. In 2014, the member states of the African Union ratified the Malabo Convention on Cybersecurity that covers, in addition to cybersecurity, cyberdefense and even the protection of personal data. Between the two, we went from an artisanal to an industrial stage and 2007 turned out to be a turning point with the massive cyberattack on Estonia.

> **" 2007 turned out to be a turning point with the massive cyberattack on Estonia."**

Cybercriminality does not have a universal definition, but there is consensus on three types of infractions: those that target the cyberspace, i.e., all attacks on the electronic data processing systems; attacks on data, which are more specific; and all attacks that deal with an improper utilization of encryption technology. Then, there are attacks in which cyberspace is the vector and whose content is propaganda, terrorism or the apology of terrorism. Finally, there are attacks that are enhanced by the cyberspace, i.e., scams. This trilogy has its limits, however, because cyberattacks today can often target systems while also utilizing their contents and scams, like identity theft. Thus, you cannot say that one category of attacks targets people, another targets primarily businesses, and another mostly states. It is all rather mixed.

In 2007, we did leave the artisanal stage and entered the industrial stage. Starting on 27 April, Estonia was massively bombarded—not by arms and ammunitions—but by a denial of service attack, which blocked the functioning of more than 85.000 computers. The words "cyberwar" and "cyberweapons" were mentioned at the time. I often say that we need to keep thinking about cyberwar but should mention it only rarely. Why? This is because the law of armed conflicts applies to war including cyberwar—even if it must be adapted—and this law of armed conflicts requires the identification of an enemy that is either a state, or a state or parastatal organization. Now, can anyone tell us who attacked Estonia? We certainly have doubts but no evidence. And it is the same in all cases—there are doubts but there is never any evidence. When one of our large French media groups, TV5 Monde, was attacked, Daesh was held responsible but it was more likely an attack by Russian hackers. So, all this shows how difficult it is to use the word "cyberwar." War in the cyber world is part of our daily life, but cyberwar is not. As long as we are not able to identify an enemy, the civil legal system applies. When cybercriminals target our businesses and our critical infrastructure, the civil legal system applies, not the law of armed conflicts. When we use the word "cyberarms," there are no cyberarms and the term may simply refer to more sophisticated weapons. Stuxnet was not the work of a small group of hackers, it was the work of a well-organized team with long-term financial means. And a denial of service

> **" When one of our large French media groups, TV5 Monde, was attacked, Daesh was held responsible but it was more likely an attack by Russian hackers. "**

1 Translated by Anne D. Baylon, *Proceedings* Editor.

attack may be motivated by financial gain, terrorism, or target a state or critical infrastructure. It is the same weapon but the difference lies in the objective, the expected end result, and the expertise of the cybercriminals. Today, moving in the direction of cyberwar would be wrong because most of the time, problems can be solved in a civil legal framework.

The difference between a small daily cyberattack that targets a single individual and a large cyberattack is very similar to the difference between owing your bank one euro or one million euros. One euro that you owe your bank is a debt; one million euros is still a debt. For one euro, the bank sends a bailiff to your house; for one million euros, the banker invites you for lunch. What I mean by that is that cybercrime is not treated in the same manner depending on the target scale or what is at stake but it remains a cybercrime. After 2007, however, the whole world understood that something had changed and that a cyberdefense policy was required, in particular to protect the critical infrastructure. This cyberdefense policy was set in place in France with the 2008 White Paper on defense and it was strengthened with the 2013 White Paper.

Cybercrime and Cyberdefense are Complementary

From now on, we are in a continuous system. Many people think that the fight against cybercrime and cyberdefense are two different fields. Without being totally incorrect, this is not correct either because cyberdefense and the fight against cybercrime feed into each other. One is the continuation of the other. When we take action to protect critical infrastructure operators, this action is the continuation of the fight against cybercrime—so, opposing one to the other is a mistake. In the case of critical infrastructure operators, action must be taken at various levels, at the same time and together. The attack against TV5 Monde involved both cyberdefense and cybercrime actors because the same event concerned different levels: the restart of TV5 Monde, an understanding of the events, technical expertise, and the judicial level since a judicial inquest was initiated. Therefore even if the actors are not the same, everything is mixed in the case of critical infrastructure operators and this brings us to having a permanent dialogue. In France we have the "Gang of Four:" Guillaume Poupard, the firefighter who fights the fire; Arnaud Coustillière, the soldier; Jean-Yves Latournerie, the prefect who is the executive side of the fight against cybercrime; and Ambassadeur Martinon, who is the diplomat. This "cartel" has to work together because there is no way to protect our critical infrastructure operators by acting separately. However, they work together with the understanding that they have their own role to play and their own professional logic. Sometimes, cyberdefense work is conducted in secrecy. Cybercrime work must be transparent. Both approaches are not exactly the same, but they are complementary.

> **"There is no way to protect our critical infrastructure operators by acting separately."**

Developing a Public-Private Partnership in order to Protect Critical Infrastructure Operators

Why should we work together? Today, we must share all information that concerns cyber because research and development is as important for cyberdefense as it is for fighting cybercrime. Also, we must provide critical infrastructure operators with a complete response—we cannot present them with scattered responses that would lead them to wonder why state actors are intervening. Finally, we will not succeed in protecting our critical infrastructure operators against cybercrimes without developing a public-private partnership. This partnership is likely to bring us to revise a number of paradigms that are currently defining the public-private separation in France.

In particular, if want cybercrime and cyberdefense actors to have the necessary technical level, we will have to deal with a narrower supply and demand market. With our private partners, we will need to find smart solutions that will make it possible for actors fighting against cybercrime to work in their companies, develop their expertise, and then return to the state system. This is why I believe that today, the fight against cybercrime is linked to the protection of critical infrastructure operators. We need to be in close contact with them, and also with their subcontractors and perhaps the subcontractors of their subcontractors as well. Our strategy should not be focused solely on parent companies but also further down on their subsidiaries in order to provide the best response possible.

> **"Today, the fight against cybercrime is linked to the protection of critical infrastructure operators."**

The EU Network Information Security Directive
A Game Changer for Protecting Critical Infrastructure?

Mr. Jakub Boratynski
Head of Trust and Security Unit, DG Connect, European Commission

This workshop has brought together people from different communities around one table, which is very good, but it shows at the same time why it is so difficult to come up with a coherent response to cybersecurity issues. There are many competing paradigms, different dimensions and perceptions, and a multitude of national authorities that are dealing with these issues. I am coming from a part of the European Commission that has set as our flagship initiative for this term the goal of constructing a digital single market; and it is very clear that, without a high degree of cybersecurity, people and companies will not have trust in the digital economy. Having worked for a number of years on cybercrime, I have been involved in the establishment of the European cybercrime center within Europol where we were also confronted with a community that had different views. At this workshop, this diversity issue is again very present as we are dealing with a profound dimension of national security.

The EU Network Information Security Directive is a Game Changer for Critical Infrastructure

I would like to show here how we are trying to solve this dilemma in the context of an EU directive which is close to being adopted. I have entitled my presentation "The EU Network Information Security Directive—a game changer for protecting critical infrastructure?" Even though there have not been many instances of attacks against critical infrastructure, we are becoming increasingly aware that critical infrastructure is vulnerable. Given this vulnerability, is the challenge to define what to do or how to do it? Critical infrastructure is often national by design and a matter of national security, yet it is becoming increasingly interconnected. Is this an opportunity or a threat for nation-states? My assertion is that the EU Network Information Security directive (NIS) piece of legislation—the first ever in the EU that deals with cybersecurity—is a game changer.

The EU Network Information Security (NIS) legislation is a game changer for critical infrastructure.

Before getting into the details, I would like to examine a hypothetical scenario since there have not been many real-life scenarios yet. We are sitting here today probably in one of the safest locations in Paris but 400 km north, an installation called the Eastern Scheldt Storm Surge Barrier is an important element of the infrastructure that protects the lowlands of the Netherlands against flooding from the North Sea. At the Neeltje-Jans artificial island at one end of the barrier, a plaque is installed with the words: "Here the tide is ruled by the wind, the moon and us (the Dutch)." So, even if you are not familiar with the barrier, I am pretty sure you are familiar with the magnificent engineering accomplishment that allows people in the Netherlands to live in relative safety, even though a significant part of the country is below sea level. But I am not so sure that you are aware that a movie-plot threat based on a cyber attack against the barrier won the 2013 contest organized by Bruce Schneier, a guru on cyber security and privacy and one of the leading global and US thinkers on the subject. The main idea in the script is that a remote cyber attack could disable the barrier's electronic control system during a storm surge, leaving the Netherlands basically defenseless and vulnerable to extreme flooding. Obviously, it is a work of fiction but it did capture the imagination of Schneier's audience as to the high stakes for cybersecurity threats to the critical infrastructure.

According to a move script publicized by Brue Schneier, a remote cyber attack could conceivably "leave the Netherlands vulnerable to extreme flooding" by opening the Storm Surge Barrier.

A NIS Directive Will Require a Risk Management System for Critical Infrastructure

Is this relevant to an NIS directive? We believe it is because, once this directive is adopted, it will make sure that operators of such barriers will be under the legal obligation to manage and mitigate cybersecurity-related risks. In other words, and this is a key element of the directive, there would be a legal obligation to put in place a risk management system. There would also be competent authorities and capabilities and cooperation issues to be worked out between member states. I will quickly go into more detail about what this piece of legislation is about and what we expect it to accomplish.

