Global Security in Crisis

Deepening cracks in the rules-based international order, the rise of radical Islam, cyber threats, and faltering globalization

PROCEEDINGS OF THE 33*rd* INTERNATIONAL WORKSHOP ON GLOBAL SECURITY

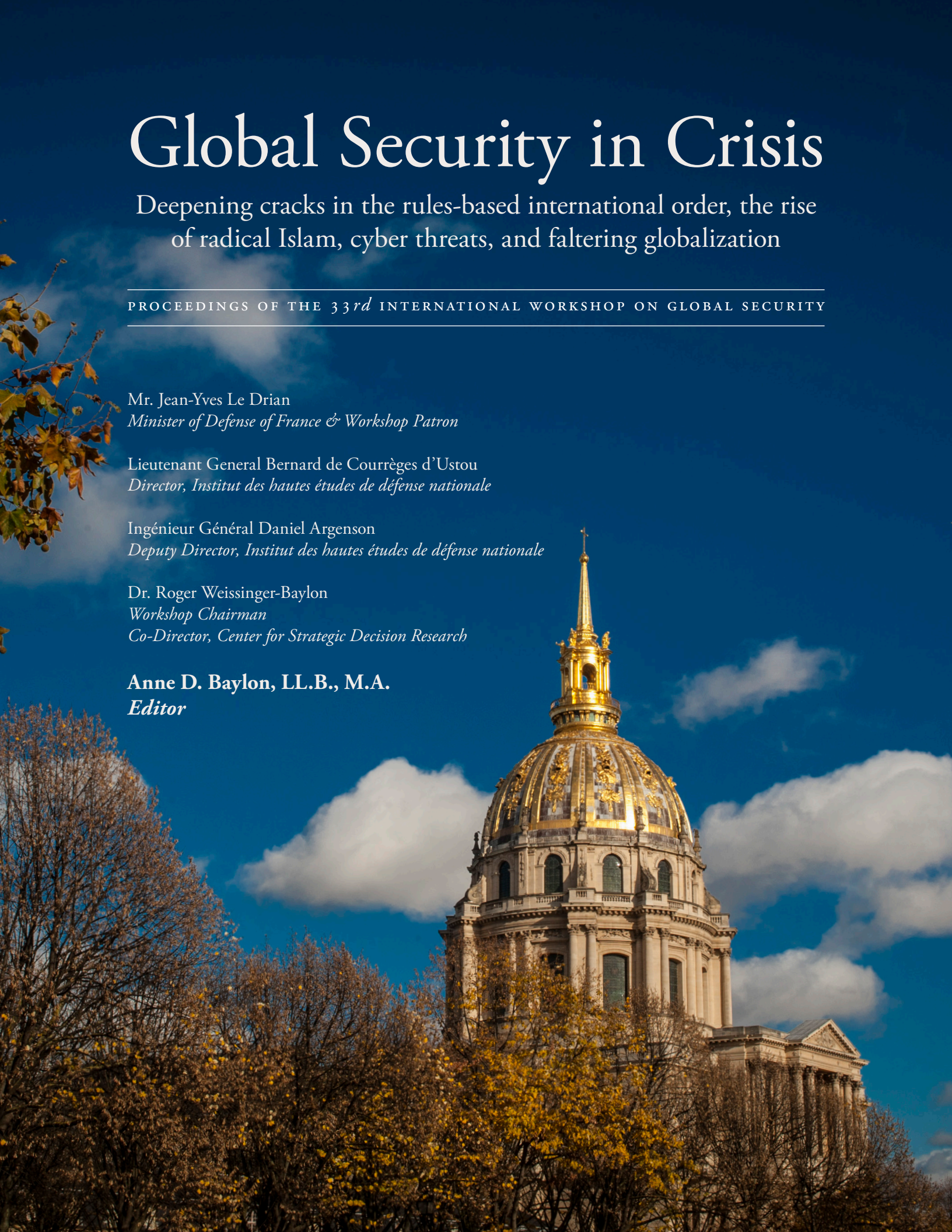
Mr. Jean-Yves Le Drian
Minister of Defense of France & Workshop Patron

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

Ingénieur Général Daniel Argenson
Deputy Director, Institut des hautes études de défense nationale

Dr. Roger Weissinger-Baylon
Workshop Chairman
Co-Director, Center for Strategic Decision Research

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



COVER IMAGE

Dome of the Hôtel National des Invalides

Published by

Center for Strategic Decision Research | Strategic Decisions Press

2456 Sharon Oaks Drive, Menlo Park, California 94025 USA

www.csdr.org

Anne D. Baylon, LL.B., M.A., Editor | anne@csdr.org

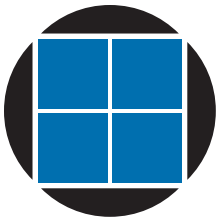
Dr. Roger Weissinger-Baylon, Chairman | roger@csdr.org

Printed in the United States of America by Almaden Press, Santa Clara, California.

Photography by Matteo Pellegrinuzzi | mail@matteopellegrinuzzi.com

International Standard Book Number: 1-890664-23-5

© 2016, 2017 Center for Strategic Decision Research



33rd International Workshop on Global Security

Workshop Proceedings

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

WORKSHOP PATRON	Mr. Jean-Yves Le Drian *Minister of Defense of France*
THEME	Global Security in Crisis *Deepening cracks in the rules-based international order, the rise of radical Islam, cyber threats, and faltering globalization*
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*
	Cisco Systems
MAJOR SPONSORS	McAfee | Intel Security · MITRE · Area SpA
ASSOCIATE SPONSORS	Cast Software · ARES · AXA

The *33rd International Workshop on Global Security* is presented by the Center for Strategic Decision Research (CSDR) in partnership with the Institut des hautes études de défense nationale (IHEDN) in the Prime Minister's organization, 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

CISCO

MAJOR SPONSORS

intel Security

MITRE

AREA

ASSOCIATE SPONSORS

CAST

ARES SECURITY

AXA

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

Contents

Lieutenant General Bernard de Courrèges d'Ustou 6
Director, Institut des hautes études de défense nationale (IHEDN)

Summary and Findings – English Version 7
Dr. Roger Weissinger-Baylon, Workshop Chairman

Sommaire et Conclusions – Version française 11
Dr. Roger Weissinger-Baylon

Mr. Camille Grand 15
NATO Assistant Secretary General for Defence Investment

Vice Admiral Arnaud Coustillière – English Version 21
General Officer Cyber Defense, French Ministry of Defense

Vice-amiral Arnaud Coustillière – Version française 26
Officier général cyberdéfense, Ministère de la Défense

Ambassador David Martinon 32
Ambassador for Cyber Diplomacy and the Digital Economy, French Foreign Ministry

Ms. Heli Tiirmaa-Klaar 35
Head of Cyber Policy Coordination, Conflict Prevention and Security Policy Directorate, European External Action Service

Ambassador Marjanne de Kwaasteniet 37
Permanent Representative of the Netherlands to NATO

Mr. Atsushi Saito 40
Director, Cyber Policy Division, Foreign Policy Bureau, Ministry of Foreign Affairs of Japan

Mr. Conrad Prince 42
Cyber Security Ambassador, United Kingdom Defense and Security Organization

Ambassador Michael Zilmer-Johns 43
Permanent Representative of Denmark to NATO

Ambassador Luis de Almeida Sampaio 45
Permanent Representative of Portugal to NATO

Ambassador Vladimir Chizhov 47
Permanent Representative of Russia to the EU

Ambassador Miguel Aguirre de Carcer 49
Permanent Representative of Spain to NATO

Mr. Pjer Šimunović 51
Director, Office of the National Security Council of the Republic of Croatia

Ambassador Mehmet Fatih Ceylan 54
Permanent Representative of Turkey to NATO

Ms. Marietje Schaake 58
Member of the European Parliament

General (Gendarmerie) Marc Watin-Augouard 62
Director, Center for Research, Officer School of the Gendarmerie Nationale

Mr. Guillaume Poupard – English Version 66
Director General, Agence nationale de la sécurité des systèmes d'information (ANSSI)

Mr. Guillaume Poupard – Version française 71
D*irector General, Agence nationale de la sécurité des systèmes d'information (ANSSI)*

Mr. Marty Roesch 74
Vice President and Chief Architect, Security Business Group, Cisco

Ingénieur Général Daniel Argenson 80
Deputy Director, Institut des hautes études de défense nationale (IHEDN)

Mr. Jamie Shea 81
NATO Deputy Assistant Secretary General for Emerging Security Challenges

Dr. Frédérick Douzet 85
Castex Chair of Cyber Strategy, Institut des hautes études de défense nationale
Professor, Université Paris 8, Institut Français de Géopolitique

Professor Kevin Limonier 88
Associate Professor, Université Paris 8, Institut Français de Géopolitique

Ms. Caroline Baylon 90
Information Security Research Lead, AXA (R&D)

Mr. Alain Fiocco 92
Senior Director, Chief Technology Officer
Head of Paris Innovation & Research Lab, Cisco

Mr. Raj Samani 94
Chief Technology Officer, Europe, Intel Security

Dr. Lin Wells II 96
Advisor, Georgia Tech Research Institute, former U.S. Assistant Secretary of Defense

Dr. Anibal Villalba 98
Senior Adviser to the President, National Cybersecurity Council of Spain

Mr. Don Proctor 100
Senior Vice President, Cisco

Ambassador Jiri Sedivy 101
Permanent Representative of the Czech Republic to NATO,
Former Minister of Defense

Mr. Sven Sakkov 103
Director, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)

Major General David Senty, USAF (Ret.) 106
Director, Cyber Operations, The MITRE Corporation; Former Chief of Staff,
US Cyber Command

Ambassador Imants Liegis 109
Ambassador of Latvia to France; former Minister of Defense of Latvia

Dr. Ioan Mircea Pascu 111
Vice President of the European Parliament, Former Minister for Defense of Romania

Ambassador Boris Grigić 113
Permanent Representative of Croatia to NATO

Mr. Andrea Formenti 117
Founder & CEO, Area SpA

Colonel Eric Freyssinet 119
Advisor to the Prefect in charge of the fight against cyberthreats,
French Ministry of the Interior

Mr. Daniel Maly 121
Senior Vice President and Country Manager, Cast Software

Mr. Kurt Westerman 123
Vice President, Business Development, ARES Corporation

Ingénieur Général Daniel Argenson 125
Deputy Director, Institut des hautes études de défense nationale (IHEDN)

Welcoming Remarks

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

Welcome to the Invalides, a place of history and heritage that symbolizes both the past and present defense and security of France. Ceremonies in memory of the victims of terrorism—such as those who died in the Paris terrorist attacks last November— are held here. This is where we also honor soldiers killed in action fighting terrorism and our enemies, like the young soldier who got killed in Mali last Friday. As the Director of IHEDN—Institut des hautes études de défense nationale—I am very pleased to greet you today for the seventh time in Paris and personally for the third time at the International Workshop on Global Security under the patronage of Minister of Defense Jean-Yves Le Drian. IHEDN has been co-organizing this Parisian edition of the seminar with Dr. Roger Weissinger-Baylon, the workshop chairman and founder, and this cooperation has been very fruitful.

During this 33rd workshop, your group of distinguished experts will reflect for two days on the subject of *"Global Security in Crisis: The deepening cracks in the rules-based international order, the rise of radical Islam, the cyber threat, and faltering globalization."* Although this is not a very optimistic subject, it reflects very important current issues.

IHEDN is an inter-ministerial, inter-agency institute that trains about 2,400 civilian and military leaders on strategic issues at the international, national and regional levels in approximately 60 sessions or seminars per year. IHEDN is also dedicated to developing European and international responsibility. At our flag/general officer national sessions, about 150 civilian and military leaders exchange views on defense and security during lectures, visits, and workshops. The general theme we chose for this year is "Strategic disruptions and their consequences."

IHEDN trains 2,400 civilian and military leaders on strategic issues…and is also dedicated to developing European and international responsibility.

What is surprising in the rise of Islam, of the cyber threat, and the actions of power states such as Russia and China is the importance and speed of the evolution.

The 2013 White Book developed ideas about the threats coming from power and the risks of being weak and I will say that the rise of Islam, the rise of the cyber threat, and the actions of power states such as Russia and China do not come as a surprise. What is surprising, however, is the importance and speed of the evolution, especially in the case of Islamic terrorism. This kind of threat is our real enemy and France has identified as such radical Islam and its terrorist actions in the Middle East, Sahara, the so-called Sahel-Sahara strip, Libya and Morocco. We do not exclude other kinds of threats, however and, like many of you, we do worry about the activities of certain power states. I am therefore happy that you chose "Global Security in crisis" and will be very interested in the results of the various workshop panels. My best wishes to you all for a constructive seminar and a pleasant stay in Paris despite what we can perhaps call a British weather.