The directive was part of a package that the European External Action Service presented in 2013 and the first ever attempt by the EU to provide a comprehensive narrative about cybersecurity. The proposal for this directive is based on three pillars:

Creation of National Common Requirements for Capabilities. The first pillar is about creating a specific benchmark—common requirements across the member-states in terms of capabilities. This sounds pretty basic but it was important to ensure that countries that are less advanced would actually retain a minimum degree of capability. According to the directive, the member-states would need to have specific strategies on how to deal with cybersecurity risks and threats. They would have to put in place competent authorities and also be required to set up computer emergency response teams (CERTs).

Creation of a Common Cooperation Framework. The second pillar of the directive is about cooperation. As a result of the directive, we would have two layers of cooperation between member states: one, the policy level cooperation, would bring together the national competent authorities; the second one—and here we had extremely difficult negotiations—was the level of operational cooperation. Discussions about to what degree we can engage in international cooperation between member-states showed the clash of these different parts. On the one hand, we know that cyber threats and risks know no borders and that there is a lot to be gained by sharing information, sharing the threat analysis, and also coordinating the response to attacks. There is value to transparency. On the other hand, because of legitimate national security concerns, there is a feeling that not everything can be shared and not everything can be transparent. We ended up with a compromise that creates a framework, a network of national CERTs that can engage in far-reaching cooperation but on a voluntary basis. It is not as much as we were hoping for, but we feel it is a very important first step. It shows that, for member-states to engage in this sort of advanced cooperation, time is needed to build sufficient trust.

"...because of legitimate national security concerns, there is a feeling that not everything can be shared and not everything can be transparent"

Creation of Minimum Legal Obligations for Critical Infrastructure Operators. The third element of the directive is specifically related to the critical infrastructure. It is the notion that certain critical elements of the economy must respect minimum legal obligations. The first obligation concerns security requirements. Critical sectors such as transport, energy, healthcare, financial institutions would have to put in place risk management practices. One difficult part of the legislation is to decide the extent to which the critical elements of the digital economy must be included in the obligations of the directive. For example, companies such as cloud services or search engines, which are online market places, would be obliged to put in place risk management measures. The second element of these obligations is the requirement to notify the competent authorities when serious security incidents happen.

Critical sectors such as transport, energy, healthcare, financial institutions would have to put in place risk management practices.

Here are the key elements of the actual directive: first, capabilities at the national level; second, the cooperation framework at the EU level; and finally, obligations of the market players in the critical sectors of the economy which, from the perspective of legislators, is the most viable. We feel this approach would be a game changer, but it will require a lot of effort to make sure that those provisions, in practice, actually lead to real change. That of course would depend on overcoming the silos that keep the different communities from talking to each other, which would be of crucial importance.

The Role of the Armed Forces in Cyberspace

Dr. Kate Langley
Head of Cyber and Space Policy, UK Ministry of Defense

Who is in Charge of Cyberspace?

An audience like this knows that such a question—who is in charge of cyberspace?—implies too simple a way of considering the related issues but when, in the late 2000s, we began to better understand the insidious nature of the cyber threat, we spent an awful lot of time on that question. Today, I think, it is pretty much accepted that cyberspace reflects the complexity of the physical world and therefore touches all of us both personally and professionally in some way, whatever our role. But should that mean that, whilst there might not be one person or organisation in charge of cyberspace, it is always clear who is in charge of what? I will set out my developing thinking on the specific role of the armed forces in cyberspace but also consider why the question of 'who is in charge of what?' is not always straightforward.

The Specific Role of British Armed Forces in Cyberspace

This is developing thinking on how we describe the role of the British Armed Forces in cyberspace—I am sure this will change based on input from other workshop participants. I should start by explaining a couple of principles that underpin our approach:

Firstly, cyberspace is the same but different—by that I mean that the role of the armed forces in cyberspace should be consistent with our role in the physical realm. This is essential because our role has evolved over centuries, and not to draw on that experience would be foolish. An example of this would be how necessity and proportionality is considered in deciding appropriate use of armed forces—there must be consistency between actions in cyberspace and the physical realm.

The second principle is that, in thinking about any cyber problem, we must not get stuck in cyberspace. Cyberspace and the physical realm are fundamentally interconnected. Were they not, if we could somehow insulate ourselves and our lives from cyberspace, we would not place such a high priority on addressing the cyber threat. It is precisely because of the impact in the physical world that this is important, so we must not think about cyber problems without the context of the physical world. Let me give you an example of what I mean by that: in considering our responses to a given cyber incident, we should consider all of the means at our disposal. Do not assume that a counter-cyber attack is the most effective means to respond. Consider the full spectrum of the means available and consider the impact in the physical realm to judge the most appropriate response—and the most appropriate lead for that response. If it is a criminal act, clearly it is a law enforcement lead.

> **"...in considering our responses to a given cyber incident...do not assume that a counter-cyber attack is the most effective means to respond.**

Using those two principles, let me outline my thinking on the role of the armed forces in cyberspace:

- Firstly, we must ensure that regardless of the threats posed by cyberspace, the armed forces can continue to operate. This is why significant investment in the resilience of our capabilities and information networks has been a strong theme of the ongoing Strategic Review in the UK.

- Secondly, we must ensure that we consider our capabilities to project power through cyberspace, just as we do in the Air, Land and Sea environments.

- Thirdly, where we would have a role in responding to a conventional attack and defending the UK, we would play a role in responding to a cyber attack of a similar impact.

- And our fourth and final role, I think, is the equivalent to what we used to refer to as 'Military Assistance to Civil Authorities'—the sorts of situations that saw the Armed Forces supporting the Civil Authorities in dealing with flooding, or severe disease in livestock, for example.

You might quite reasonably observe that what I have described here is no different from the usual role of the Armed Forces. That is a natural consequence of my first principle—that this is merely an extension of the role of the Armed Forces into cyberspace. But in implementing those roles in cyberspace, the second principle must be born in mind: we must not fall into the trap of considering our role in cyberspace in isolation of the other operating environments.

Who is in Charge of What?

For example, in that first role—ensuring our capabilities are resilient to the cyber threat—our priorities should take into account the impact in the physical realm and role—power projection in cyberspace—don't assume cyber should always be fought with cyber. Perhaps improving resilience and diplomatic/economic measures is more appropriate? Perhaps a conventional armed response is more appropriate. Of course that applies to the third and fourth roles too: we must consider the full range of capabilities available to us in responding appropriately or supporting others' lead in responding. Our support to civil authorities in the event of a major cyber attack might have very little to do with cyberspace at all. It might have more to do with getting food to a hungry population.

> **"Our support to civil authorities in the event of a major cyber attack ...might have more to do with getting food to a hungry population."**

So if the role of the Armed Forces is just an extension of the role in the physical realm, what is the fuss about? Surely this is quite simple? What about the challenges to which I referred earlier? Is this no more complex than the Royal Navy operating in the same waters as the Coastguard? Is this no more complex than the intelligence agencies operating in the same villages as the Special Forces in a theatre of war? Is this no more complex than military and civilian aircraft operating in the same airspace for different purposes? The list of civilian and military organisations operating in the same environment could go on and on. All these examples depend on a good understanding of the role that each organisation is fulfilling. Good progress has been made on this in recent years through cross-Government and international exercises and that must continue. Like international exercises, cyberspace does not respect geography.

> **"we need to focus on the handoff between different organisations as much as we do understanding the specific role that different organisations have to play."**

There is plenty more to be done to improve this but there is a further complexity that I want to raise before I close: when we see a fire, we know what to do. When we see a middle-aged businessman crumple to the ground, there's a good chance it's a heart attack or a stroke and we respond accordingly. When we uncover a spy ring, we have a practiced diplomatic response. The challenge with a cyber attack is that, in the early stages, it might be difficult to tell the difference between a fire, a heart attack, a stroke, and a spy ring. That is why we need to focus on the handoff between different organisations as much as we do understanding the specific role that different organisations have to play.

Cyberwarfare and the Growing Militarization of Cyberspace

Mr. Koen Gijsbers
General Manager, NATO Communications and Information Agency

I represent a NATO organization, the NATO Communications and Information Agency (NCI) in which the 28 nations make rules to give us guidance and we execute them. My responsibilities are to operate and defend NATO networks and my agency helps nations get better at working together in order to be able to operate their own networks. Our discussions with the NATO leadership are intensive. It was in 2002 that NATO started to have a cyber representation on its board. Already at the 2002 Prague Summit, NATO had set goals, targets and objectives for implementing cyber capabilities within its organization. As to industries, they started having cyber on their board almost fifteen years ago. Cyber has been discussed at each subsequent summit and new goals and objectives have been set. Through this process, NATO has been maturing step by step. NATO has its own capability and the capabilities of the member nations as well, and when it comes to warfare, I fully agree with the speakers before me that it is unclear in the current situation whether or not a cyberwar is taking place. According to the doctrine, when a situation starts that is vague, it is the normal rules of law that we have to deal with, not the law of war.