Global Security in Crisis:
The Deepening Cracks in the Rules Based International Order, the Rise Of Radical Islam, the Cyber Threat, and Faltering Globalization

Dr. Roger Weissinger-Baylon
Workshop Chairman and Founder[1]

Summary and Findings

"Clearly NATO has never been more relevant, but it has never been more challenged by threats that are more dangerous than ever in its history. The key component of the Alliance—mutual trust and confidence—needs to be restored. Yet I am not confident it will be. The next six months will be critical for both the Alliance and the United States of America."
- General George Joulwan, USA (Ret.),
11th Supreme Allied Commander, Europe (SACEUR)

Finding 1. Global security is undergoing concurrent disruptions that are creating deep and dangerous cracks in the international order.

Brexit, the surprising triumph of Donald Trump, the defeat of the Italian referendum, and the rise of far-right political groups suggest that deep cracks are opening up in the international security system, partly due to the rejection of globalization's undesirable side effects (growing inequality, austerity policies, and refugee flows); spreading terrorism fueled by the strict salafist/wahhabist brands of Islam and new internet and other technologies that amplify these forces. These disruptions will be exploited by Russia and other state actors, by terrorists, and by criminal groups.

Finding 2. One of the serious disruptions is the extraordinary vulnerability to cyber attacks of most organizations—including multinational corporations, governments, and international organizations like NATO or the EU. All of them must significantly increase the resources allocated to cyber defenses and take new approaches to improve overall cyber resilience—or face the consequences.

There is an extreme "lack of cyber maturity" within most of the largest international corporations, governments, and other organizations." Consequently, even the largest corporate giants—Coca Cola, Exxon, Boeing, or Volkswagen—or governments are at risk.

So great are the weaknesses that "there needs to be an increase of fully 100 to 150% in cyber resources—to effectively recruit, retrain, and ultimately retain the most talented engineers" to deal with these dangerous vulnerabilities and improve organizational cyber readiness. Critical capability improvement priorities include (1) addressing systemic application vulnerabilities (2) improving breach detection and response and (3) reducing security system complexities.

[1] Director, Center for Strategic Decision Research email: roger@csdr.org website: https://www.csdr.org

Finding 3. According to secret CIA assessments, Russia is believed to have intervened in the US Presidential Election campaign with a massive cyber influence operation and ultimately saw its preferred candidate, Donald Trump, triumph as the President-elect. [2]

With an intensive and highly effective cyber influence operation, Russia is believed to have targeted the Democratic National Committee (DNC). The attack succeeded in obtaining emails of Hillary Clinton's presidential campaign, which were released through WikiLeaks. Since the election was close—with Hillary Clinton actually winning the popular vote with a nearly 3 million-vote margin, Russia appears to have been influential in tipping the race in favor of its preferred candidate, Donald Trump.

Tellingly, the election does not seem to have been decided by the substance of the materials released by Russian hacking groups but instead by the "unrelenting drip feed of email leaks…none of them contained any damning or even faintly compromising material… [but] the constant flow and the FBI intervention it provoked created the impression that there was something murky and suspicious." Worse, "fake news" on the elections were amplified by Facebook and Google algorithms as well as tweets from Trump supporters to reach millions of voters in the final days of the campaign.

Finding 4. If the CIA's attribution is correct, Russian intervention in the US election[3] may have been one of the most serious cyber influence operations ever conducted, since it undermined trust in electoral processes. The 2017 French and German elections face risks of disruption as well.

The Russian hacking should be taken as an urgent warning to the international community—especially since Russia is widely believed to have influenced the Brexit vote in the UK as well as regional elections in Germany. It is currently wielding influence in the French Presidential election, where a Russian bank is financing the campaign of Marine Le Pen—and "if the US couldn't stop the interference, do European States have any chance of preventing a similar attack/intervention?"

Finding 5. As their Caliphate weakens, ISIS/Daesh will need to find new ways to mount terrorist attacks. Organized groups of cyber criminals (cyber mercenaries) and Islamic terrorist groups such as ISIS/Daesh may eventually come together to create violent cyber attacks.

---

[2] "Secret CIA assessment says Russia was trying to help Trump win White House." Entous, Adam, Nakashima, Ellen, and Miller, Greg. *Washington Post,* 10 Dec 2016. Pg. 1.

[3] "The Perfect Weapon: How Russian Cyberpower Invaded the U.S." Lipton, Eric, Sanger, David E., and Shane, Scott. *New York Times.* Pg 1. Dec. 13, 2016 Is this the "Cyber Pearl Harbor" of which Secretary of Defense Leon Panetta warned in 2012?

To deal with this danger, "we need a coalition of governments, private citizens, internet service providers, information technology companies, and NGOs to combat the use of the web by terrorists and jihadists."

There are reasons for great concern: "mafias, linked to organized crime—and sometimes even protected by states, have the means to execute extremely violent attacks." And terrorist groups such as ISIS/Daesh have wealthy salafist/wahhabist supporters who want to spread terrorist attacks. Consequently, the probability that cyber mercenaries and these terrorist groups "will come together, if they have not done so already, is evidently extremely high."

Finding 6. Dealing with ISIS/Daesh requires recognizing that the enemy is salafist jihadism that seeks global supremacy through the replacement of Western influences by a Caliphate and the use of violence. Yet, most governments currently prioritize the financial benefits of strong relationships with the oil-rich Gulf States that continue to fund radical Islam.[4]

Most governments and large international organizations are reluctant to attribute the spreading terrorist attacks to "radical Islam," "political Islam," "salafism," or "wahhabism." And they take great pains to not mention the financial sources for these terrorist activities in the Gulf States (Kuwait, Qatar, or Saudi Arabia). According to a broad consensus that has held for decades, it is preferable to accept the spread of salafism rather than risk losing investments from wealthy oil-rich countries or access to their armaments, civil aviation, infrastructure, or other markets.

Nonetheless, we may be witnessing a sea change—with political figures ranging from the leading Presidential candidate in France, François Fillon, to Donald Trump proposing extreme measures to stop the spread of radical Islam in their countries.

Finding 7. While public opposition to trade agreements (TTIP, TISA, NAFTA) appears to be a key factor behind Brexit and other ongoing political upheavals, some provisions of these treaties may also have unexpected cyber security consequences: they may limit or even block the ability of countries to impose certain vital cybersecurity standards that will protect their citizens.

The cybersecurity implications of so-called trade agreements like TTIP, TISA, or NAFTA are not well known. Will the investor protection provisions of such agreements limit or block the ability of countries to impose cyber security standards such as those that ANSSI considers to be vital in France? Will they prevent countries from imposing localization requirements so that certain critical data can remain within their national borders?

Finding 8. The exponential growth of the Internet of Things (IoT)—headed toward 50 billion connected devices—opens up vast vulnerabilities that range from cyber crime to

[4] Such approaches can be likened to the idioms of "running with the hare and hunting with the hounds" or "ménager la chèvre et le chou" (accommodating both the goat and the cabbage).

cyber attacks on critical infrastructure. (A Mirai malware attack recently exploited 100,000 poorly protected devices including surveillance cameras in order to take down a portion of the internet.)

Since the Mirai malware was able to generate a massive 1 terrabyte per second distributed denial of service attack (DDoS) using 100,000 internet-connected security cameras, a 10 terrabyte per second attack cannot be too far behind. And even large attacks could come later, potentially taking down a large section of the internet backbone. A Mirai botnet can be rented by any of us for 7,500 euros a week, and the availability of a 400,000 device botnet is already being touted on the dark web.

Finding 9. Governments can no longer rely on market forces to protect their societies. This approach has failed. Instead, governments and industry must work together to develop standards that will protect the internet and their citizens from even larger attacks. As for the terrorist threat, it may require coordinated action by NATO, the EU, or the UN.

In order to involve everyone in cyber security, every country needs "a large scale cyber campaign, both in schools and the public arena" and, to make this possible, a highly visible government minister responsible for cyber. Cyber programs are needed not just for schools and the public, but to train tens of thousands of cyber professionals. Should the right to use the internet depend on passing a test similar to a driver's license exam?

Finding 10. What matters most are the social, economic, and political impacts on our societies—a hospital patient whose operation is blocked, a telecom company that loses over 100,000 customers after a cyber attack, a country like Ukraine whose electrical grid is shut down, or a country like Germany that reports a loss of more than 1% of GDP to cyber attacks. And, now, perhaps for the first time, citizens in the US are losing trust in their governments because another country is reported to have interfered in its elections.

Post-workshop note. The above findings do not account for certain influences that were not fully understood at the time of the workshop—such as the role of "fake news" in elections and referendums, or the harmful effects of social media in accelerating their spread. Strategies will be needed to curb their effects before other countries are harmed.

La Sécurité globale en crise:
Les fissures grandissantes dans l'ordre international fondé sur Des règles, la montée de l'Islam radical, la cybermenace, Et l'échec de la globalisation

Dr. Roger Weissinger-Baylon
Workshop Chairman

Sommaire et Conclusions

« Clairement, l'OTAN n'a jamais été aussi nécessaire tout en n'ayant jamais fait l'objet d'autant de menaces graves. La confiance mutuelle, qui est l'élément central de l'Alliance, doit être restaurée. Cependant, je ne suis pas convaincu que cela puisse se faire. Les six prochains mois seront une période critique à la fois pour l'Alliance et aussi pour les Etats-Unis. »
- Général George Joulwan, USA (Ret),
11e Commandant suprême des forces alliées en Europe (SACEUR)

Conclusion 1. La sécurité globale traverse un moment de difficultés qui est en train de créer de profondes et dangereuses fissures dans l'ordre international.

Le Brexit, le triomphe inattendu de Donald Trump, la défaite du référendum Italien, et la montée de groupes politiques d'extrême droite suggèrent l'apparition de profondes fissures dans le système de sécurité international, dues en partie au rejet des effets secondaires indésirables de la globalisation (inégalités grandissantes, politiques d'austérité et flux de réfugiés) ; à la propagation du terrorisme alimenté par les groupes salafistes et wahhabites de l'islam, ainsi qu'à l'internet et autres technologies variées qui amplifient ces forces. Ces difficultés sont exploitées par la Russie, par d'autres états, par les terroristes et les groupes criminels.

Conclusion 2. Une difficulté particulièrement sérieuse tient à l'extraordinaire vulnérabilité de la plupart des organisations—sociétés multinationales, gouvernements, et organisations internationales telles que l'OTAN ou l'Union Européenne—face aux attaques cyber. Toutes ont besoin d'allouer davantage de ressources à la cyber défense et d'améliorer leur résistance cyber. Elles devront sinon en subir les conséquences.

Beaucoup de sociétés internationales, gouvernements, et organisations similaires souffrent d'un manque extrême de « cyber maturité ». En conséquence, même les plus grands géants industriels— Coca Cola, Exxon, Boeing, ou Volkswagen—et les gouvernements sont en danger.

Leurs défaillances sont telles qu'il faudrait une augmentation des ressources cyber de 100 à 150% pour recruter, former et, au final, garder les ingénieurs les plus compétents afin de corriger ces vulnérabilités dangereuses et améliorer la préparation cyber de ces organisations.

Conclusion 3. Selon des analyses effectuées par la CIA, la Russie serait intervenue dans la campagne présidentielle américaine grâce à une opération cyber massive afin d'aider son candidat préféré, Donald Trump, à gagner la présidence.

La Russie aurait monté une opération cyber très efficace visant le Comité national démocrate. L'attaque a permis d'obtenir les emails de la campagne présidentielle d'Hillary Clinton qui ont été diffusés par WikiLeaks. Etant donné que l'élection était serrée—Hillary Clinton ayant gagné le vote populaire avec une marge de près de 3 millions de votes—la Russie semble avoir influencé le résultat en faisant basculer la course électorale au profit de Donald Trump.

Il est intéressant de relever que l'élection ne semble pas avoir été décidée par le contenu des documents diffusés par les pirates informatiques Russes mais plutôt par un goutte-à-goutte incessant de fuites d'emails…aucune n'étant particulièrement compromettante… mais leur flux constant et l'intervention du FBI que ce flux a provoqué ont donné l'impression de quelque chose de trouble et de suspect. Pire encore, de « fausses nouvelles » concernant les élections ont été amplifiées par les algorithmes de Facebook et Google et par les tweets des supporters de Trump, qui ont atteint des millions d'électeurs dans les derniers jours de la campagne.

Conclusion 4. Si l'attribution faite par la CIA est correcte, l'intervention Russe dans les élections américaines est peut-être l'une des plus graves opérations cyber jamais menées puisqu'elle a affaibli la confiance dans le système électoral. Les élections de 2017 en France et en Allemagne courent le même risque de perturbations.

L'attaque cyber russe doit être vue comme un avertissement urgent à la communauté internationale puisque la Russie est soupçonnée d'avoir aussi influencé le vote du Brexit[5] en Angleterre et les élections régionales en Allemagne. Son influence pèse également sur l'élection présidentielle en France où une banque russe finance la campagne de Marine Le Pen. Si les Etats-Unis n'ont pas réussi à stopper cette interférence, les états européens ont-ils la moindre chance d'empêcher une attaque/intervention similaire ?

Conclusion 5. Au fur et à mesure que leur califat s'affaiblit, ISIS/Daesh doit trouver d'autres moyens de monter des attaques terroristes. Par exemple, des bandes organisées de cyber criminels (cyber mercenaires) et des groupes terroristes Islamiques comme ISIS/Daesh pourraient s'associer pour monter de violentes attaques cyber.

---

[5] *Newsweek. Opinion.* « Is the Brexit Vote Legitimate If Russia Influenced the Outcome? » Baylon, Caroline. 12/2/16 at 4:32 AM

Face à ce danger, « nous avons besoin d'une coalition de gouvernements, de citoyens, de fournisseurs de service internet, d'entreprises informatiques, et d'ONG pour lutter contre l'utilisation de la toile par les terroristes et les djihadistes. »

Il y a lieu de s'inquiéter : les mafias, liées au crime organisé et parfois même protégées par des états, ont les moyens d'exécuter des attaques extrêmement violentes; et les groupes terroristes comme ISIS/Daesh ont de riches supporters salafistes/wahhabites qui veulent propager les attaques terroristes. Il est donc fortement probable que les cyber mercenaires et ces groupes terroristes fusionneront, si ce n'est déjà fait.

Conclusion 6. Pour faire face à ISIS/Daesh, il faut d'abord reconnaître que le djihadisme salafiste est l'ennemi qui vise la suprématie globale en remplaçant l'influence occidentale par un califat et l'usage de la violence. Pourtant, la plupart des gouvernements préfèrent actuellement accorder la priorité aux bénéfices financiers qu'ils retirent de leurs relations privilégiées avec les Etats du Golfe riches en pétrole qui continuent de financer l'islam radical.

La plupart des gouvernements et des grandes organisations internationales hésitent à attribuer les attaques terroristes toujours plus nombreuses à l'Islam radical, au salafisme, ou au wahhabisme. Et ils évitent de mentionner dans les Etats du Golfe (le Koweït, le Qatar, ou l'Arabie saoudite) les sources financières de ces activités terroristes. Selon un consensus bien établi, il est préférable d'accepter la propagation du salafisme plutôt que de risquer de perdre les investissements des pays riches en pétrole ou l'accès à leurs marchés d'armement, d'aviation civile, et d'infrastructure. Un changement radical peut toutefois se produire avec l'apparition de personnalités politiques comme le candidat à la présidence en France, François Fillon, ou Donald Trump, qui proposent des mesures extrêmes pour stopper l'Islam radical dans leurs pays.

Conclusion 7. Tandis que l'opposition du public aux accords commerciaux (TTIP, ACS/TISA, ALENA/NAFTA) semble avoir été une motivation essentielle derrière le Brexit et d'autres bouleversements politiques, certaines provisions de ces traités peuvent aussi avoir des conséquences sur la cyber sécurité : elles peuvent limiter ou même bloquer la capacité des pays à imposer des standards de cyber sécurité qui sont essentiels pour protéger leurs citoyens.

Les retombées cyber sécuritaires d'accords commerciaux comme TTIP, TISA, ou NAFTA sont mal connues. Les dispositions sur la protection des investisseurs de ces accords vont-elles limiter ou bloquer la capacité des pays à imposer des standards de cyber sécurité comme ceux que ANSSI considère essentiels en France ? Vont-elles empêcher les pays d'imposer des critères de localisation afin de pouvoir conserver certaines données critiques à l'intérieur des frontières nationales ?

Conclusion 8. Le développement exponentiel de l'Internet des objets (IoT/IdO)—avec bientôt 50 milliards d'objets connectés—introduit de vastes failles de sécurité qui vont de la cybercriminalité jusqu'aux attaques cyber sur l'infrastructure critique. (Une

attaque malveillante Mirai a récemment exploité le manque de protection de 100.000 objets, comme par exemple des caméras de surveillance, pour fermer une partie de l'internet.

Etant donné que Mirai a pu provoquer une attaque massive par déni de service (DDoS) de 1 téraoctet par seconde en utilisant 100.000 caméras de sécurité connectées à l'internet, une attaque de 10 teraoctet par seconde ne peut pas être bien loin derrière. Des attaques encore plus grandes ayant le potentiel de fermer une grande partie du réseau internet pourraient suivre. Un botnet Mirai peut actuellement se louer pour 7.500 euros par semaine, et le dark web vante déjà la possibilité d'acheter un botnet de 400.000 objets connectés.

Conclusion 9. Les gouvernements ne peuvent plus compter sur les forces du marché pour protéger leurs sociétés. Cette approche a échoué. Ils doivent plutôt travailler avec l'industrie pour développer des normes capables de protéger l'internet et leurs citoyens d'attaques encore plus importantes. Quant à la menace terroriste, elle demandera probablement une action coordonnée OTAN, UE et ONU.

Chaque pays devra mobiliser ses citoyens en matière de sécurité cyber en organisant une grande campagne cyber dans les écoles et auprès du public et en nommant un ministre responsable pour la cybersécurité. Il faudra également des cours cyber pour former des dizaines de milliers de cyber professionnels. Etant donné la gravité des dangers, faudra-t-il passer un test semblable à un permis de conduire pour avoir le droit d'utiliser l'internet ?

Conclusion 10. L'impact social, économique, et politique sur nos sociétés est ce qui compte le plus—un patient dans un hôpital dont l'opération est bloquée, une société de télécommunications qui perd plus de 100.000 clients à la suite d'une attaque cyber, un pays comme l'Ukraine dont le réseau électrique est coupé, ou un pays comme l'Allemagne qui signale la perte de plus de 1% de son PIB. Et pour la première fois maintenant, les citoyens américains sont en train de perdre confiance dans leur gouvernement puisqu'un autre pays se serait immiscé dans leurs élections.

Note : Les conclusions ci-dessus ne tiennent pas compte de certaines influences qui n'étaient pas bien comprises au moment du workshop—comme le rôle des « fausses nouvelles » dans les élections et référendums, ou les effets nuisibles des médias sociaux qui accélèrent leur diffusion. Il faudra mettre en place des stratégies pour limiter ces effets avant que d'autres pays ne soient atteints.

Developing the Right Capabilities to Face the Global Security in Crisis

Mr. Camille Grand
NATO Assistant Secretary General for Defence Investment

To open this important event, my presentation will focus on developing the right set of capabilities in the face of a global security in crisis. I will not describe the environment that many of you are very familiar with but rather tell you what we are doing at NATO towards that goal.

Security Environment—Ever Changing and Challenging

Today the security environment is extremely challenging and it is evolving rapidly. As General de Courrèges pointed out, this environment is undergoing a major transformation and it is also fast-paced, placing heavy demands on nations and organizations like NATO or the EU. In a way, this current security environment is the most complex we have seen in a couple of decades. We are facing at the same time threats and challenges from both state and non-state actors; from the south and from the east; from conventional military forces and from unconventional forces, including non-state actors.

We are facing…threats and challenges from both state and non-state actors; from the south and from the east; from conventional military forces and from unconventional forces, including non-

These threats, such as cyber threats and hybrid warfare, also evolve in multiple forms. In order to deal with such diverse threats, the Alliance must have the right set of capabilities at hand. So, at the Warsaw Summit the Allies confirmed that: "We will ensure that NATO has the full range of capabilities necessary to deter and defend against potential adversaries and the full spectrum of threats that could confront the Alliance from any direction."

Russia

Concerning the relationship with Russia—I welcome the Russian participation today—it is important for us to see clearly what we are talking about. We are not in a new Cold War but we should also admit that we are no longer in the post-Cold War era. Cooperation has ceased to be the dominant narrative. It can happen, it does happen in specific cases but the partnership mode that was hoped for and desired is no longer obvious to either side. The current relationship with Russia can be characterized as a "Cold Peace," a situation in which war remains unlikely but the nature of the relationship has been radically transformed. There can be no doubt that the security situation across the Euro-Atlantic area has deteriorated markedly. The annexation of Crimea and the aggression against Eastern Ukraine have created a situation that is very different from the previous setting and

The relationship with Russia can be characterized as a "Cold Peace"… war remains unlikely but the nature of the relationship has been radically transformed.

changed some of the key principles of the post-Cold War era. Russia's decision to multiply large-scale exercises is also raising a new set of questions. Some of these "snap exercises" have been large-scale, without early notice, and have involved a whole spectrum of capabilities right on NATO's border. I am not questioning the right of Russia to hold such exercises but my point is that it really transforms the perception of Russia's neighborhood vis-à-vis the Russian Federation. There are also major political debates over the policy regarding Ukraine and Syria. All this is creating a situation in which the tensions with Russia are probably at a peak if one compares with the past twenty years.

NATO's Response

NATO's reaction to this was a combination of defense, deterrence and diplomacy. As an observer, I noted the rather unified response that NATO was able to develop from the Wales Summit to the Warsaw Summit. This does not mean that there are no debates within the Alliance but the message of unity is clear. It combines firmness and resolve when it comes to deterrence and defense, as well as openness to dialogue and an effort not to seek confrontation with Russia. While there is a push for a meaningful and constructive dialogue, there is also a real effort to build the right set of capabilities in order to face any contingencies. The confirmation of the readiness of the Alliance to hold regular NATO-Russia Council meetings is a sign of that balanced approach.

The readiness of the Alliance to hold regular NATO-Russia Council meetings is a sign of that balanced approach.

On the Southern flank… Situations involve failed states, terrorism, grave threats to pillar states and the rise of a form of radical Islam terrorism, which is creating dangerous threats to the very heart of Europe.

It is also important to look south. On the Southern flank, there has been a vast degradation over the last few years. Situations involve failed states, terrorism, grave threats to pillar states and the rise of a form of radical Islam terrorism, which is creating dangerous threats to the very heart of Europe, as we have seen with the Paris and Brussels attacks in particular.

In response, to this new environment, NATO has developed a 360-degree-approach that has led to the development of the Readiness Action Plan. This plan has expanded the NATO Response Force to more than 40,000 troops, created a Spearhead Force within the NATO Response Force capable of reinforcing any ally within 2-3 days, and established a chain of small headquarters in the eastern part of the Alliance.

At the Warsaw Summit, the Allies also agreed on the need to enhance our presence in the east and southeast, and to take other steps to strengthen our deterrence. We will soon deploy 4 multinational battalion size battle groups—I insist on the word battalion because we are not talking about large size forces—one each in Poland,

We will deploy 4 multinational battalion size battle groups…one each in Poland, Estonia, Latvia and Lithuania, to be led in turn by the U.S., Germany, Canada and the United Kingdom.

Estonia, Latvia and Lithuania, to be led by the U.S., Germany, Canada and the United Kingdom with contributions of many Allies. The message is that an action against any ally will be treated as an attack on all allies, which has been the core principle of the Alliance since its creation while also being a very proportionate response in terms of size and type of deployment. On the Southern part, the effort has been on protecting stability. In the NATO jargon, this means both training and supporting forces of partner countries in the South with a specific focus on Jordan, Iraq, and Tunisia, and supporting the coalition against ISIS with the deployment of NATO AWACS.

Defence Investment Pledge

Since the Wales Summit, which is about equipping the Alliance with the right set of capabilities, requires commitment and resources, it has been an effort to work on the Defence Investment Pledge.

Allies committed to halt decades of cuts to defence spending and gradually increase spending to…2% of GDP.

With the NATO Defence Investment Pledge, Allies committed to halt decades of cuts to defence spending and gradually increase spending to reach the goal of 2% of GDP over the next decade when currently only a handful of allies are close to this objective. This is important, as raising defence spending does not only make more resources available to invest in our security, but also proves the Allied solidarity and willingness to do what is necessary to ensure our individual and collective security. It also has an impact on the effort to address the burden sharing debate, which was very much part of the US presidential campaign. Fairer burden sharing is a strong message of the Trump administration.

We Must Spend on the Right Things

It is not just about how much we spend, it is also about how and on what we spend. The Defence Investment Pledge includes a commitment by all Allies to spend 20% of their defence budgets on new equipment and on research and development. Interestingly, this 20% investment commitment might be even more difficult to fulfill than the 2% over the long term but it is just as important. As national budgets increase, we look to nations to make investments in capabilities that contribute to NATO objectives.

So, we need to spend efficiently and on capabilities that are really needed. As every single euro, dollar and pound counts, we must spend our resources in a smart way. NATO is uniquely positioned to foster this approach because it provides Allies and partners with a venue for nations to exchange views on capability development and to share lessons learned from operations and exercises. NATO also promotes and facilitates multinational cooperation by bringing together like-minded nations with similar requirements or by overseeing the implementation of NATO common-funded projects. Let me give you a few examples of that:

Precision-Guided Munitions (PGM). One good example of multinational cooperation has been the project on precision-guided munitions led by Denmark. At the October 2016 Defence

Ministerial I hosted the signature of Poland, the ninth partner in that group that will collectively buy precision-guided munitions that have been lacking in the past.

Joint Intelligence Surveillance and Reconnaissance (JISR). This example is more about our common-funded capabilities. As you may know, Joint Intelligence Surveillance and Reconnaissance is essential since timely access to accurate information is the linchpin of success in every operation. It is a critical component of NATO's readiness and responsiveness. Operations in recent years, including in Libya, have revealed some challenges in the ways we collect, interpret and share intelligence within the Alliance.