> **"When a situation arises that is not clear, it is the normal rules of law that we have to deal with, not the law of war."**

Cyber is an Indivisible Part of Allied Security

> **According to the Wales Summit, "the focus of the NATO organization and of my agency... should be on defense and improving resilience."**

That is why, at the last Wales Summit, NATO gave a uniquely clear guidance. First, NATO stated that cyber is an indivisible part of allied security. It is not a separate entity but it is an integral element of it. Second, the focus of the NATO organization and of my agency, which runs NATO's networks, should be on defense and improving resilience. This does not mean that we exclude other activities because NATO will never say in advance what its reaction will be, but it is very important that resilience should be seen as the most important part of what we do as an organization. It is not only the resilience of NATO's networks but also the resilience of national networks on which NATO relies for its operations and, of course, there are many of them.

Helping Nations Work Better Together

When NATO operates, it is not always well understood that we always bring together a federation of the NATO owned network and national networks. Basically, NATO is the glue between all these different national entities so that they can work together. This is part of our challenge because we cannot see information assurance in cyber as a separate element from interoperability. The most challenging part comes with the more complex elements of warfare where we share very complicated central data and data weapon systems, and we share all these complex elements over boundaries of national and NATO systems. That is easy when things are unclassified, but when encryption is in place, it becomes much more difficult, especially when the encryption is sometimes national, or sometimes a NATO encryption. This creates a complexity that NATO has actually been

> **"... industry does not tend to build things that work together. They tend to build things that do not work together, because they believe that they earn more money this way;"**

pretty good at dealing with, but it is an environment that is really difficult to manage, especially—and this is not an attack against industry—since industry does not tend to build things that work together. They tend to build things that do not work together because they believe that they earn more money this way; so nations often buy "national" and the result is that it is not always easy to work together. That is our first challenge.

Our second challenge is to keep doing all this in a secure environment in order to avoid being attacked via the weakest link. This is why NATO wants to influence nations to implement high standards, the same standards that NATO applies to its own international network environment. It should not be done only through the defense planning system where we set targets for nations to implement certain elements but also through NATO's move into a cloud-based environment with a federated mission network where we have thought through how we are going to operate in the future. We have learned from Afghanistan where we did that and that was very successful. We will also set clear standards for nations to be able to connect to NATO, which will have to be met before we operate. These are the developments that we see at the moment.

Of special importance are "collaboration partnerships—with NATO member nations and with partner nations, including Sweden, Finland and Australia."

In all this, two elements are fundamentally important to improve resilience: the first one is collaboration partnerships—partnerships of course with NATO member nations and partnerships with partner nations. For example, Sweden, Finland and Australia share standards and security levels that are similar to the ones we want to implement. The second element is agility, the ability to find good problem solutions faster. This is not easy for governments because governments tend to operate pretty slowly but we are currently working closely with industry under the NATO industry cyber partnership. There was a step in this direction at the summit last year under the leadership of the UK, Estonia, and the Netherlands. We feel that it is important that the boundaries between industry, NATO and the nations should not be limited to just a procurement that makes it difficult to work together. We need to find a way to share data and ideas in order to get better at it because 90% of what we do is either owned by industry or built by industry. So for me, collaboration and agility are two elements that will be my main focus for the near future—not just talk about it but actually doing it. This needs to be practical and we are trying different ways of doing that with industry by getting correctable data sharing, innovation ideas, incubators etc. in order to get things done faster. A good example of this Euro-Atlantic resolve could be seen over these past few days with exercise Trident Juncture where 37,000 troops of NATO and partner nations operated in a high-level ready war type scenario and were able to exchange data in a secure manner. We also conducted some cyber activities and showed that we can do this. This is really the essence of what NATO is all about and how we can operate as a NATO organization together with the nations in order to reach our objectives.

"We need to find a way to share data and ideas with industry...because 90% of what we do is either owned by industry or built by it."

Cyberwarfare and the Growing Militarization of Cyberspace

Ambassador Lauri Lepik
Estonian Ambassador to NATO

What I am going to say does not represent my country's position but the position of someone who has spent quite a lot of time at NATO and who was present at the creation of what we call our NATO cyberdefense policy. I was quite intrigued by the title of this panel, "Cyberwarfare and the Growing Militarization of Cyberspace" and by what it means for cyberspace. I also appreciated what Kate Langley said earlier about this. We do have to look at this issue with clarity and ask if militarization is actually happening in cyberspace. Since it was mentioned that nearly fifty countries have actually announced the creation of cyber commands and that millions of dollars and euros—if not billions—are being poured into these activities, it is only stating the obvious to say that cyberspace is being militarized. Moreover, as is the case for other weapon systems or domains of war, nations are now developing both defensive and offensive capabilities.

> **"Nearly fifty countries have actually announced the creation of cyber commands and billions of dollars are being poured into these activities"**

So the question is, "What should be done about this, and how should we regulate this activity?" I would argue that it is perhaps too early to come to a final conclusion, although most people acknowledge that regulating nation states' behavior in the cyberspace war domain is necessary. I would also argue that NATO might be the sort of platform that could serve as a facilitator to arrive at that conclusion and build norms, because in principle we are all allies in NATO and there is a certain amount of trust between NATO nations. NATO could facilitate the thinking process and make it easier to reach a conclusion. Certainly, questions like how the cyber domain is different from other domains is important, but the question that has been raised here and how we can come to a conclusion is equally important. In any case, whether we are talking about armed attacks on land, sea, air, or cyber, the decision to call it an armed attack is a political decision and the response is based on a political decision as well. So if we speak about governments, and I am speaking only about governments, the mechanisms are quite dissimilar and, as we say in NATO, we recognize it when we see it and we then come to the conclusion that this is it. So in that sense for me personally, the question is how nation states indeed would act in the cyberspace which is a warfighting domain.

I am not too optimistic that we will arrive at a quick conclusion on this because, as the previous panel mentioned, it took decades before we could agree on safety standards, for example for cars, other vehicles etc. and although the cyber domain is developing at the speed of light, it will take some time before we can build trust among different nation states and even within NATO. I do not know if it will be possible at all to reach the same kind of conclusions and arrangements we have in NATO with our conventional weapons in which a pool of weaponry and capabilities is shared under the united command of 28 allies. Maybe we will be able to arrive at a similar arrangement in cyberspace with our cyber capabilities, or maybe not. For the moment at least, it will be important to build trust through exercises by practicing together in order to create an atmosphere that will be conducive to developing policies on how we should act in cyberspace in times of conflict and in times of peace as well. This is why I am quite happy that the Center of Excellence in Tallinn has produced and published a manual on international law—a second volume is hopefully coming out soon. Without giving all the answers, this manual is a compilation of the existing international law, and I believe that, if the political will exists, it might help us come up with solutions.

> **"It will take some time before we can build trust among different nation states and even within NATO."**

To sum up, I would like to give a practical example of how thin the line is between civilian and military domains in cyberspace. We have here General Kert, who was one of the creators of the Estonian Cyber Defense League, a voluntary paramilitary organization that unites IT specialists and others who gather and exchange information. If need be, it can be placed under a military command, which would require a political decision as well. So there are many aspects to this militarization, which is a good topic to start with. But we have to go much deeper and tackle this issue, which is already developing and of which we are a part.

A Risk Management Framework for both Government And Industry

Major General David Senty, USAF (Ret)
Director, Cyber Operations, The MITRE Corporation, Former Chief of Staff, U.S. Cyber Command

I will talk about some of the challenges that we see in both describing cyber risk and cyber threats. Looking at cyber risk from both the private sector and government military perspectives, it is difficult to have a common framework of cyber risk. We worked through years of certification and accreditation schema that we thought would help supply information about the conditions of our networks, but it was a sort of one size fits all based on certain practices. Working with the national Institute of Standards, which is very much like ENISA in terms of their role or ANSSI here in France, we developed a risk management framework for both government and industry so that they can look at their sector and the threats that may come out at them given their sector, whether it is for their intellectual property, their personal information, or—if they are in the health care industry, their health records. They can then form their cyber security strategy around their risk framework and make investments accordingly. So it is now more customized to their particular sector and way of doing business.

"Working with the national Institute of Standards...we developed a risk management framework for both government and industry."

In working on the risk management frameworks, we are also looking at how to convey those decisions to a board of trustees, a board of directors, or a military commander, because they have a need to understand parameters and the risk surface of a decision. Your message is "Here is the context for our investment approach for cyber security. We have shared responsibility for this risk. How do we show our shared risk framework to you about your responsibility to understand our actions and our risk framework for having made these investment decisions?" This is not a very easy conversation. Usually, the board member will ask, "Have we been breached? That is all we want to know." So, as an approach to looking at how to convey iterative information to a board of directors or an expeditionary commander about the decisions that are being made about the network, network conditions and other things, I use an example of an old T-33—not the airplane but its radar cross-section. A radar cross-section looks like a Rorschach ink-blot, and the side lobes on the diagram are driven by the T-33 wing tanks. For stealth, you need a small RCS (radar cross section). If I am looking at a network for security, not stealth, and I have different lobes of risk, let's say, it might be a large lobe because of a single authentication—I am in an environment where I can only use only one form of authentication, not two forms, so I have a larger lobe of risk. If I achieve two factor authentication, you will see the next cross-section after I have made that adjustment and, that way, you will have a repeatable graphical reference for your decisions, tightening the loop of risk around your environment. The graphic can also depict the benefit and risk trade-offs in security investments.

Usually, a board member will ask, "Have we been breached? That is all we want to know."