Operations, including in Libya, have revealed some challenges in the ways we collect, interpret, and share intelligence within the Alliance.

In response to those challenges, Allied Heads of State and Government launched the JISR initiative at the Chicago Summit in 2012, and reaffirmed their commitment to it at Wales in 2014. The goal is to improve the way we handle intelligence and since the launch of this initiative, we have made solid progress working on procedures, intelligence library, training resources and enhancing technical interoperability. Last but not least, the Allied Ground Surveillance drone system will enter service in the coming year or so, providing the Alliance with a new capability that is impressive.

Ballistic Missile Defence (BMD). Ballistic Missile Defence is meant to protect our populations, territory and forces against the increasing threat posed by the proliferation of ballistic missiles. In Warsaw, we announced the initial operational capability for NATO BMD. The next focus of our efforts is the delivery of a full operational capability that will provide full coverage and protection to NATO European populations, territory and forces as required by Heads of State and Government. It will be a long-term endeavor. Let me stress that NATO BMD is not targeted at Russia but specifically targets threats outside the Euro-Atlantic area. It will remain relatively limited in scope and capability. The NATO system is primarily focused on the command and control of the system and assets will be provided by allies individually.

Let me stress that NATO BMD is not targeted at Russia but specifically targets threats outside the Euro-Atlantic area. It will remain relatively limited in scope.

AWACS. Finally, we are also working on a successor program to the AWACS, called the Alliance Future Surveillance and Command System (AFSC). The AWACS fleet will reach the end of its life cycle around 2035 and now is the right time to start thinking about its replacement. As those of you who are engaged in acquisition know, this is around the corner and we are already short on schedule if we want to meet that 2035 schedule. For decades, the AWACS fleet has been NATO's "Eye in the sky" and it has played an important role in recent operations. For the follow-on to the fleet, we are exploring all sorts of solutions including drones, linked sensors, manned platforms or a mix of systems. We need to be innovative in the way we approach such major projects.

Innovation—To Have the Right Capabilities

Keeping the technological edge through innovation is key to preserving the Alliance's ability to deter and defend in the years to come. The military has a long history of promoting innovation—The Global Positioning Satellite network and the creation of the internet have changed the world. Now in the digital age, innovation often comes from commercial entrepreneurs, as the cost of computing has plunged, access to markets has eased and new manufacturing technology has developed. What does it mean for us as military and commercial technologies converge, technology costs drop and barriers to employing new technologies fall? This is something that we are working on at NATO to identify opportunities and challenges that come along with this new reality.

In the digital age…what does it mean for us as military and commercial technologies converge, technology costs drop and barriers to employing new technologies fall?

We must increase our awareness of what is happening outside traditional defence circles. We need to consider available capabilities to meet the current and future requirements the armed forces have identified. And we should be looking at emerging technologies from all perspectives. While introduction of new technologies has in many cases brought about great advantages, those same technologies have at times ended up being misused by humans, thereby creating new vulnerabilities for our societies.

Cyber

Cyber Security is now high on NATO's agenda. Cyber threats and attacks are becoming more common, more sophisticated and more damaging. All of you probably heard about the recent cyber attack on 'Dyn', a US infrastructure company that acts as a switchboard for internet traffic of sites such as Twitter, PayPal and Spotify. In this attack, the hackers 'weaponized' everyday devices with malware to mount the assault. This huge attack on global internet access, which blocked some of the world's most popular websites, is believed to have been unleashed by hackers using common devices like webcams and digital recorders. What if such method were used to block or bring down the communication means of our militaries during an operation?

In the recent huge attack on Dyn, the hackers 'weaponized' everyday devices with malware to mount the assault…which blocked some of the world's most popular websites.

We are working to confront the wide range of cyber threats targeting NATO's networks on a daily basis and we are also facilitating cooperation among Allies and partners in the field. At the Warsaw Summit, Allies pledged to strengthen their national cyber defences. They reaffirmed NATO's defensive mandate and recognised cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea. During the October 2016 meeting of Defence Ministers, Allies also stressed the importance

of making good on the Cyber Defence Pledge so that we can show real results in the next few years.

Closing Remarks

For nearly seven decades, NATO has helped keep peace in Europe. Allies have been united by a common set of values—democracy, human rights and the rule of law, and this has forged a very strong bond across the Atlantic. Over the years, NATO has changed as the world has changed. We must remain committed to our values, to our determination to defend one another, and to help promote peace and security for future generations.

France Is at War—The Ramifications in Cyberspace

Vice Admiral Arnaud Coustillière
General Officer Cyber Defense, French Ministry of Defense

For the third time, I am particularly happy to address this workshop, since cybersecurity brings new challenges every year—especially in the war against terrorism. Djihadism, which strikes us on our own soil, gives my Ministry of Defense a vital mission: to protect and defend our nation against an increasingly unpredictable enemy—today it is Daesh, in a month it could be Al-Qaeda, or even other groups. Nonetheless, it is the same threat that will evolve and reuse the same techniques of combat.

Today, the enemy is Daesh, in a month it could be Al-Qaeda … Nonetheless, it is the same threat that will evolve and reuse the same techniques of combat.

This particular enemy utilizes propaganda as well as relatively low-level cyber attacks in an attempt to target and terrorize both civilians and the military. Like most nations that are represented here today, France is facing adversaries with offensive capabilities that they can utilize directly—or indirectly through groups, such as mafias, that rent their services. Therefore, our forces, whether purely national, participating in coalitions, or operating within an alliance, must be able to deploy and to execute their missions. This means that we must first guarantee our capacity to protect against cyber attacks by detecting them, identifying their authors, and also preparing to respond by all available means, which are not necessarily either digital or cyber.

In any case, all of these missions respond to the notion of national sovereignty. Although cyberspace has been entirely created by man, we are becoming aware that perceptions in cyberspace can be disrupted and manipulated. We also see that national borders can be entirely erased, and that cyberspace has become a new domain of strategic combat, alongside land, sea, air, and space. The emergence of this new domain is especially striking, since it has shortened the usual passage of time. Its history dates back only ten years, and the awareness of cyber attacks go back only to 2008 or 2010—and we are now just in 2016. In the case of air war, it took 30 or 40 years to develop into an area of strategic importance. Therefore, this compression of time is a unique challenge for our armed forces, for our diplomats, for the establishment of norms, and for our work in the UN, NATO, the EU, and for all of our societies.

Perceptions in cyberspace can be disrupted … national borders can be erased, and cyberspace has become a new domain of strategic combat, alongside land, sea, air, and space.

The cyber domain has brought surprises. The years 2014-2015 were marked by Daesh propaganda, which led to attacks on our territory. During 2015-2016 there were new kinds of events—groups of Russian origin making attacks that appear to be of a strategic nature. These are not mafia groups, because they have a strategy. In addition, there were distributed denial of service (DDoS) attacks of a new kind. In the past, DDoS attacks generally served to slow or block websites. But recently, these attacks reached an

unprecedented scale by using connected devices (IoT), which is cause for considerable concern. One attack was directed at a large French operator, OVH, which housed many websites. Another DDoS attack knocked out a portion of the Vietnamese internet for several hours. Using the same malware, another attack targeted an internet DNS (domain name server) hosting service, knocking out large sections of the internet for several hours. These brute force attacks highlight the issue of internet resilience. When the internet fails in one country, or in part of a country for several hours, it is not necessarily economically serious, but if the failure triggers others and if the interruptions of the internet last for several days, the consequences in the real world become serious. In this case, large sections of the global economy, principally banks or others, can collapse and the interdependence of states can be impacted.

Recently, these attacks reached an unprecedented scale by using connected devices (IoT), which is cause for considerable concern.

Therefore, we need to respond in a manner that is strategic, globally operational, and permanent. At the military level, this means assuring control over the cyberspace, just as our conventional forces must deploy in order to protect themselves and their liberty of action. In this case, our forces—both defensive and offensive—generally intervene from or are deployed within a theater of operations. They act independently or in support of conventional forces. This represents a major revolution in our operations and the way that we conduct them. Today, no operations are launched without the deployment of a cyber element. Nonetheless, these information systems, which have been considered until now as force multipliers that provided information superiority over an enemy, present such an extremely large number of vulnerabilities that we must be able to adapt and protect our devices.

The need for a strategic response can also require us to disrupt a potential adversary by interfering with his liberty of access to cyber space and to attack our enemies from the moment when they themselves are vulnerable.

The need for a strategic response can also require us to disrupt a potential adversary by interfering with his liberty of access to cyber space and to attack our enemies from the moment when they themselves are vulnerable. This requires a capacity for reactive action and defensive operations in order to weaken or neutralize the effects of a cyber attack on our operational capacities. The latest military planning law in France authorizes our military cyber defense as well as civilian cyber defense, under the direction of Guillaume Poupard, to act together with our partners to neutralize cyber effects on those of our systems that are considered vital. In our military operations today, we systematically integrate this requirement in both our planning and in the actual conduct of our operations. This is why our cyber posture and capabilities are adapted to each of our theaters: we structure our capabilities just as we do for another space of warfare. Today, the Middle East is our principal theater of engagement, but it is an enlarged Middle East that extends all the way to the Sahel band, since the Islamic groups inspired by Salafism that we know are as

active in Iraq as in Syria, with reversals in the real world that will motivate them to redeploy in the virtual world in a more significant way.

A barbarian conception of the digital world plays a central role in the doctrine of the Islamic Salafists. There is an excellent document concerning Al-Qaeda's doctrine, which is called "La Gestion de la Barbarie" in French and "The Management of Savagery" in the initial English version that was written in Pakistan in 2004, which describes this new element of their military operations. Countering their barbarian activities is an integral part of our reaction to their propaganda. Beyond this, in order to strike Daesh wherever they may be found, we must act collectively in order to strike their exposed digital attack surface, in full respect of the laws of armed combat when the attack occurs in a theater of operations as well as the laws in force in each of our countries. If the propaganda originates in the Rakka zone or Mosul, it has a material dimension in the form of digital records located in various countries. Accordingly, it is subject to their laws and regulations, and actually to the laws of every country since they are found in Belarus, in Germany, in France, in the US, and in Britain and they are normally housed by large international internet service providers. Without citing names, all the large international companies participate, but that means that each state much mobilize itself, and learn through its own intelligence services and police forces how to neutralize and eliminate all of the propaganda already on its territory. This is why we need international organizations to cooperate. In this respect, I would like to recognize the importance of the NATO Centers of Excellence in Tallinn and in Riga, which work principally on these subjects and which are good places for exchanging information and for discussions. We must understand the tactics of the adversary, develop intelligence adapted to his methods and his behavior in cyberspace. It is also necessary to confront his liberty of maneuver as we do in other spaces and be capable of destabilizing or even neutralizing him within his digital sanctuary. Therefore, the responsibility of the ministry of defense covers a field of action where the rapidity and the adaptability of our response must counter the intensity of the threat, which can be at the same time extremely technical or, without being technical, extremely clever at exploiting niches in the internet.

A barbarian conception of the digital world plays a central role in the doctrine of Islamic Salafists … one book describing it is called "La Gestion de la Barbarie" in French and "The Management of Savagery" in English.

Attribution will be the result of converging factors—technical elements and less technical—which will not allow us to say immediately if the attack comes from a certain country.

We must prepare for a deepening of our bilateral cooperation and coalitions. Cyberspace is not a space for tactical combat, and that is why it cannot be easily compared to air or maritime spaces. In tactical combat, there would be two cyber forces attacking each other and responding with malware. This is not the way it occurs today. Cyberspace has a special rhythm. The time required to understand that you have been the victim of a cyber attack can be very long, and therefore it does not occur concurrently with the response. In a cyber attack, you learn that an information system has crashed, and you see

the consequences immediately, but it takes time to understand how it occurred and attribution is difficult to achieve with certainty. Generally, attribution will be the result of converging factors—technical elements and less technical ones—which will not allow us to say immediately if the attack comes from a certain country as one would be able to do in another space where you know very well that an aircraft has taken off with a bomb and where the bomb has been dropped. Attribution is a complicated subject that will be the result of a political decision at the highest level in each of our countries. We can see that in the two examples in the United States where it has been the president who made the announcement on two successive occasions to attribute the attack to a state, North Korea in one case, and Russia in the other case. Therefore, it is a situation where the cyber action is especially indirect and it will attack in preference the weak link of our societies and seek to destabilize areas that are known to cause harm to a country. That is why, in this space, one cannot act alone. It is necessary to reinforce our relationship of strong trust with our closest allies who have the capabilities necessary to act. These are the members of NATO and the European Union, who have the capabilities and a particularly important role to play. We must also collectively encourage the development of cyberdefense within NATO and the European Union by recognizing it as a complete domain alongside the others, and these are the efforts that will be engaged within NATO in the years to come.

It is important to develop close relations with a larger circle of important actors in order to better anticipate the evolution of threats, and to engage a dialogue with all the others in order to avoid escalation.

It is equally important to develop close relations with a larger circle of important actors in order to better anticipate the evolution of threats, and to engage a dialogue with all the others in order to avoid escalation. We must research the establishment of norms for the employment or de-escalation of cyber arms. With our key allies—I am thinking first of our American and British partners—the operational stakes constitute a very strong basis for increased cooperation in this area.