I am trying this idea out on you, because we have not put a lot of energy behind this yet. Quantification of risk into a visual dimension is useful for conveying some of the things that we are talking about. We would like to know your views, because we think it is a better way to exchange information about the evolution of the network stature and posture when you are dealing with impatient board members and military commanders. It has parameters of the risk surface, it can be used to describe readiness, and it can be used with people who can understand things better when presented visually. I remember that, when General McChrystal was assigned at the Pentagon after having been in Afghanistan, he was frustrated by having to give narrative descriptions of cyber capabilities and issues instead of having a graphic that he could show in order to highlight key points such as "this is what we are going to do," or "these are the options and results."

The graphical representation can be improved beyond just something merely similar to a radar cross section. We need something more representative of not only the cyber top 10 as we would have done but which also includes other risk exposures such as electronic warfare and the physical protection of information.

We do assessments of cyber capabilities for government and industries and part of our assessment is the work force. It is hard to measure quantitatively, but you can get a sense for the work force posture and that can also be quantified over time. It is useful to have risk thresholds, similar to a barometer that can change over time. If you are going to have an unexpected connection to your network, a representative comparison of the new partner and your cyber RCS, you can get at least share a graphic of what things look like and how to improve it over time.

The Cyber Threat Intelligence Integration Center (CTIIC)

I said that I would talk about risk and threats. Threats are near to me as a former intelligence officer. What is the threat? How do we quantify and measure threats and attribution in order to provide a single answer for a decision maker, which she or he will need in order to make a political decision. We struggled with that over the last couple of years in the U.S., because there were many opinions about Sony and too many voices speaking to the senior leadership in the policy areas. Consequently, having coherence and an authoritative voice is necessary, especially given what do we do. As a result, they are forming in the U.S. a cyber threat intelligence integration center—which might be relevant to a NATO decision apparatus for cyber. It will bring an integrated cross-agency view, instead of just a signature analysis of the threat. It will provide an all-source analysis, because much of what is known about threat actors can be found in the diplomatic and economic worlds as well as the cyber signatures world. And it will provide all source context, which is very important and something that you do not want to lose by just looking at network security intelligence.

> **"How do we measure attribution to provide a single answer for a decision maker, because it will need to be a political decision?"**

Admiral Coustillière mentioned the logical physical semantic networks. I did not get to ask what he meant by semantic, but it might be the persona layer of cyberspace or it could be more contextual information. In our context, over the last two years, the questions we have had to answer very quickly were: "What is happening? What does it mean? Who is doing it? What can we do about?" And that last question—what can we do about it?—is very important in terms of a whole of government or, in the case of NATO, a whole of nations approach that is formed by that integrated view. This means that "what can we do about it" is not just cyber on cyber, as we have already discussed and as Admiral Coustilliere mentioned specifically. It can be any of the levers of government, whether economic or diplomatic, and that is part of our active defense strategy. It does not have to be non-kinetic. It can be démarche. There are many methods of dealing with some of the tension, particularly as you look at available courses of action and escalation, instead of going all in with a disconnection, or denial of service, or other such interactions. To render decisions on cyber threat actions and response opportunities, decision makers need integrated and authoritative information, in timely context for action.

> **Our response is "not just cyber on cyber... It can be any of the levers of government, whether economic or diplomatic."**

La Cybersécurité et les Enjeux Liés à la vie Privée

Mr. Eduardo Rihan Cypel
Deputy (Seine-et-Marne), French National Assembly

Je voudrais parler aujourd'hui de la cybersécurité et des enjeux liés à la vie privée face à l'avènement de l'informatique dans nos sociétés. J'ai travaillé sur ce sujet dès mon élection à l'Assemblée Nationale en juin 2012, et j'ai eu l'honneur de participer aux travaux de la Commission du Livre blanc sur la défense et la sécurité nationale, qui est le document stratégique de la France en matière militaire, de défense et de sécurité nationale. Dans ce Livre blanc, nous avons confirmé et approfondi ce qui se trouvait déjà dans le Livre blanc précédent de 2008, à savoir que les questions des cyberattaques, de cyberdéfense et de cybersécurité sont des questions hautement stratégiques pour notre pays. Nous avons traduit ces engagements, notamment dans la Loi de programmation militaire, par un renforcement financier considérable et sans précédent d'un milliard d'euros dédié à la cyberdéfense pour la période 2014-2019 dans ce que le ministre de la Défense a appelé le Pacte défense cyber. Il s'agit d'augmenter la puissance de notre pays et de préparer l'ensemble de nos infrastructures à la cyberdéfense et à faire face aux cyberattaques.

> **« la Loi de programmation militaire incorpore un renforcement financier considérable et sans précédent d'un milliard d'euros dédié à la cyberdéfense. »**

Comment Concilier Sécurité dans le Cyberespace avec la Vie Privée ?

Il reste la question qui nous occupe aujourd'hui—celle de la sécurité dans le cyberespace et comment la concilier avec la vie privée et la liberté de disposer de nos données privées. D'un point de vue politique ou même d'un point de vue de philosophie politique, nous répétons là un vieux problème—la question de la liberté et de la sécurité et comment aménager les deux—que les penseurs de la philosophie politique du 17e siècle comme Hobbs et Spinoza avaient déjà à traiter. Nous retrouvons cette question aujourd'hui avec la révolution informatique et l'avènement d'un nouvel espace, le cyberespace, qui est une nouvelle dimension de la réalité inédite parce qu'elle est totalement créée par l'homme. Ce n'est pas un espace naturel, ce n'est pas l'air, ce n'est pas la mer, ce n'est pas l'espace, c'est le cyberespace, création humaine dans un monde qui est de plus en plus interconnecté, de plus en plus lié aux technologies de l'information et aux systèmes d'information. C'est presque toute l'organisation de la société que nous devons revoir pour assurer des équilibres qui étaient uniquement dans le monde matériel physique.

Par ailleurs, le cyberespace n'est pas uniquement immatériel. Il a également des conséquences physiques puisqu'une cyberattaque peut en effet produire des dégâts matériels aussi destructeurs que n'importe quelle arme. Nous n'avons pas traité ces questions dans le Livre blanc sur la défense et la sécurité nationale et il apparaît, à travers l'ensemble des débats que l'on peut avoir aujourd'hui, que ces équilibres ne sont pas complètement trouvés. Pour nous français et en tout cas, pour moi qui suis parlementaire, je crois que la question des cyberattaques et de la cybersécurité pose trois enjeux de souveraineté : il s'agit d'abord d'assurer la souveraineté de l'Etat à travers l'ensemble de son organisation puisque on peut porter atteinte aux infrastructures vitales de la société et porter ainsi atteinte à l'appareil d'Etat et à son fonctionnement, donc à l'ordre public en général. C'était l'objet du Livre blanc sur la défense et la sécurité nationale, de la Loi de programmation militaire, et de l'ensemble des dispositifs qui les accompagnent. La deuxième souveraineté concerne tout ce qui relève des entreprises et des industries puisque il n'y a pas un jour en France, et c'est sans doute pareil dans le reste du monde, sans cyberattaques contre des entreprises, soit pour piller leurs informations, soit pour chercher à détruire des infrastructures ou déstabiliser des entreprises industrielles. La troisième souveraineté, et c'est peut-être celle qui nous concerne davantage aujourd'hui, est la souveraineté des citoyens. Malheureusement, on n'en parle pas suffisamment de manière à permettre de trouver des solutions puisqu'a travers la question de la protection des données personnelles, nous devons assurer la souver-

> **« La souveraineté qui nous concerne davantage aujourd'hui est la souveraineté des citoyens. »**

aineté des citoyens. Aujourd'hui, la vie concrète des gens est de plus en plus en ligne dans le cyberespace, avec des données à la fois personnelles, qui vont de la photo, du texte très personnel qui n'a d'intérêt que pour l'individu ou la famille, jusqu'à des données qui peuvent être beaucoup plus lourdes de sens pour l'individu puisqu'elles peuvent concerner, par exemple, la sécurité sociale, des données bancaires, toutes les données qui peuvent intéresser la cybercriminalité.

La Prise de Conscience Mondiale de la Nécessité de Protéger les Données Personnelles

Je crois qu'il y a deux dimensions a traiter aujourd'hui : il faut sans doute avancer sur le plan réglementaire et législatif. C'est très difficile parce chaque pays joue sa carte, personne ne veut réguler au maximum afin de pouvoir bénéficier d'un « espace gris » sur le plan juridique sur lequel il est possible éventuellement d'opérer au profit d'autres intérêts qui so nt tout à fait légitimes et également d'état. Il n'y a pas actuellement de législation suffisamment importante pour pouvoir faire face aux enjeux liés à la protection des données personnelles. Ce besoin de protection va aller en grandissant avec les objets interconnectés, les imprimantes 3D etc., et toucher l'ensemble de la société car il touche la vie intime des gens, mais c'est peu visible parce qu'il n'y a pas encore de prise de conscience massive chez les individus. L'autre protection importante doit venir des citoyens et des individus eux-mêmes, qui n'utilisent pas toujours tout ce qui est à leur disposition pour protéger par exemple leur ordinateur ou smartphone personnels. Nous avons besoin de travailler en synergie avec le monde des entreprises et industries pour que l'ensemble des objets, ordinateurs, logiciels, smartphones, tout ce qui sera créé et interconnecté, puisse disposer d'un minimum légal de protection des données personnelles. Il faut aujourd'hui que cette prise de conscience se fasse dans la société pour qu'elle puisse être anticipée en amont par les industries et les entreprises. On peut prendre en exemple un objet connu, l'iPhone, dont Apple a justement renforcé le niveau de protection, ce qui n'a pas nécessairement plu à un certain nombre d'entités étatiques, mais ce renforcement a été fait sous la pression des citoyens.

> **« Il n'y a pas actuellement de législation suffisamment importante pour pouvoir faire face aux enjeux liés à la protection des données personnelles. »**

Aujourd'hui, il faut continuer à débattre pour cadrer de plus en plus la protection des données personnelles sans pour autant entraver le travail nécessaire des institutions qui ont vocation aussi à sécuriser l'Etat, les entreprises et les industries tout comme les citoyens. Pour l'instant, ce chemin ne paraît pas tout à fait satisfaisant et c'est l'enjeu qui nous reste à définir. Un élément positif que j'ai observé dans l'affaire Snowden, c'est qu'elle a permis une prise de conscience au niveau mondial, national, et partout où cela était possible, de la nécessité d'aborder la question de la protection des données personnelles. Je ne crois pas en des systèmes rigides et je ne pense pas que tout se fera par la loi ou par les organisations internationales. Cette question devra bien sûr un jour ou l'autre être débattue aussi à l'ONU ; cela dépendra de la capacité des nations à vouloir le faire mais c'est un débat qui viendra parce que, au fur et à mesure, les citoyens prendront conscience que c'est quelque chose qui touche au plus près de leur intimité. Je crois, et c'est ma conclusion, que c'est un mouvement d'ensemble de la société qui permettra d'avancer et d'anticiper des produits qui seront plus efficaces pour protéger la vie intime des gens et le cas échéant, protéger un certain nombre de systèmes qui sont aujourd'hui plus vulnérables parce qu'il n'y a pas encore eu cette prise de conscience. Il faut noter qu'en France, il existe une différence entre les grandes entreprises qui sont mieux armées et les petites et moyennes entreprises qui n'ont pas toujours pris conscience des risques qu'elles encouraient. Il y a une image que je donne très souvent: quand vous sortez le matin de votre maison, vous ne laissez pas la porte ouverte ou avec les clés à l'extérieur. Vous fermez tout sauf si vous êtes dans un pays où il n'y a pas de problèmes de sécurité. C'est la même chose pour les objets—ordinateurs, smartphones, et objets interconnectés. Pour résumer, il faut continuer de faire pression et de mener un travail à la fois au niveau international et Européen. Les Européens doivent travailler sur ce sujet pour définir des normes, définir des règles, et la société elle-même devra se mettre en mouvement pour que les entreprises puissent protéger en amont les produits qui sont destinés au public.

> **« L'affaire Snowden…a permis une prise de conscience au niveau mondial, national, et partout…de la nécessité d'aborder la question de la protection des données personnelles. »**

Cybersecurity Issues Linked to Privacy

Mr. Eduardo Rihan Cypel[1]
Deputy (Seine-et-Marne) French National Assembly

The advent of information technology in our societies has brought about cybersecurity issues that have affected our privacy. I started working on this subject when I became a French National Assembly's deputy in June 2012 and had the privilege of participating in the development of the French White Paper on Defense and National Security—France's strategic document for military, defense and national security matters. In this White Paper, we confirmed and expanded what the previous White Paper of 2008 had already stated, i.e., cyberattacks, cyberdefense and cybersecurity issues are of the utmost importance for our country. We translated these commitments in the Military Programming Law by adding for the 2014-2019 period a considerable and unprecedented financial reinforcement of one billion euros specifically for cyberdefense. Our Minister of Defense called it the Defense Cyber Pact. Its goal is to increase our country's power and prepare our whole infrastructure for cyberdefense and cyberattacks

> **"The Military Programming Law added…a considerable and unprecedented financial reinforcement of one billion euros specifically for cyberdefense."**

How Can Cyberspace Security Be Compatible with Privacy?

Can we find a balance between security in the cyberspace and privacy, which is the right to protect our personal data? From a political or political philosophy point of view, we are confronted with an old problem— how to reconcile freedom and security—that 17th century political philosophers like Hobbs and Spinoza already had to deal with. The digital revolution and the advent of the cyberspace, which is a new dimension of reality entirely created by man, have brought this problem to the forefront again. Cyberspace is not a natural space, it is not air, sea, or space; it is a human creation in a world that is increasingly connected and linked to information technology and information systems. This will require us to revise practically the entire organization of our society in order to create balances that were only found previously in the physical world. The cyberspace is not completely intangible either. It can have physical consequences too since a cyberattack can cause material damages that are as destructive as any weapon could be. We have not addressed these questions in the White Paper on Defense and National Security, but it seems clear from the current discussions of these issues that a balance has not been found quite yet.

> **Cyberspace "can have physical consequences too since a cyberattack can cause material damages that are as destructive as any weapon."**

As a member of the French Parliament, I view cyberattacks and cybersecurity as raising three sovereignty issues: first, we must secure the sovereignty of the state in its entire organization since an attack against our country's critical infrastructure is an attack against the proper functioning of the state and a disturbance of the public order. This was the purpose of the White Paper on Defense and National Security, the Military Programming Law, and their supporting provisions. The second sovereignty concerns everything that is relevant to companies and industries since cyberattacks against companies to plunder their information, destroy their infrastructure or destabilize businesses are daily occurrences in France and most likely in the rest of the world as well. The third sovereignty, which is perhaps of particular concern today, is the sovereignty of our citizens. Today, people spend more and more time online and in cyberspace. The data they share can be personal—photos, private messages that are only of interest to friends and family—or important documents that are directly relevant to the individual such as social security or banking data and all data that can be of interest to cybercriminals.

> **"the sovereignty of our citizens… is of particular concern today."**

1 Translated by Anne D. Baylon, *Proceedings* Editor.

The New Global Awareness that Personal Data Must be Protected

I believe that there are two ways to protect personal data: one is to move forward on the legislative and regulatory levels. This is difficult to do because countries like to play their own game and stay away from maximum regulation in order to enjoy a legal "grey area" that they can potentially use for other legitimate or state interests. Currently, no legislation is powerful enough to protect personal data but the need for legislation will grow with the development of interconnected objects, 3D printers etc., and it will affect our societies because it affects people's personal lives. This need is barely visible at the moment since individuals have not become fully aware of it yet.

> **"No legislation is powerful enough to protect personal data but the need for legislation will grow."**

The other important protection must come from citizens and individuals themselves who often fail to use what is a their disposal to protect their personal computers or smartphones. We need to work in synergy with businesses and industries so that whatever objects are created and become connected—computers, software, smartphones as well as the personal data they contain—can benefit from a minimum legal protection. This awareness must take place in our societies now if businesses and industries are to anticipate it. For example, Apple has reinforced its iPhone's level of protection, a decision that a number of states may not have necessarily appreciated, but this reinforcement was the result of citizen pressure.

We must keep discussing how to protect personal data without interfering with the essential work done by institutions that are in charge of securing the State, businesses and industries, and all the citizens. For the time being, this path is not quite satisfactory and it will be our job to define it. The Snowden revelations have produced a positive outcome, which was to create at global and national levels the awareness that personal data had to be protected. I do not believe that rigid systems will work and doubt that everything will be accomplished by legislation and international organizations. Of course, this question will have to be debated at the UN at some point: it will depend on nations' willingness to do so but this debate will take place as citizens come to realize that it is at the heart of their private lives.

In conclusion, anticipating the products that will most effectively protect people's personal data and systems that are more vulnerable today because this awareness has not taken place yet will require an overall social movement. In France, there is a difference between large corporations that are more resilient and small and mid-sized companies that are not always aware of the risks they are taking. I like to give this comparison: when you leave your house in the morning, you do not leave the door open or keys in the keyhole. You lock everything unless you happen to live in a country where there are no security issues. It is the same for objects—computers, smartphones, and objects that are interconnected. In summary, we need to maintain the pressure at the international and European levels. Europe will have to work on this subject to define norms and rules and society as a whole will have to move forward so that businesses can think ahead and create products that will protect the public.

> **"The Snowden revelations have produced a positive outcome, which was to create at global and national levels the awareness that personal data had to be protected."**

Privacy in the 21st Century

Mr. Karsten Geier
Head, Cyber Policy Coordination, German Foreign Ministry

Last June, German Foreign Minister Frank-Walter Steinmeier gave a speech on international cyber policy. Building on Abraham Lincoln's famous phrase, he proposed an "Internet of the people, by the people, for the people." Foreign Minister Steinmeier called for an internet "of the people", i.e. a decentralised global commodity. Secondly, he argued that the internet should remain an internet "by the people," a multi-stakeholder space. Thirdly, the Foreign Minister called for an internet "for the people." Digitalization and the internet have already radically changed our lives, but the changes brought about by the internet will accelerate even more in the future. Take industry, for example: we are now at the start of the "Internet of Things," or in more technical terms, of "Industry 4.0." However, internet "for the people" means something else, too: equal opportunities in the digital sphere. If we do not succeed, if the internet is closed off to some or state-controlled or simply unaffordable, tomorrow's world will be even more unequal than today's. The internet has become too important, the repercussions of "cyber" in the real world too resounding to be put in danger. The consulting firm McKinsey estimates that during the last 5 years, the internet has contributed twenty-one percent to GDP growth in advanced industrial countries. Three quarters of this contribution are in the traditional, non-IT economy. And there is more: the very data generated in the process of using modern communication and information technologies creates opportunities. It allows firms to tailor their products to consumers' needs and decision makers to target scarce resources.