Finally, this extremely technical capacity rests above all on men and women. We can develop all of the information systems that may be possible to attack or defend, but if we do not have competent human resources, qualified, and in sufficient numbers, we will be ineffective. The cyber world is above all about human intelligence, tactical innovation, and technology, but above all it requires individuals who are capable of thinking in a different manner. The principal challenge is more than ever the investment in human resources. One of the efforts in France is the creation of a cyber defense reserve, with special work conditions for its personnel since they must work in conditions fairly close to those who work on information systems. Their biological rhythm is determined by the rhythm of the theater of combat in which they are engaged. Even if they are based in Paris, they can be in the rhythm of operations that take place in Iraq or in Syria, at tens of thousands of kilometers. This cyber defense reserve must be capable of being at the disposal of State services and work

We can develop all of the information systems that may be possible to attack or defend, but if we do not have competent human resources, qualified, and in sufficient numbers, we will be ineffective.

principally with the National Agency for the Security of Information Systems (ANSSI), as well as for the Gendarmerie Nationale (the National Police) which is our point of entry into the Ministry of the Interior. We foresee 400 reservists who will be very specialized in order to perform rapid interventions that occur in partnership with the principal French actors in cybersecurity, as well as a reserve of 4,000 people that we will more likely seek in partnership with the engineering schools that form engineers for cyber defense in France.

To conclude, information systems have become indispensable tools for the majority of the sectors of activity of our modern societies. They will evolve and we can see that easily with the arrival of connected objects (IoT). If one can already see that the richness of cyberspace is the digital domain, the actor of cyberspace is the IP address and the number of IP addresses is about to be multiplied by factors of a thousand, or even ten thousand—enough possibilities to multiply the power of calculations that organizations can mobilize to attack and put in danger the resilience of the internet.

The response of all democratic nations to these attacks … must be to conceive national and international legal frameworks, which must be able to evolve as necessary, be relatively flexible, and be appropriate for evaluating the threats.

Cyberspace is marked by notions of asymmetry, "fog of battle," and surprise. In my opinion, the response of all democratic nations to these attacks, which are generally hidden, must be to conceive national and international legal frameworks. These frameworks must be able to evolve as necessary; they must be relatively flexible and appropriate for the evaluation of the threats—while we know that the law operates with a speed that does not necessarily correspond to that of strategic surprise. The adversaries show initiative and they have many forms. Some of them belong to the cyber criminality, which today is galloping, and hiding among the cyber criminals are groups that have much more strategic goals. The actors of cyber criminality and these groups with strategic interests are often the very same and they often use the same tools. They know our areas of weakness perfectly, know how to exploit them, and the possible scenarios range from massive attacks—some even speak of a cyber Pearl Harbor—to the scenarios in the form of propaganda that are even more destabilizing. This domain, as you have very well understood, is a very high priority of the Minister of Defense, Jean-Yves Le Drian, who has dedicated very significant resources—my organization has been multiplied in size by a factor of 100 in four or five years—and he will announce in mid-December a new and seminal speech concerning this domain.

L'Espace numérique comme espace de combat et de confrontation stratégique

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

Je suis très heureux d'intervenir pour la troisième fois devant vous car chaque année le domaine cyber nous réserve des surprises et la menace cyber nous concerne tous, surtout aujourd'hui dans la guerre contre le terrorisme. Le djihadisme, qui frappe jusqu'à notre propre sol, confère à mon ministère une mission majeure, celle de protéger et défendre notre nation contre un ennemi de plus en plus imprévisible—Daesh aujourd'hui, peut-être de nouveau Al-Qaeda dans quelques semaines, ou encore d'autres noms, mais il s'agit de la même identité qui va muter et réutiliser les mêmes techniques de combat.

La mission de mon ministère est de protéger et défendre notre nation contre un ennemi de plus en plus imprévisible—Daesh aujourd'hui, peut-être de nouveau Al-Qaeda dans quelques semaines…

Cet ennemi imprévisible utilise sans grand succès pour l'instant des moyens numériques plus ou moins techniques, la propagande, mais aussi des attaques informatiques de bas niveau pour cibler et tenter de terroriser les populations civiles et militaires aussi bien chez nous que chez nos partenaires qui sont engagés. Comme la majorité des nations représentées ici, la France est confrontée à ces adversaires ou à des adversaires dotés de capacités offensives qu'ils peuvent utiliser directement ou à travers des groupes, des mafias, qui louent leurs services. Donc la maîtrise de cette nouvelle donne doit permettre à nos forces, qu'elles soient engagées sur le théâtre national, engagées dans une coalition ou au sein d'une alliance, de se déployer et de conduire leur mission. Nous devons tous tout d'abord garantir notre capacité à nous protéger contre les attaques informatiques en les détectant, en identifiant leurs auteurs, et aussi en se préparant à y répondre par tous les moyens disponibles, qui ne sont d'ailleurs pas forcément une réponse informatique.

En tout cas, l'ensemble de ces missions répond aujourd'hui à une notion de forte souveraineté nationale. L'espace numérique a été entièrement fabriqué par l'homme mais on prend conscience aujourd'hui que c'est un espace où les perceptions peuvent être perturbées et manipulées. On voit aussi que les différentes frontières y sont totalement gommées et que cet espace est devenu un nouvel espace de combat et de confrontation stratégique au côté des autres espaces de combat que sont l'espace terrestre, maritime, aérien et spatial. Les particularités de cet espace, qui raccourcit le temps, sont particulièrement intéressantes. Quand on regarde l'introduction de la donne stratégique de l'espace numérique, son histoire remonte à une dizaine d'années. La prise de conscience des grandes attaques informatiques

L'espace numérique est devenu un nouvel espace de combat et de confrontation stratégique au côté des autres espaces de combat que sont l'espace terrestre, maritime, aérien et spatial.

à but stratégique remonte à 2008, 2009, 2010 et on est aujourd'hui en 2016. Le monde aérien, en revanche, a mis plus de trente à quarante ans pour s'imposer comme une donne stratégique de grande importance. Donc, ce raccourcissement du temps est un défi à la fois pour les forces armées, pour les diplomates, pour l'édiction de normes, pour tout le travail qui se fait au sein des instances spécialisées de l'ONU, de l'OTAN, de l'UE, et il concerne l'ensemble de nos sociétés.

Ce domaine réserve des surprises. Si la période 2014-2015 a surtout été marquée par l'introduction de la propagande islamiste de Daesh qui a permis de frapper nos territoires, entre 2015 et 2016, on voit apparaître deux phénomènes à la fois complémentaires et différents. On voit d'abord des groupes d'origine russophone mener des attaques à but stratégique ou du moins présentées comme telles. Ces groupes ne sont pas mafieux car ils ont bien une stratégie. Ensuite, on voit revenir une technique d'attaque dite par saturation ou déni de service qui servait généralement à neutraliser un site web. Récemment, ces attaques par déni de service ont acquis une ampleur inégalée par l'utilisation des objets connectés et donnent à réfléchir. Une attaque a visé un gros opérateur français, OVH, qui héberge de nombreux sites. Par utilisation détournée ou par saturation de plaque de l'internet, elle a fait tomber pendant quelques heures une partie de l'internet Vietnamien, tout simplement parce qu'au Vietnam, la plaque internet n'était pas assez résistante. Dans ce cas, il s'agit d'une attaque d'un opérateur en France qui fait tomber une partie faible de l'internet. Mais avec le même logiciel, une autre attaque a visé un prestataire de service de l'Internet sur ce que l'on appelle en jargon le DNS (domain name system) et a fait tomber des pans entiers de l'internet pendant plusieurs heures. Cette technique d'attaque en force brute met en avant le problème de la résilience de l'internet. Quand l'internet tombe dans un pays ou sur une partie d'un pays pour quelques heures, ce n'est pas grave—économiquement peut-être—mais si cette fêlure en entraîne d'autres et si l'interruption de l'internet dure plusieurs jours, les conséquences dans le monde réel deviennent sérieuses. Ce sont des pans entiers de l'économie mondiale, principalement bancaires ou autres, qui peuvent s'écrouler et l'interdépendance des Etats à ce moment là peut être atteinte.

Récemment, ces attaques par déni de service ont acquis une ampleur inégalée par l'utilisation des objets connectés.

Donc nous devons apporter une réponse stratégique et opérative globale et permanente. Au niveau militaire, il s'agit de s'assurer de la maîtrise du cyber espace comme de la maîtrise des espaces dans lesquels nos forces sont appelées à se déployer afin de préserver et protéger nos forces ainsi que nos libertés d'action. Dans ce cas, nos forces—défensives ou offensives—interviennent en général à partir d'un territoire ou sont déployées sur des théâtres. Elles agissent de façon autonome ou en soutien et pleine complémentarité avec des forces conventionnelles. C'est une évolution majeure dans nos opérations et dans la façon de les conduire, et il n'y a pas aujourd'hui d'opérations qui démarrent sans que l'on ne déploie le volet cyber. Cependant, ces systèmes d'information, présentés jusqu'à maintenant comme des multiplicateurs de forces permettant d'avoir la supériorité informationnelle sur un ennemi, présentent aujourd'hui un tellement grand nombre de vulnérabilités qu'il faut être capable d'adapter et de protéger nos dispositifs.

Cette réponse stratégique peut aussi nous demander de perturber un adversaire potentiel en entravant son propre libre accès au cyber espace, et d'attaquer nos ennemis à partir du moment où ils sont eux aussi vulnérables. Le contrôle demande à la fois des capacités d'action réactives et d'opérations défensives permettant d'atténuer, voire de neutraliser les effets d'une attaque cyber sur nos capacités opérationnelles. Les évolutions législatives de la dernière loi de programmation militaire mettent en place en France un article qui autorise les agents de la cyberdéfense militaire et de la cyberdéfense civile sous le commandement de Guillaume Poupard à mener un certain nombre d'actions avec nos partenaires pour neutraliser les effets d'une attaque contre nos systèmes considérés comme importants. Dans les opérations militaires d'aujourd'hui, nous intégrons systématiquement cette dimension, aussi bien en anticipation et planification qu'en conduite. C'est pourquoi la posture cyber et les moyens d'action sont adaptés à chacun de nos théâtres : on taille un dispositif comme on le fait pour les autres espaces. Le Levant est aujourd'hui notre principal théâtre d'engagement, mais c'est un Levant élargi jusqu'a la bande Sahélienne puisque les groupes islamiques d'inspiration Salafiste que nous connaissons agissent tant en Irak qu'en Syrie avec des revers dans le monde réel qui vont les amener à se redéployer dans le monde virtuel de façon plus importante.

Cette réponse stratégique peut nous demander de perturber un adversaire en entravant son propre libre accès au cyber espace, et d'attaquer nos ennemis au moment où ils sont eux aussi vulnérables.

La barbarie numérique des groupes islamiques Salafistes fait partie de leur doctrine. Il existe un excellent document de doctrine des djihadistes d'Al-Qaeda qui s'appelle « la Gestion de la Barbarie » en français et « The Management of Savagery » dans sa version initiale anglaise écrite au Pakistan en 2004 qui décrit ce nouvel élément de leurs opérations militaires. Contrer leur barbarie fait partie intégrante de la stratégie de l'action et nous devons adapter notre réaction face à leur propagande. Au-delà, pour frapper Daesh partout, il nous faut agir de façon collective et nous attaquer à leur surface d'exposition numérique dans le respect du droit des conflits armés quand l'action se passe sur le théâtre d'opérations mais aussi dans le respect des lois en vigueur dans chacun de nos pays. Si cette propagande est inspirée à partir de la zone de Rakka ou de Mossoul, elle a une matérialisation, des documents numériques qui sont hébergés dans nos différents pays, donc soumis aux lois et règlements de nos différents pays principalement, et également de tous les pays puisque on en trouve aussi bien en Biélorussie, en Allemagne, en France, aux Etats-Unis, au Royaume-Uni et ce sont généralement les grands opérateurs de l'internet qui les hébergent. Sans citer de noms, toutes les grandes compagnies participent mais cela veut dire que chaque Etat doit apprendre à se mobiliser, apprendre à l'intérieur de ses propres services de renseignement et de police à traquer cette propagande qui est un crime contre la démocratie et les citoyens de nos pays et apprendre à neutraliser et faire disparaître l'ensemble de cette propagande déjà sur son propre territoire. C'est bien pour

Pour frapper Daesh partout, il nous faut agir de façon collective et nous attaquer à leur surface d'exposition numérique dans le respect du droit des conflits armés…et des lois de nos pays.

cela que nous avons besoin d'instances internationales pour coopérer. Je salue dans ce sens l'action des centres d'excellence de l'OTAN de Tallin et de Riga, qui travaillent principalement sur le sujet et qui sont des bons lieux d'échanges et de discussions.