Or consider the importance of social media: one third of all people in Germany are on Facebook; many others are on LinkedIn; Germany is among the top ten countries in terms of Twitter usage. Figures are similar or higher in other advanced industrialized economies. And we should not limit our view to middle class families "liking" photos of cute babies and funny-cat-videos on Facebook and YouTube: The waves of refugees that are flowing into Europe as we speak are turning to social media for orientation and inspiration. It is important to note that from the point of view of a person fearing for dear life in Homs or Aleppo, the internet may hold the keys to safety.

The internet offers unimaginable chances and opportunities. It can help increase economic growth and innovation, foster freedom of information and expression, allow access to ideas and enable democratic participation in a knowledge society. The internet allows a truly global discourse, not between leaders, but between citizens. It creates opportunity for education and science— students are pursuing degrees from universities in distant countries; scientists around the world collaborate on research projects without having to leave their home labs.

> **"Many countries–not only authoritarian regimes–harbor fears that online communication can be destabilizing."**

Cyber technology also has introduced a new dynamic into the relationship between the state, society, and the private sector. Many countries—not only authoritarian regimes—harbor fears that online communication can be destabilizing. One reflection of this can be found in the Russian-Chinese proposal for a "Code of Conduct," containing multiple provisions that aim at restricting freedom of speech and information online. Even among NATO allies, there are varying views on issues such as hate speech online, the use of the internet for terrorist propaganda and recruiting, the use of social media for organizing and mobilizing political opposition, and also the right to privacy in the digital age.

The Universal Right to Privacy

In the face of these challenges it is important to maintain a clear, coherent and coordinated narrative. One important point of this narrative has to be that individuals enjoy the same universal human rights "offline" as "online". This includes not only freedom of expression—including the freedom to seek and impart information—and freedom of assembly and association, but also the right to privacy, enshrined in the Universal Declaration of Human Rights as well as the International

Covenant on Civil and Political Rights. The UN General Assembly and the UN Human Rights Council have just recently reaffirmed the interdependence of these rights, with the consensual adoption of three important resolutions.

The right to privacy has proven to be a particularly thorny issue. The discussion comes down to difficult questions, such as whether States have the right to collect unlimited electronic data on individuals, or whether States have the right to insist that the business community (i.e. private IT service providers) assist in doing so. An argument can be made that in times of crisis and in an age of global terrorist threat, the state has the right, even the obligation, to do so to avert potential dangers from society. Others hold that piling up a haystack does not make finding the needle any easier. Beyond such arguments of practicality: the very essence of democracy requires that every person retains a personal space free of state surveillance and interference. If such a space is missing, if every message we write, every phone call we make, even every step we take are recorded, how can opinions be formed, controversies be fought out?

"...the essence of democracy requires that every person retains a personal space free of state surveillance and interference."

The debate leads to acknowledging the importance of necessity and proportionality, and to the question of how to ensure that they are universally respected. This past summer, the Human Rights Council has appointed a Special Rapporteur on the Right to Privacy. In the future we can expect annual reports from Joseph Cannataci, who is also mandated to identify possible obstacles to the promotion and protection of the right to privacy, report on alleged violations, identify and promote principles and best practices.

Another part of the debate on the right to privacy addresses a set of question that arises when discussing the collection, storage, processing and analysis of personal data not by states, but by private companies. Some firms associated with the use of such data are facing critical questions on their respect of individuals' privacy rights. Unless clients are satisfied with the answers, these firms' business may suffer. The European Court of Justice laid down some important markers in its 8 April 2014 decision on the European Data Retention Directive. The Court made clear that within its jurisdiction— the 28 Member States of the European Union—the retention of personal data, when it is wide-ranging and particularly seriously interfering with fundamental rights, needs to be sufficiently circumscribed to ensure that interference is actually limited to what is strictly necessary. In its 6 October 2015 decision in the case of Maximillian Schrems v Data Protection Commissioner, the Court added that legislation permitting the public authorities to have access on a generalized basis to the content of all and everyone's electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life. Likewise, the Court observed that legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, compromises the essence of the fundamental right to effective judicial protection, the existence of such a possibility being inherent in the existence of the rule of law.

Drawing on these decisions, two points seem of particular importance concerning states' access to citizens' data online: (a) limit access to personal data to what is strictly necessary—this implies appropriate political oversight; and (b) provide for appropriate and effective legal remedies. The European Court of Justice has stated that full control of compliance with the requirements of data protection and security, carried out on the basis of EU law, is an essential component of the protection of individuals. This jurisprudence subjects the transfer of personal data beyond the confines of the European Union to clear conditions—and in effect may even set limits to it. In light of its potentially tremendous importance for the future of international data flows, allow me to emphasize one point: European insistence on data protection has nothing to do with protectionism, favoring a "Euro-Cloud" or "Schengen-Routing;" it is motivated by a deep-seated concern about fundamental rights.

"Jurisprudence subjects the transfer of personal data outside the European Union to clear conditions."

My personal summary is as follows: Data privacy is an issue of personal freedom. Those who sacrifice personal liberty for the sake of safety will end up with neither. This, of course, is a line stolen from Benjamin Franklin. What rang true 250 years ago in North America still resounds around the world today.

International Approaches to Tackling Cybercrime: A UK View

Mr. Nick Dean
Head of Cyber Policy, United Kingdom Foreign and Commonwealth Office

A Transnational Cybercrime

The UK was recently recognised by the G20 as the most cyber-dependent economy in that group. It means that protecting UK users from network intrusions that could cause harm to them is a clear government priority. The UK Government listed this priority in the 2010 National Security Strategy as a top tier risk, alongside terrorism, natural disaster and conventional conflict. Cybercrime represents the most prevalent online threat to UK interests, and the true scale of it is unclear, as are the exact costs it imposes. We see cybercrime as being transnational, and the methods and practices used by criminals change rapidly. The criminal marketplace is maturing quickly, and the 'industrialisation' of cybercrime is clearly taking place. Russian language-speaking organized criminal groups in Eastern Europe and neighbouring states represent some of the most capable criminal actors, with a particular focus on financial crime.

"Cybercrime represents the most prevalent online threat to UK interests... cyber-criminals in Russia and neighbouring states represent some of the most capable criminal actors"

We see a growing threat from blended multi-stage attacks: for instance a DDOS attack to divert network defenders' attention from a more damaging intrusion. Looking ahead, we are concerned by the vastly growing 'attack surface' that technical progress in cyberspace brings. In October 2015, the UK Government started to measure cybercrime in our official crime statistics for the first time. This resulted in more than doubling the reported incidence of crime in the UK to 5.1 million per year (although it should be recognised that this was largely the result of the change in the reporting procedures). We observe traditional criminals carrying out cybercrime activity to an increasing degree.

We observe traditional criminals carrying out cybercrime activity to an increasing degree.

Tackling Cybercrime Requires an International Response

Given the transnational nature of cybercrime, we need to have an international response. We are active in encouraging this in three ways:

- *Harmonising legislation:* we see the Council of Europe's Budapest Convention as the best way to do this. It represents a high-quality set of legislation and practices for cooperation. The UK Government is also active in working with a range of jurisdictions to improve or bring their legislative processes into line with others.

- *Building law enforcement capability through capacity building:* the Foreign and Commonwealth Office holds a fund for capacity-building for improved cybersecurity and spends over £2m per year in support of this work. We have worked with law enforcement colleagues around the world to share best practices.

- *Supporting international cooperation:* including through our participation in EUROPOL's European Cybercrime Centre (EC3) in The Hague, the Joint Cybercrime Action Taskforce (J-CAT) operational taskforce for 24/7 sharing of threat

information, and the Council of Europe's centre in Romania.

This cooperation has resulted in an increase in the number of large-scale operations we have been able to mount with overseas law enforcement. But challenges remain, including how to scale up this activity in order to tackle the increasing criminal use of cyberspace. We are committed in particular to tackling online child sexual exploitation, which we see as one of the most significant manifestations of cyber-enabled crime. In late 2014, the British Prime Minister hosted a ground-breaking #WeProtect Children Online Global Summit in London, which saw governments, civil society and the private sector from over 50 countries coming together to pledge action against criminals, to identify and protect victims, and to track down and take steps against indecent images and videos. The UK also launched a global fund to support this work, run by UNICEF, and pledged £50m over five years.

Japan's Cybersecurity Policy

Mr. Atsushi Saito
Director, Space Policy Division, and Senior Negotiator for International Security Affairs, National Security Policy Division, Japanese Foreign Policy Bureau

The Current Cybersecurity Situation in Japan and the Asia-Pacific Region

As the only Asian participant in the workshop, I would like to address Japan's cybersecurity policy in the context of the Asia-Pacific region. Cyberspace has developed as a free space, primarily through the initiative of the private sector, and has become an indispensable domain. At the same time, the use of cyberspace has raised serious concerns in Japan due to powerful cyberattacks that have targeted government entities. In May 2015, the Japan Pension Service, which administers people's pensions, was hacked, resulting in the theft of more than 1.25 million personal data. Cyber-attacks have also targeted the private sector. In 2011, Japan's biggest defense contractor, Mitsubishi Heavy Industries Ltd, was attacked by foreign entities in the first known cyber attack on Japan's defense industry.

"In May 2015, the Japan Pension Service, which administers people's pensions, was hacked, resulting in the theft of more than 1.25 million personal data."