Nous devons comprendre le mode opératoire de l'adversaire, développer un renseignement adapté à ses tactiques, sa façon de procéder et de se déployer dans l'espace numérique. Il faut aussi contester sa liberté de manœuvre comme nous le faisons dans les autres espaces et être capables de le déstabiliser ou même de le neutraliser dans ses sanctuaires numériques. Donc, la responsabilité du ministère de la défense recouvre un champ d'action où la rapidité et l'adaptabilité de la réponse doivent pouvoir contrer l'intensité de la menace qui peut à la fois être extrêmement technique ou peu technique mais habile à exploiter de façon remarquable les recoins de l'internet. Nous devons nous préparer en approfondissant nos coopérations bilatérales et nos coalitions. L'espace numérique n'est pas un espace de combat tactique et c'est pour cela qu'il est difficilement comparable à l'espace aérien ou à l'espace maritime. Dans le combat tactique, on aurait deux forces cyber qui s'attaquent ou qui se répondent avec des malwares. Ce n'est pas comme cela que cela se passe aujourd'hui. L'espace numérique a un temps particulier. Le temps pour comprendre qu'on a été victime d'une attaque informatique est du temps long, donc il n'est pas dans le temps de la réponse. Dans une attaque informatique, on comprend qu'un système informatique est tombé, on en voit immédiatement les conséquences, mais il nous faut du temps pour comprendre la panne et l'attribution de façon certaine est difficile. Généralement, l'attribution va reposer sur la convergence de facteurs d'appréciation—d'éléments techniques et d'éléments moins techniques—qui ne permettent pas de dire immédiatement si l'attaque vient d'un tel pays comme on peut le voir dans un autre espace où l'on sait très bien d'où un avion décolle avec une bombe et où la bombe a été larguée. L'attribution est un sujet compliqué qui résulte le plus souvent d'une décision politique au plus haut niveau dans chacun de nos Etats. On le voit bien avec les deux exemples récents aux Etats Unis où c'est bien la présidence qui s'est prononcée deux fois de suite pour attribuer une attaque à un état, la Corée du Nord dans un cas, et la Russie dans un autre cas. Donc, c'est bien un domaine où l'action informatique est particulièrement indirecte et elle va aller s'attaquer de préférence au maillon faible de nos sociétés et chercher à déstabiliser dans des endroits où on sait que cela peut faire mal à un pays. C'est bien pour cela que dans cet espace, on ne peut pas agir seul. Il faut renforcer nos relations de très grande confiance avec nos alliés les plus proches qui possèdent des capacités en la matière pour opérer. C'est bien là où les membres de l'OTAN et de l'Union européenne qui disposent de capacités ont un rôle particulièrement important à jouer. On doit aussi collectivement encourager le développement de la cyberdéfense au sein de l'OTAN et de l'Union européenne en la faisant reconnaître comme un domaine à part entière aux côtés des autres, et ce sont les travaux qui vont s'engager au sein de l'OTAN dans l'année à venir.

L'intensité de la menace…peut à la fois être extrêmement technique ou peu technique mais habile à exploiter de façon remarquable les recoins de l'internet.

Généralement, l'attribution va reposer sur la convergence de facteurs d'appréciation—qui ne permettent pas de dire immédiatement si l'attaque vient d'un tel pays.

Il faut également apprendre à développer des relations étroites avec un cercle plus large de grands acteurs pour mieux anticiper l'évolution des menaces, et entretenir un dialogue avec tous les autres pour éviter les escalades. Nous devons rechercher l'établissement de normes de comportement et d'encadrement dans l'emploi ou dans la désescalade de ces armes informatiques. Avec les grands alliés—je pense en premier lieu à nos partenaires américains et britanniques—les enjeux opérationnels constituent un lien très fort pour une coopération accrue dans ce domaine.

Nous devons développer des relations étroites avec un cercle plus large de grands acteurs pour mieux anticiper l'évolution des menaces, et entretenir un dialogue avec tous les autres pour éviter les escalades.

Enfin, cette capacité extrêmement technique repose avant tout sur des hommes et des femmes. On peut développer tous les systèmes informatiques possibles pour attaquer et se défendre mais si nous ne disposons pas derrière d'une ressource humaine compétente, qualifiée, et en nombre suffisant, nous serons inefficaces : le monde cyber est avant tout de l'intelligence humaine, de l'innovation tactique, technologique, mais surtout des individus capables de penser de façon différente. Le principal défi est plus que jamais l'investissement dans les ressources humaines. L'un des enjeux en France est la mise en place d'une réserve de cyber défense avec des conditions de travail particulières pour ce personnel parce que s'ils travaillent dans des conditions assez proches de ceux qui travaillent sur les systèmes d'information, leur rythme biologique est fixé par le rythme du théâtre de combat dans lequel ils sont engagés. Même s'ils sont basés à Paris, ils peuvent être dans le rythme d'opérations qui se déroulent en Iraq ou en Syrie à des dizaines de milliers de kilomètres. Cette réserve de cyberdéfense doit être capable de se mettre à la disposition des services de l'Etat et travailler principalement avec l'Agence nationale de sécurité des systèmes d'information (ANSSI) mais aussi avec la gendarmerie nationale qui est notre point d'entrée vers le ministère de l'intérieur pour ce domaine. Nous prévoyons 400 réservistes très spécialisés pour faire de l'intervention rapide qui seront mis en place en partenariat avec les grands acteurs français de la cybersécurité, ainsi qu'un réservoir de 4000 personnes que nous allons plutôt chercher en partenariat avec les grandes écoles qui forment des ingénieurs en matière de cyberdéfense en France.

Si nous ne disposons pas derrière d'une ressource humaine compétente, qualifiée, et en nombre suffisant, nous serons inefficaces.

Pour conclure, les systèmes d'information sont devenus des outils indispensables à la majorité des secteurs d'activité de nos sociétés modernes. Ils vont évoluer et on le voit bien avec l'arrivée des objets connectés. Si l'on peut dire aujourd'hui que la richesse de l'espace numérique, c'est la donnée numérique, l'acteur de l'espace numérique est l'adresse IP et cette adresse est en train d'être multipliée par des facteurs de mille, voire dix mille— autant de possibilités de relais pour agir dans l'espace numérique et multiplier la puissance de

L'acteur de l'espace numérique est l'adresse IP et cette adresse est en train d'être multipliée par des facteurs de mille, voire dix mille.

calcul que des organismes peuvent mobiliser pour attaquer et mettre en péril la résilience de l'internet.

L'espace numérique est marqué par des notions d'asymétrie, de brouillard, de surprise et, à mon avis, la réponse de l'ensemble de nos nations démocratiques à ces attaques généralement masquées doit s'inscrire dans un cadre légal national et international. Ce cadre légal devra être très évolutif, rester relativement flexible et approprié à l'évaluation de la menace alors que l'on sait que le droit est dans une constante de temps qui n'est pas celle de ce que l'on pourrait appeler les surprises stratégiques. Les adversaires, eux, font preuve d'initiative, ils sont multiformes. Certains utilisent et font partie de la cybercriminalité, qui est aujourd'hui galopante, et au milieu de la cybercriminalité se cachent des groupes qui ont des visées beaucoup plus stratégiques. Les acteurs de la cybercriminalité et de ces groupes sont souvent les mêmes et ils utilisent souvent les mêmes outils. Ils connaissent parfaitement nos failles, savent les exploiter et les scénarios vont depuis des attaques massives—on parle même de Pearl Harbour cyber—jusqu'a des scénarios qui sont plus déstabilisants en matière de propagande. Ce domaine, comme vous l'avez compris, est une très forte priorité du ministre de la défense Jean-Yves Le Drian, qui y a consacré des moyens très importants—mes effectifs ont été multipliés par 100 en quatre ou cinq ans—et il prononcera à la mi-décembre un nouveau discours fondateur dans ce domaine.

Certains groupes ont des visées beaucoup plus stratégiques—on parle même de Pearl Harbour cyber—jusqu'à des scénarios qui sont plus déstabilisants en matière de propagande.

The UN Group of Governmental Experts: Perspectives for the 2016/2017 Round

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

Since I am a speaker in this session, I am confronted with a constraint: as France's national expert at the UN group of governmental experts (GGE), I am not supposed to disclose what we are talking about in New York but, at the same time, we have been invited by the chairman of the GGE to do a lot of outreach. Therefore, I will speak on behalf of France about our ideas and will try to open a few perspectives.

Where are we right now? We have started the 2016/2017 round of the GGE after the two very successful 2013 -2014 and 2014-2015 rounds, which were extremely productive. The experts agreed that the last two reports were really ambitious, very clear, and very good, which is quite something since the partners were absolutely not on the same page at the beginning of the discussions. There was great success in clarifying or acknowledging the fact that international law is fully applicable to cyberspace, and that we must create norms of behavior and put a new focus on the need to have very ambitious capacity building programs. This is our starting point.

International law is fully applicable to the cyberspace; we must create norms of behavior…and have very ambitious capacity building programs.

We are all fully convinced—and we are now 25 national experts—that we need to keep working on those norms and be ambitious because the situation is quite crazy. It is the Wild West out there and so far, our response has been smart, but not that efficient. Our first challenge is to make our work better known around the world. It is the challenge of the universalization of the GGE work and of its reports. Sometimes, it seems that the Tallin manual is better known than the GGE report and it is a shame. So, how shall we universalize our work? We will probably think about a UN resolution, not for 2016, but this is something that we have to bear in mind. The universalization and publication processes have started, and the G20 has endorsed the GGE report, which included influential people like President Obama.

Our first challenge is to make our work better known around the world… it sometimes seems that the Tallin manual is better known than the GGE report.

Second, we should try to think a bit differently about these topics and keep in mind our main objectives, which are: prevention, cooperation, and stability. We are now going in that direction.

Prevention

Concerning prevention, we keep thinking that our main objective should be to reduce the attack surface of critical national infrastructure. We all agree on the fact that states are primarily responsible for enforcing their Information and Communication Technology (ICT) security—what NATO Assistant Secretary General Camille Grand said earlier is exactly consistent with this—and thus contributing to the global security and stability of cyberspace. This responsibility is particularly strong when it comes to protecting the critical national infrastructure (CNI). An attack against a privately or state-owned critical infrastructure which significantly impairs its functioning may be considered as damaging that state's national security. So, we have presented two additional norms of behavior on that very topic.

Cooperation

We believe that it is important to ensure a better management of the spread of malicious ICT tools and techniques, but there is no consensus on that, which is why we want to push on this. In 2015, the experts agreed that—I quote—"states should seek to prevent the proliferation of malicious ICT tools and techniques." As you may know, the 41 members of the Wassenaar arrangements agreed in 2013 to work on controlling the exports of intrusion software as a means to prevent this proliferation. There is still no consensus on that, but we are absolutely convinced that, if we want to stabilize the cyberspace, we need to create a norm of behavior and try to make it as operational as possible via exports control.

On the management of ICT vulnerabilities, the group agreed in 2015 that—I am quoting again—"States should encourage responsible reporting of ICT vulnerabilities." In order to increase the global level of cyber security, states should commit more clearly to prioritizing responsible reporting and patching over the exploitation of ICT vulnerabilities for offensive means. This proves all the more difficult when intelligence and cyber security functions are intertwined within a state's organization. We will make a proposal on this topic too, because we think we will not be in a position to reach any kind of stability without a clear understanding of what a responsible management of ICT vulnerabilities is. As regards cooperation, we should work on creative cooperative mechanisms for the implementation of the norms that we have produced. We know that the 2015 GGE report has come up with a large set of positive norms of behavior as well as confidence-building measures intended to increase the resilience of states and prevent conflict stemming from ICT. It is extremely difficult, given the attribution challenges that Admiral Coustillière discussed, to verify the implementation of norms of restraint by states, namely what states should not do—the so-called negative norms. But we think it is possible to assess the implementation of so-called positive norms by states. These norms relate to the protection of critical infrastructure, the prevention of proliferation, the responsible handling of vulnerabilities, the cooperation in incident handling etc. We could

We can assess norms relating to the protection of critical infrastructure, prevention of proliferation, responsible handling of vulnerabilities, cooperation in incident handling etc.

create a sort of peer review mechanism on a voluntary basis for states that want to be assessed on what they have been doing to try and implement all those norms. So, we are in favor of multilateralism in the field of cyber; we will see if it flies or not, but we think it is a necessary beginning.

Stability

We believe that we should draw all the concrete consequences from the previous GGE reports that acknowledge the fact that international law is now fully applicable. This really means that we assume that the UN Charter is fully applicable. We have a few ideas on this that we would like to verify and start discussing. I will conclude with two points:

In this round, we face the same tension that we faced in the past between:

- A need to keep cyber issues fully dependent on sovereign policies and sovereign decisions. France wants to hold on to that because we need our military to be able to make decisions and implement policies and this is fully part of the French doctrine on cyber defense and,
- The perspective of building a cyber collective security or stability in the cyberspace by looking at what has worked in other fields of disarmament and incorporating those processes and principles that have worked, including what the UN has produced. There are many good things in the international criminal justice, in international investigative commissions, and all this can be extremely promising. Of course, the main condition to open such a path remains the issue of attribution and it is not only attributing the attack to a set of computers, it is also attributing it to one person behind a computer or behind a keyboard and maybe attributing it to those who have ordered the attack. It is already difficult to find the machine, it is even more difficult to find out who is behind the keyboard. So, we know that all those ideas won't fly today and we just want to create a discussion around them because we think they are promising.

It is already difficult to find the machine, it is even more difficult to find out who is behind the keyboard.

For my second point, I would say in conclusion that the GGE covers state actors and state behaviors, but we also need to talk about non-state actors and non-state behaviors. Again, we have to find a way to talk about that. We do not hope to be in a position to make progress on this topic inside the GGE because it is not the GGE's mission, but we must find a way to talk about this and find solutions. And I am not only talking about legitimate or illegitimate actors; there are also hacking boutiques that work very efficiently on behalf of many governments.

EU Efforts in Increasing Global Cyber Stability

Ms. Heli Tiirmaa-Klaar

Head of Cyber Policy Coordination, Conflict Prevention and Security Policy Directorate, European External Action Service

Background

The 2013 EU Cybersecurity Strategy proposed that cyberspace should not be a domain without norms, rules and principles. Cyber should be governed by the same norms that apply offline in the physical world. This means that our existing laws such as the law of armed conflict or criminal justice legislation apply in cyberspace without having to create new instruments, treaties and laws. We just need to mainstream these norms and laws as they apply to cyberspace.

New cyber developments have shown a trend towards increasing instability, tension and disruption. It seems that we mostly hear bad news about cyberattacks intent on causing disruptions and it is sort of the Wild West. However, those who have been dealing with cyber issues for a long time are witnessing a paradigm shift and some good news. First, we have progressed from a very uncertain period where key cyberspace actors did not want to talk to each other. Now, they want to talk to cooperate on ways to achieve more stability. At the UN, the Groups of Governmental Experts (GGE) are working on creating norms of behavior and on ambitious capacity building programs. In the OSCE, we have approved two sets of confidence-building measures (CBMs) on cybersecurity and we have a confidence building measure on cyber at the ASEAN Regional Forum. We are in a process of rapidly globalizing a norms-based approach on cyber issues. Thanks to the efforts of EU countries, the United States, other like-minded governments, and the UN GGE countries that are discussing cyber norms, we are at a stage where responsible international actors and major nation-states are moving toward a political agreement on the cyber domain's future.

We are in a process of rapidly globalizing a norms-based approach on cyber issues.

Today, all developed governments have their own advanced cyber policies, strategies and doctrines. Only a couple of years ago, many governments, even in the EU, did not have even a clear understanding of who the ministers in charge of cyber were. I can assure you that the situation is quite different now and all twenty-eight EU countries know their cyber ministers. These international and national efforts that have been achieved over the past decade are carrying us to a new stage where cyberspace is not separated from the real space. NATO's decision to declare cyberspace as a domain clearly indicates that a major international organization is already thinking in terms of doctrine, planning, training and capability advancement and development in cyber.

EU Efforts towards Improving Global Cyber Security

We are fostering cyber cooperation with key international partners and have a dialogue with the most technically-advanced countries—the US, Japan, South Korea, as well as countries that are rapidly growing in the cyberspace area like China, Brazil and India. With these partners, we are discussing all international security issues and norms, the applicability of international law, and capacity building. Since the EU is known for its very strong policies on cyber resilience and fighting cybercrime, most of our international partners would like to learn from us, with the exception of advanced countries. We are also pushing to make the normative approach in cyberspace more global through the OSCE's two sets of confidence building measures and the very valuable UN GGE process that we just discussed. But this is still a "small club" type of discussion and not all countries understand what we talk about when we discuss application of international law in cyberspace, the kind of norms we need, or what cyber confidence building measures are.

Internally, the EU seeks to help enhance cyber resilience. The new Network and Information Security Directive (NIS Directive) make sure that all 28 governments have put the necessary efforts and funding into cyber resilience. We also have a few criminal justice laws that are now all implemented in the 28 countries to make the EU stronger in fighting cybercrime. All these internal practices are driven by the notion that we need norms and principles and sensible but strong regulations, because the private sector can offer very little if the government does not create a cybersecurity demand.

The private sector can offer very little if the government does not create a cybersecurity demand.

The EU is also active in the important field of cybersecurity capacity building. We need more capacity, awareness, education, training and understanding of the technical cyber issues and how all these different bits and pieces of the cyber puzzle come together. The EU is one of the largest donors of global capacity building programs and those are used in developing countries to fight cybercrime and enhance their cybersecurity.

A lesson we have learned from our mistakes is that it is not easy to go to our global partners and talk to them about the need for more cybersecurity, because developing and emerging countries have so many other needs that cybersecurity might not be their most important one. But we are glad to see that other international initiatives are developing like the Global Forum on Cyber Expertise which took place in the Netherlands two years ago and other initiatives where technologically advanced states would arrange a clearinghouse mechanism that would benefit emerging and developing countries that need more cyber capacity. The EU will keep paying attention to these issues as it continues to advance its cooperation with NATO. The EU-NATO declaration that was signed on 8 July of this year contains a cyber chapter that we are actively working on. We are also thinking of updating the 2013 EU Cybersecurity Strategy in order to take the strategic cyber efforts to their next level in the coming years

Developing and emerging countries have so many needs that cybersecurity might not be their most important one.

Cyber Defense: From Wales to Warsaw

Ambassador Marjanne de Kwaasteniet
Permanent Representative of the Netherlands to NATO

From Wales to Warsaw

Cyber defence is an important issue for NATO. Like many other organizations, we have several hundred incidents each month. At the Summits in Wales in 2014 and Warsaw in 2016, we took important decisions:

- In Wales, NATO adopted the Enhanced Policy on Cyber Defence, which focused on defending our networks and decided that cyber is part of our collective defence. We concluded that a cyber attack can cause such destruction or loss of life that an ally could invoke article 5. This important step recognized that cyber is increasingly used in crises and military operations. In a way, we acknowledged that our potential adversaries used cyberspace as an operational domain.
- At the 2016 Warsaw Summit, the logical next step to take was for NATO to recognize cyberspace as an operational domain to better defend ourselves in our missions and operations, and worst case, in an article 5 situation.

Before jumping to such a worst case and less likely scenario, I will first pay attention to the everyday reality of hybrid warfare because we need to be prepared for everyday threats. I will also touch upon the Alliance's Cyber Defence Pledge, NATO's recognition of cyberspace as an operational domain, and offensive cyber. Finally, I will briefly mention cyber partnerships.

Cyber and Hybrid Warfare

Hybrid Warfare is nothing new, but the cyber dimension is relatively new and it has become more relevant. Cyber operations are the hybrid weapon of choice because they can be calibrated along a spectrum of violence.

Cyber has the ability to increase the fog of war and thereby impede our ability to react.

Although I am confident that attribution is possible for NATO, cyber operations do allow for a high degree of ambiguity and this may be one of their main purposes. Cyber has the ability to increase the fog of war and thereby impede our ability to react. This is a challenge to NATO: because of Article 5, only an attack that reaches the qualifying level as an *armed attack* can be responded to collectively. And although a hybrid crisis may potentially lead to the invocation of article 5, most attacks remain well below the threshold of what would be considered an armed attack. The first responder to such attacks is the nation concerned and, as a result, all allies are responsible to be cyber resilient.

Need to Enhance our National Cyber Resilience

In the Alliance, we are all interconnected and are only as strong as our weakest link. Therefore, our heads of state and government have pledged in Warsaw to strengthen the cyber defences of their national infrastructures and networks. The Cyber Defence Pledge aims to ensure that the Alliance keeps pace with the rapidly evolving cyber threat. All Allies ought to be capable of defending themselves and thereby the Alliance at large: this is a priority for the Alliance. It relates to our policy on resilience, which focuses on critical infrastructure protection, continuity of government and, to a certain extent, the maintenance of redundancy systems.

The Cyber Defence pledge is focused on national efforts, but we realized that NATO as an organization has to keep pace and take its responsibility as well. This led to NATO's recognition of cyberspace as an operational domain at the Warsaw Summit.

Recognition of Cyberspace as a Domain

In cyberspace we must defend ourselves as effectively as on land, air and sea. Instead of limiting our focus on ensuring network availability and data integrity, NATO will broaden its focus on mission assurance. The primary and immediate purpose of our cyber defence policy then becomes securing our missions and operations. This includes our operation in Afghanistan and soon our deterrent presence in the Baltic region.

- As a first step, NATO is currently reviewing the way we do business in cyberspace. We need to train, exercise and equip our forces so that we can operate in a contested cyber environment. We are updating our doctrine to seamlessly integrate cyber into our operational planning.
- Next, NATO will have to establish procedures to integrate national sovereign offensive cyber capabilities into a military operation. NATO cannot and should not develop its own offensive capabilities. It always relies on us allies to offer our means. An offensive cyber capability assumes the application of sensitive intelligence. Again, this is gathered by nations, not by NATO.

Allies that have such capabilities at their disposal could be asked by NATO to achieve a specific military effect. How this is achieved is up to the nation. Cyber should be one among the many military instruments at the commander's disposal. Offensive cyber could be used to create various effects that can range from manipulation of the adversary's information to the temporary disruption of information systems, or even the definite destruction of a military weapon system. Of course, the potential offensive use of cyber operations shall only be possible in a legitimate NATO operation under international law, including under Article 5 (article 51 of the UN Charter). This would not differ from the use of any other military capability, like the employment of a jet fighter. To be clear, all of this does not change NATO's mission or mandate, which is defensive. We act

Offensive cyber could be used to create various effects that can range from manipulation of the adversary's information to the temporary disruption of his information systems...

in accordance with international law. We all stand to benefit from a more transparent and secure cyberspace.

Partnerships

All of our ambitions would be without a chance if we tried to advance alone. We place a high value in our partnerships with allies, partner-countries, and the EU. NATO and the EU both face a similar hybrid environment and cyber information sharing is essential. Another indispensable partner is the private sector. NATO requires access to the most innovative solutions to cyber challenges. We all know that innovation does not come from governments alone. Collaboration with academia and industry has to be fostered. We should pay particular attention to our ties with smaller and medium enterprises and create an environment where both parties benefit from a closer relationship. Examples of these partnerships are the NATO-Industry Cyber Platforms, a NATO-cyber incubator pilot, and nine Industry Partnership Agreements.

Concluding Remarks

NATO is facing a serious threat every day and we have shown in Warsaw that we take this threat seriously. The Cyber Defence Pledge and the recognition of cyberspace as a domain are two sides of the same coin. The Alliance is only as strong as it weakest link. Both NATO and the Allies have a role to play: it is to be resilient, to deter and if need be, to be able to defend ourselves in cyberspace.

Japan's Diplomatic Efforts in Promoting Cybersecurity

Mr. Atsushi Saito
Director, Cyber Policy Division, Foreign Policy Bureau, Ministry of Foreign Affairs of Japan

Until very recently, the Japanese government did not have a cyber security policy division. Given the growing concerns over cyber security, however, we created a new cyber security policy division within the Foreign Ministry, and I am assuming the Directorship. Accordingly, I would like to describe Japan's concept of the cyber environment, as well as our government's recent efforts in cyber security. Over the last two years when I began participating in this workshop, the cyber environment has been significantly deteriorating and every country has become more vulnerable. We have already discussed the recent threat in Ukraine, but in the Asian region there are many cyberattacks: in Vietnam in July, for example, we saw cyberattacks at airports. In Asian countries, the critical infrastructure has become a target of cyberattacks. Japan is not an exception to this new trend. We have not seen cyberattacks against our critical infrastructure, but in June the Japanese Travel Bureau, our country's best-known agency, became a victim with information stolen on 8 million customers. The Japanese pension service also lost data on 1.25 million people.

In June, the Japanese Travel Bureau was a cyberattack victim, with information stolen on 8 million customers. The Japanese pension service lost data on 1.25 million people.

Following the G20, the number of cyberattacks was said to actually be decreasing. However, this is not true because cyberattacks are simply becoming harder to detect. Therefore, it is important to carefully observe the development of cyber capabilities, not only within our countries but across the international community as well. Cyber threats continue to evolve in our region. At this stage, I would like to draw your attention to one specific issue concerning North Korea. As you know, with North Korea there is no transparency as to their cyber activities. Nonetheless, some sources attribute to the North Korea the attack on Sony pictures as well as the February attack on the Bangladesh central bank. In our region, the origin of cyberattacks is always very opaque and intentions are never clear. Sometimes North Korean conduct becomes even more proactive, especially concerning the test of nuclear bombs or test launches of ballistic missiles. Cyberattacks are now conducted in connection with some of these highly provocative actions. For such reasons, we must pay close attention to the development of the cyber sphere for North Korea.

Our three pillars consist of: promoting the rule of law in cyberspace; the promotion of confidence building measures within the ASEAN community; and the enhancement of capacity building measures.

Based on this situation, we are now conducting our own diplomatic efforts based on three pillars: first, promoting the rule of law in cyber space; second, the promotion of confidence building measures within the ASEAN community, third, the enhancement of the capacity building measures of our neighboring countries. Concerning the rule of law in cyber space, our emphasis is not on the

control or administration of cyberspace by states or authorities. Rather it has been to establish a rule to prevent intentionally wrongful acts in cyberspace, in conformity with universal values such as freedom and democracy. This is a very important point.