Japan views the digital divide and the cybersecurity vulnerabilities of developing countries as another source of concern. While cyberspace has greatly contributed to the rapid economic growth of the countries in the region, their cyber security systems have not yet reached a satisfactory level. In addition, some governments are trying to impose excessive state control over the cyberspace, which is another matter of concern for Japan—a country that cherishes the principles of free flow of information as well as fundamental human rights, including the freedom of speech in cyberspace.

Japan's 2015 Cybersecurity Strategy: Objective and Basic Principles

Objective. Under the strong initiative of Prime Minister Shinzō Abe, Japan's Cybersecurity Strategy was approved in a September 2015 cabinet meeting. This strategy sets the objective to "Ensure a free, fair, and secure cyberspace; and subsequently contribute to improving socio-economic vitality and sustainable development, building a society where the people can live safe and secure lives, and ensuring the peace and stability of the international community and national security."

Five Basic Principles. In order to reach this strategy's objective, Japan has affirmed five basic principles:

- *The Assurance of the Free Flow of Information.* "It is imperative to create and ensure a cyber environment where the transmitted information will be neither censored nor altered without any legitimate reason, and will be delivered to intended recipients. … [and] maintain the proper balance between necessary regulations and the protection of privacy. "

- *The Rule of Law.* "The rule of law should be thoroughly applied to cyberspace in the same way it is applied in the physical space… International law and other international rules and norms are applicable to cyberspace, and thus cyberspace should be governed by the rule of law in an international context as well."

- *Openness.* "Cyberspace must not be exclusively dominated by a certain group of actors, but must be open to all people who want to utilize it."

- *Self-governance.* "With a view to achieving the coexistence of order and creativity in cyberspace, Japan respects self-governance capabilities that the Internet has developed, and regards every stakeholder's self-reliant activities for the Inter-

net management as the basic foundation of cyber governance"…

- *Cooperation among Multi-stakeholders.* "Cyberspace is a multi-dimensional space composed of various stakeholders' activities in a variety of layers. From this viewpoint, it is necessary for the Government and all cyberspace-related-stakeholders, including Critical Information Infrastructure (CII) operators, enterprises, and individuals, to share a common vision of cybersecurity and fulfill their organizational responsibilities and duties or make individual efforts."

Japan's Diplomatic Efforts

Japan's basic policy for national security is to further contribute to the peace and stability of the Asia-Pacific region and international community. For cybersecurity, Japan has been promoting three kinds of efforts, or three main pillars.

International Rule-making. First, Japan is seeking to enhance the cyber dialogue with like-minded countries such as the EU countries in order to promote international rule-making, i.e., the establishment of the "Rule of Law." This does not mean control by the state or any other power, but seeks the creation of "international rules" to control "wrongful" international activities in cyberspace, in compliance with the universal values of freedom and democracy. When countries have different perspectives, such as China and Russia, Japan has called on them to take a responsible role in the international community. Our country is taking part in various frameworks. It has contributed to the UN Group of Governmental Experts on Cybersecurity (GGE) for enhancing the rule of law; it has participated in the London Process and the Global Conference on Cyberspace, whose goal is to create global perspectives on security, freedom, and economic and social benefits through a multi- stakeholder approach. Through the framework of the Cybercrime Dialogue with ASEAN countries, Japan and ASEAN countries have focused on countering terrorism and cyber crime and stressed cooperation among relevant agencies.

"When countries have different perspectives, such as China and Russia, Japan has called on them to take a responsible role in the international community."

Confidence-Building Measures. The second pillar is the promotion of transparency and confidence-building measures. Japan considers it important to improve and expand confidence-building measures in peacetime in order to reduce the risk of escalation between parties that may lead to cyber conflict. To this end, we have been discussing the current cyber environment, including global and national cyberthreats and international and regional engagements, at the Japan-China-Korea Trilateral Cyber Dialogue and at the Japan-Russia Cybersecurity Dialogue. We are also promoting cooperation among national CERTs as well as in the CyberGreen project of the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC). The aim of this project is to check for internet infections and malicious activity. Accordingly, we try to establish global internet visibility by demonstrating cyber health and risk conditions. Cooperation among national CERTs in this regard will help promote cybersecurity transparency in the world. Japan is also contributing to regional forums, such as the Asean Regional Forum (ARF), in order to enhance confidence-building and promote transparency.

Capacity-building for developing countries. As a third pillar, it is essential to strengthen the capacity-building assistance and human resource development of CERTs, law enforcement agencies and other relevant entities in developing countries to address their vulnerabilities in cyberspace. Japan will cooperate and share experiences with developing countries, particularly ASEAN member states, including through the Information Security Policy Meeting.

The Way Forward

Japan shares common universal values such as freedom, democracy and the rule of law. We believe we can contribute to the peace and security of cyberspace by acting as the Asia-Pacific region bridge between like-minded countries and countries with different perspectives on cybersecurity frameworks. We will work to promote the rule of law in cyberspace and develop a comprehensive and effective cyber diplomacy through confidence-building and capacity-building measures focused around the Asia-Pacific region.

How Can Insurance Companies Contribute to the Prevention of Cybercrime?

Ingénieur général des mines Henri Serres
High Council for Economy, Industry, Energy and Technology,
French Ministry of the Economy and Finance

As the risks of cyberattacks keep growing, the insurance sector has the potential to provide a better protection for economic activities and make companies, especially small and medium enterprises, more competitive. But the different stakeholders tend to look at the development of these insurance activities with a certain amount of hesitation: prospective clients are not fully convinced of the real added value of having a specific cyber insurance, as compared to their current contracts. They also seem to underestimate the impact of cyberattacks on their commercial activity.

On their side, insurance and reinsurance companies are welcoming the growth potential of this new activity, although they seem reluctant to face excessive risks since they have no history of past events and often lack human expertise in cyber security. They are concerned by the rapid evolution of technologies, which would make an initial audit obsolete much faster than, for instance, a fire insurance policy audit. They also worry about he possibility of systemic attacks, which could hurt a large number of their clients at the same time and compound their losses.

"...insurance companies welcome the potential of cyber insurance, but they seem reluctant to face excessive risks, including a history of past events"

Insurance as an Important Addition to a Company's Risk Management

With better threat prevention, "...investments in cyber security could lead to a lower rate of insurance costs."

We believe that we should prove movement by action, and promote a better consciousness of economic actors. By increasing the threat prevention level, we hope to build a win-win situation where investments in cyber security could lead to a lower rate of insurance costs. A larger number of contracts would allow insurance companies to refine their economic model of residual risks, thus leading to gains for both sides.

Top management must take action to protect the continuity of activities and bridge the gap between risk managers and chief information officers; consultants can be very efficient in providing technical, legal, crisis management advice that can complement insurance contracts; governments should also be involved in promoting exchange of data, certified security products, specific rules for critical infrastructures, as is done in the French legal system.

Finally, through data protection legislation and ENISA's expertise, Europe could bring about a decisive momentum. Currently cyber insurance is mostly developed in the United States. This is due to a 2003 California state regulation that makes it compulsory for companies to notify all their customers of data protection infringements. This legislation was subsequently and widely adopted by other states. While insurance is not a substitute to good cyber security, it can be an important addition to a company's overall risk management. Insurers can help guide and encourage significant improvements in cyber security practices. Companies, especially outside critical infrastructures and regulated sectors, need to upgrade their risk management, introducing stress testing and top management coordinated recovery plans, bringing together finances, operations, and communication.

Trends in Internet Infrastructure Attacks

Mr. Jim Cowie
Chief Scientist, Dyn Research

When we read about threats to critical infrastructure, we are often thinking of gas pipelines, the water supply, the railroads, the power grid, and so forth—the networks that deliver the resources that society depends on. Today I will describe some trends in infrastructure attacks that focus instead on the particular vulnerabilities of information networks, and share with you how the internet operations community tends to think about the operation and protection of critical infrastructure. I will review three surprising ways in which the information infrastructure is vulnerable at a very low level.

On the operations side, we sometimes say that we will be happy when there is no more critical information infrastructure, that we have done our job right when the term itself becomes meaningless. The very term "critical internet infrastructure" implies the existence of single points of failure (buildings, cables, landing stations, physical switches) whose failure would cause a serious problem with the flow of global information. Our goal as a community is for the internet to grow and diversify and create enough built-in redundancies that ultimately there will be no more critical infrastructure to defend, which is an unusual perspective. Today, its safe to say that we are not there yet.

Three Different Types of Critical Infrastructure Attacks

Before I start, it is important to calibrate our mental model. These kinds of information infrastructure attacks are different, in some fundamental ways, from traditional security threats. When we think about the word "attack" in the classical sense, we imagine someone breaking into our house, and taking our television set or our wallet.

When we think of a cyberattack, we might be thinking along similar lines: the bad guys are after specific resources, specific pieces of information, that they want to take from our locked houses. But an infrastructure attack takes place at a different level of abstraction: for us, it would be like taking control of the streets, or of the air itself through which objects move, in order to accomplish the attacker's goals on a much broader scale. These are cyberattacks in the purest sense, that do not really have direct counterparts in the real world.

Let me summarize three different types of infrastructure attacks without necessarily distinguishing the motivation, whether that is to draw attention (terrorism) or divert attention (financial crime). Today we are after a basic understanding of the methods and their potential for harm.

IP Squatting

> **"If you have heard about IPv6, you know that we have exhausted the pool of IPv4 addresses that are used to uniquely number each of the computers and things on the internet."**

The first vulnerability I would like you to be familiar with is called IP squatting. If you have heard about IPv6, you may be aware that we have exhausted the pool of IPv4 addresses that are used to uniquely number each of the computers and things that communicate on the internet. As a result, all the numbers we had in the old system, which is still going strong, are actually becoming valuable. These numbers are no longer simply given away; there is now a burgeoning commercial market for them, and they can be traded like any other intangible asset on a corporate balance sheet. It currently costs about ten to fifteen dollars per IP address on the open market, and as you would expect, there are white, grey, and black markets for IP addresses. Dyn monitors the world's use of internet address resources within the Border Gateway Protocol (BGP) by service providers around the world. We commonly see people actually taking other people's address blocks, using them to connect machines to the internet by making false advertisements in BGP, and not

paying anyone.

For example, one group in Saint Petersburg has been taking idle IP address blocks from people who did not even realize that their space was being borrowed. They might use this borrowed space to help other people establish a presence on the internet for propagation of malware, hosting of botnet command and control, or sending spam. It is purely commercial. In another example, the Italian National Institute for Nuclear Physics had their space borrowed and used in January, then put right back in the pool. Would your organization be equipped today to determine that such a thing had even happened, let alone pursue the squatters?

"One group in Saint Petersburg has been taking idle IP address blocks from people who did not even realize that their space was being borrowed."

A couple of weeks ago, at a network operators' conference in the Ukraine, I described a situation in which blocks of IP addresses were borrowed from (among other sources) the Brazilian Home Shopping Network. The borrowers were very careful to cover their tracks; in the global routing system, the borrowing was crafted to look like legitimate use by various Brazilian internet Service Providers. It was actually being used by unknown persons in the People's Republic of Donetsk in Eastern Ukraine. This was very mysterious and, although the space did not belong to these people in Donetsk, it did not stop them from recycling that space. So, if you thought that cyberattack attribution based on endpoint IP addresses was hard before, it has just become a lot harder.

The Interception Threat

The second attack is a refinement of the IP squatting attack, to create an active interception capability. If you can borrow space through BGP hijacking—remember, this is the manipulation of the underlying routing protocols—the other thing you can do is get in the middle of secure communications; that is, create an interception threat. Back in February 2014 in Montreal, some people creatively rewired internet routing to interpose themselves between bitcoin miners and the people giving out bitcoin tasks. They were then able to substitute their own tasks and get people to mine bitcoins for them, making about $80,000 dollars from a short experiment. They might have been doing it for fun, but it was a reasonable amount of money. Here in Paris, if you are a wine aficionado, just think in terms of 8 bottles of Grand Cru, or 800 bottles of Premier Cru.

More seriously, in March 2015, a Ukrainian organization hijacked a number of British Telecom address blocks. If you ran a network traceroute during this period and were trying to send a message from Houston to London to an address in one of these blocks, you would actually see a path from Houston through Kiev to London. The potential victims were primarily corporate organizations: Pepsi, Walmart UK, the underwear company Fruit of the Loom, but also the United Kingdom Atomic Weapons Establishment.

"A Ukrainian organization hijacked a number of British Telecom address blocks...The potential victims were primarily corporate organizations: Pepsi, Walmart UK...but also the UK Atomic Weapons establishment."

Now, the damage from such an attack should be pretty limited, because we assume everyone is using good end-to-end encryption over the internet, particularly government organizations and corporations who care about data security. Right? A few months later, though, a paper called the Logjam Exploit was published (https://weakdh.org/) showing that you could use a flaw in Diffie-Hellman key exchange to weaken or break the crypto used to protect a large percentage of all secure websites. And if you could get in the middle of a conversation, you had a chance to record handshakes and examine the traffic later after decrypting it. It casts these kind of traffic redirection attacks in a new light, and the timing here was really unusual.

The Threat to the Deep Infrastructure

The final threat I will describe affects the physical information infrastructure: the cables and facilities that, unsurprisingly, are vulnerable to physical attack. This is an easy one for us to study because, fortunately or unfortunately, infrastructure damage at that level happens a lot. Most of it is very innocent and accidental (think of fishermen catching cables in their nets, or ships running over cables with their anchors), and we do have good maps now. After years of observation of the global internet's failure modes, we have accumulated pretty good data about what happens in all the different parts of the world when particular cables go out. So we do not have to game this and play "What if?"

For example, a recent fault on the IMEWE cable transiently impacted internet communications in Pakistan and Lebanon. Last week, Algeria lost 80% of its connectivity because of a fault on the SEA-ME-WE4 cable. In Iraq, the GBI cable that is extremely important for the connectivity in Southern Iraq has been having problems for the past couple of weeks. When their traffic fails, however, it fails over to terrestrial routes through Iraqi Kurdistan, so they are fine—an example of diversity in action.

"In March 2013, the Egyptian navy intercepted off the coast of Egypt a boatload of divers who were supposedly attempting to damage a critical submarine cable."

This sort of thing happens all the time and we do not hear much about it, because problems of that sort are anticipated. But when it is not an accident, when it is not simply a technical fault, we get more worried. In March 2013, the Egyptian navy intercepted off the coast of Egypt a boatload of divers who were supposedly attempting to damage a critical submarine cable. In Eastern Libya, someone blew up the landing station for the Silphium cable in order to prevent connectivity from coming to Benghazi.

We normally think that governments are the ones shutting off the internet, but as these cases suggest, intentional internet disruption can be a game played by all kinds of actors. Consider the scenario after Maroc Telecom bought out the local phone company in Gabon, as local protestors took down the internet as a form of work stoppage, both by attacking the facilities and damaging the cables. In December 2013, Thailand protestors who were upset with the government's coverage of the protests broke into the nation's central telecommunications facility and switched off the internet. Are these actions cybercrimes, or a legitimate form of protest?

Of course, the potential for geopolitically-motivated cable damage was in the news this year, as Russian submarines were reported to be aggressively operating near the vital undersea cables that carry almost all global internet communications. The media significantly exaggerates the threat, but to what degree?

We have conducted research to determine the level of resilience of every country on the globe and rank them in order. Uzbekistan comes up as the most fragile country, with just one or two paths into the country taking all the traffic. The United States, on the other hand, is probably the most resilient, with tens of thousands of paths. I would hope that this kind of research will take some of the stress out of the discussion over Atlantic cable disconnection. I think that in a worst-case scenario, we could see a lot of local damage but we would not see broad damage to the internet. Financial people who depend on special-purpose connectivity to trade between London and New York on the lowest latency cables would be very upset if they lost those, but by and large, the connectivity that supports the United States, with consumers accessing content by using dry land cables inside the United States, would still be available. The American internet would survive.

I will wrap up with one observation, based on our previous discussions today of the role of radicalization and social network effects in combating terrorism. I am not a cybersecurity expert, or a public policy specialist, like most of you. I am here as a visitor from a different social network, a network of people who either run the internet, or who know how to provide accurate, objective information about the internet's operation from minute to minute. Our social networks are largely disjoint, but probably of similar size and global span. It would be very interesting to make random connections between these networks, bypassing traditional vendor relationships to promote dialogue between the internet's technical specialists and the policymakers, without necessarily respecting our traditional professional hierarchies. If I can "radicalize" you into joining my social network today, I encourage you to do so!

Concluding Remarks

Major General (ret.) Robert Ranquet
Former Deputy Director, Institute for Higher Defense Studies, (IHEDN)

This will be a seminar to remember! Actually, this year is the tenth anniversary of the first time when the International Workshop on Global Security first came to France. This was back in 2005. That year, the seminar was held in a nice "château-hotel," remotely situated in the Chantilly forest. It was opened by the then French minister of defense, Michèle Alliot-Marie, who chaired a panel of five or six of her colleague ministers of defense from all over Europe. The main topics were the Balkans, Afghanistan, a rising China, a troubled Africa. We did not anticipate the 2008 events in Georgia, nor the 2007 attacks on Estonia… and of course, Daesh was totally unknown, for good reasons.

We did not talk much about cyber. Yes, there was secretary Linton Wells, who was delivering some sort or early warning. But most of us were thinking : "Hey, what is this new kind of whim coming from the Pentagon?"

So, yes, our world has evolved since 2005. And this workshop also has evolved to reflect this evolution. Now, the question is: Is this world today more secure than it was 10 years ago?

On the one hand, we have witnessed the many efforts by the international community to adapt to these new threats, by strengthening cooperation, creating new instruments: political, diplomatic, military, technical—–to better address these threats. Encouraging progress, but also still many frustrating shortfalls. On the other hand, we have the feeling that we are desperately running after an enemy who is still more rapid and more agile than we are.

So, is the glass half full, or half empty? In this situation, it is vital that we keep exchanging our analyses and our views on how to best face these challenges together. I cannot think of a better opportunity than this workshop to do so, with the vast array of expertise that you represent, around this table.

Again, on behalf of the IHEDN, many thanks to all of you for coming and sharing your expertise and your views on these vital issues. I wish you a safe trip back to your countries.

Closing note: These remarks were prepared only four days after the dreadful and deadly attacks in Paris, that have ended 129 young and innocent lives and that left a hundred more wounded. For this, I am terribly sad. But I am even more confident that we together can face this barbarian behavior and defeat it. Pray for Paris, and "Vive la France!"