In preparation for this year's Group of Seven meeting, we want to address the cyber issue comprehensively in the Chairman's statement and in an annex document. In the annex document, we can confirm that international law, including the UN Charter, is applicable in cyberspace and also agree to promote a strategic framework for security in cyberspace. In this context, we confirmed the right of self-defense as recognized in Article 51 of the UN charter in accordance with international law. This is a strong and important message. In addition to this effort, and as Ambassador David Martinon has mentioned, Japan is a member of the GGE, the UN Group of Governmental Experts. While we are committed to this process of establishing the rule of law in cyberspace, we emphasize the importance of implementing already existing norms and principles and making them much more universal. Based on the 2013 GGE report, we can see that important progress has been achieved. While the applicability of international law is now generally agreed among all experts, there are difficulties in determining how to apply international law in cyberspace because this space is quite different from other domains such as land, air, and sea. Since it is not feasible to establish new internationally binding laws, we should deepen our understanding of how to apply international law in cyberspace. At the next GGE, we would like to concentrate on the issue of how to do this.

There are difficulties in determining how to apply international law in cyber space, since this space is quite different from other domains such as land, air, and sea.

In the ASEAN region, developing confidence building measures is also important since we have so many divergent capabilities and differences in the awareness of cyberspace. Accordingly, we are trying to establish a framework of dialogue with many countries, and especially within ASEAN. We are promoting outreach activities to these countries through the framework of the ASEAN regional forum and the ASEAN Japan Forum. We are especially promoting cooperation for capacity building in the region, which has not been well coordinated in the past. While various government entities have provided their own capacity building efforts, we have recently established a single policy for supporting capacity building in developing countries. We will try to strengthen this in the future.

Since we have so many divergent capabilities and differences in the awareness of cyberspace…we are promoting outreach activities through the framework of the ASEAN regional forum and the ASEAN Japan Forum.

These are our efforts in cybersecurity from a diplomatic perspective, and this year is important because we are conducting the GGE. Our priority should be to concentrate on the creation of norms for the responsibilities of states in collaboration with other like-minded countries. That is our hope.

Cyber Security as a National Priority in the United Kingdom

Mr. Conrad Prince
Cyber Security Ambassador, United Kingdom Defense and Security Organization

Our government's "National Cyber Security Strategy 2016 to 2021" was just published. It is built on three core pillars—defend, deter and develop—and is underpinned by a transformational investment of £1.9 billion over a five-year period. This more than doubles the previous £860 million five-year budget. A new National Cyber Security Centre has been established as a focal point with about 700 people who will work closely with GCHQ (Government Communications Headquarters) and subsume the CERT UK functions. The new strategy is intended to stimulate market forces that have led to insufficient cyber investments and are now being outpaced by technological change. Significant shortfalls in cyber-security skills need to be addressed as well. Key elements of the UK strategy are:

- *Public-private partnerships.* An international approach using public-private partnerships (PPPs) with the telecoms.
- *Security by default.* Moving toward systems that are "secure by default."
- *Protection of Critical National Infrastructure.* Since most Critical National Infrastructure (CNI) is owned by the private sector, solutions will be made available to the public on an "opt-out" basis.
- *Deterrence of cyberattacks.* As part of the need to "deter" cyberattacks, the UK is acknowledging that it has an offensive cyber program. The increased capacity that is being funded by the new cyber security strategy is needed to enable responses within international law.
- *Attribution of cyberattacks.* Building better ways to attribute cyberattacks is a priority.
- *Capacity building*. There is a global shortage of cybersecurity skills, and the UK needs to strengthen theirs. Large capacity increases are desired in all areas.
- *Education and training of digital workers, school children, and teachers.* All those who do digital work must understand and practice some form of security. This can be done by conveying more information on security to young children. We need to train teachers, as well.
- *Protection for the Internet of Things (IoT).* One hundred thousand internet-enabled cameras were the basis for the Dyn DNS attacks, indicating the growing power of the IoT. Suppliers need to be convinced of the need for security, but small companies say they don't have the time or expertise to provide it properly.
- *Unintended consequences of trade agreements and other cyber decisions* It is also important to consider the unintended consequences of cyber-related decisions, and the cyber provisions in trade treaties.
- *Cyber security as a national priority.* The UK wants to make cyber security a national priority next year, including the security of cars and other vehicles.

The Relationship with Russia—Searching for a New Approach: A Northern Perspective

Ambassador Michael Zilmer-Johns
Permanent Representative of Denmark to NATO

Since the Ukraine crisis in 2013, we have seen the relationship between Russia and NATO, Russia and the EU, and Russia and the West in general deteriorate significantly. We could have a long discussion about the causes for this deterioration, but this is unlikely to be constructive or to bring much new insight. It is preferable to look ahead and see how we can get beyond that unsatisfactory situation. From a NATO perspective, it seems that Russia still lives in, or has reintroduced, a world of old fashioned power politics—Realpolitk—as the Germans call it. It is a world where only national interest and geopolitics count, basically a world based on "zero-sum" calculations. This clashes with our understanding of a world characterized by complex interdependence and lots of potential "plus sum" games; a world where states and their fortunes are inextricably tied together; a world where the use of military force and coercive power in international relations has to a large extent been replaced by cooperation and mutual interest.

It seems that Russia still lives in…a world where only national interest and geopolitics count. This clashes with our understanding of a world characterized by complex interdependence…

This has proven not to be true, so we are faced with another situation. It is obvious that Russia and NATO both agree that it will not be possible, at least in the foreseeable future, to return to the level of trust and cooperation that existed before 2013. We cannot aim at business as usual, but as one of my colleagues once put it:

> "The present situation is dangerous business because we have tensions that can sort of suddenly run out of control. Unexpected, unintended crises can begin to grow and get a life for themselves and that could be very dangerous for the West and for Russia. Therefore, we must ask ourselves whether we are doomed to continue sliding down the negative spiral or if there is a possibility to reverse the trend."

I will look at this question from a Northern perspective and my Portuguese colleague will provide a Southern perspective. My country—the Kingdom of Denmark—is situated in the Baltic Sea Region, but with Greenland and the Faroe Islands we are also an Arctic and a North Atlantic country. This means that we are living with two very different relationships with Russia.

The Baltic Sea Region

In the Baltic Sea region, the relationship is one of competition and increasing tension. Large-scale Russian military exercises just next to the Baltic republics are causing concern, in particular because they are accompanied by harsh and aggressive political rhetoric. Denmark had its own dose of such rhetoric when the Russian ambassador threatened the use of nuclear weapons against our navy if we equipped frigates with radar systems that

can be used for ballistic missile defense. Finland and Sweden have received similar reactions to their domestic debates on membership in NATO. Rumors reported in the media this summer that nuclear-armed Iskander missiles may be deployed to Kaliningrad add to the tension. A strong increase in the number of Russian military flights in the region has also raised concern among civilian airlines and their customers. And at sea, both military and civilian ships from NATO countries have experienced Russian harassment.

Even in this climate of tension and distrust there are small glimmers of hope. In a special Baltic subcommittee of the international Civilian Aviation Organization (ICAO), it was possible to have a calm and realistic discussion that resulted in practical recommendations on the coexistence between military and civilian aircrafts in the region

The Arctic

In the Arctic, the relationship is very different. It has—largely—been possible to preserve the Arctic as a low-tension area and exclude it from repercussions from the overall deteriorating relations between Russia and the West. It has actually been possible for the Western Arctic powers, the US, Canada, Norway, and Denmark, to continue to cooperate (constructively) with Russia on issues like the environment or Search and Rescue.

It has largely been possible to preserve the Arctic as a low-tension area…and to cooperate constructively with Russia on issues like the environment.

This is all the more remarkable that the Arctic is undergoing a very dynamic development due to the climate change, which is causing all the Arctic powers to increase the level of economic activity and military presence in the region. Furthermore, there are unresolved territorial issues with overlapping claims on the continental shelf that could have given rise to tension. But here all the Arctic Powers have committed to solving these issues by peaceful negotiations on the basis of the UN Convention on the Law of the Sea. Of course, we are keeping an eye on the Russian military build-up—the reopening of old Soviet bases in the high North, the creation of an Arctic Brigade etc. But until now, we have not seen measures that indicate any Russian appetite for an arms race in the High North.

A Way Forward

In conclusion, if I had to answer the question: "Is it possible to reverse the trend" based only on the situation in the Baltic Sea region or the climate in the OSCE, it would be difficult to be optimistic. But looking also on the more constructive relationship in the Arctic, I still hope that it will be possible to reverse the trend, and slowly begin to rebuild a minimum level of trust and to reinvent some of the confidence-building measures that have been lost. Such a process would first and foremost require a genuine Russian buy-in. It would also require us to be more capable of identifying Russian strategic interests as well as our own in a harsh and competitive environment, to be more capable of predicting tactical moves from Russia and to engage Russian leadership and civil society at large.

The Relationship with Russia—Searching for a New Approach, A Southern Perspective

Ambassador Luis de Almeida Sampaio
Permanent Representative of Portugal to NATO

The Arc of Instability: A Test and an Opportunity

Let me start with public opinion perceptions. If you were to consult the Portuguese, Spanish, Italian, or French public opinion concerning the threats they perceive as the most clear and present dangers, I have no doubt that instability and threats coming from our close southern neighbors, terrorism, and the flux of migrants and refugees, would be included in their answers, at least as far as the Portuguese public opinion is concerned. But first and foremost, it would be terrorism, this sense of a very unpredictable threat that could strike at any time and anywhere in the very heart of our cities, as has happened in the very recent past.

This sense of instability, of living in a rather insecure world, poses a lot of challenges for us—NATO and European Union member nations—but also for Russia because these threats are also threats and challenges to Russia. And the fact that we reflect on the challenges stemming from that very close arc of instability is a common challenge but also a common opportunity for us to talk more and talk better. This will be a litmus test, because the arc of instability in the South is not going to disappear with the defeat of Daesh in the arc or in Syria. Terrorism will remain with us. The problems posed by the flux of migrants and refugees will be with us for decades. The potential for mischief and misunderstanding, but also the opportunity for better understanding between Russia and us will be with us for many years to come. It is with this very important strategic reflection that I would like to start. We should not look at the South as a region that will become more stable in two or three years from now because we all know that it is not going to be the case. The South poses huge economic, sociological, ideological, religious challenges that we will need to address in a rather strategic way, and we need Russia to do that. I would dare to say that Russia needs the West to do that as well. This is not necessarily an optimistic remark from my side. I am making it in order to underline this opportunity that we need to seriously reflect upon together. A lot will depend on Russia and a lot will depend on the NATO and EU member nations.

The potential for mischief and misunderstanding, but also the opportunity for better understanding between Russia and us, will be with us for many years to come.

The Defining Traits of a Major International Power Player

For my second reflection, which hopefully will prompt a debate around the table, I am referring to the fact that a lot will depend on Russia and Russia's behavior, because I fully understand that Russia wants to play a more important international role as is due for a country with Russia's history, demography, economic and military power. Russia is bound

to play a very important and crucial international role in years to come. But when I hear Russian friends telling me about how important Russia is, how decisive Russia's place is in the world, I always try to tell what in my mind defines a great nation, in a friendly way of course. What defines an important international actor in the 21st century is first and foremost the respect for and full abidance by international law and internationally agreed common behavior. This implies respecting internationally recognized borders. This means respecting the fundamental freedoms, including freedom of speech, freedom of meeting, freedom of the press, and full respect for human rights. In my mind that is the definition of a great power, a power that can say loud and clear, "we are a great power because we respect international law and we give an example to others that do not." It is in that sense that I see Russia playing a role as a major international actor. I am very much looking forward to that because I feel that we would be much better off with Russia playing a crucial and responsible international role, especially in light of the instability that I mentioned earlier coming from the South.[6]

What in my mind defines a great nation is first and foremost the respect for and full abidance by international law and internationally-agreed common behavior.

The Warsaw Summit Conclusions

My last reflection is connected to my two previous comments. We met in Warsaw during the summer for a very important NATO meeting and were surprised by the smooth way it went since it is not easy to strategize among 28, soon to be 29, democracies. The Summit was a success. One of the key decisions was that we should talk more and better with Russia because the more the misunderstandings, the more the need to talk. Of course, some will say, "this is meaningless talk, why talk when there are no results, why talk with low objectives?" I would argue that it is much better to talk than to do otherwise, even if that otherwise would only be to remain silent. So we decided to talk and we are convinced that our Russian friends are also willing to talk about our shared concerns, and we have a lot of shared concerns in in our Southern vicinity.

[6] Of course, when I speak about the South, to be totally clear, I am not talking about the Algarve or other parts of Portugal.

The Relationship Between Russia and the West: Searching for a New Approach

Ambassador Vladimir Chizhov
Permanent Representative of Russia to the EU

We are meeting at a time when volatility in the security situation in Europe has become the new norm. What started as a domestic crisis in Ukraine has developed into a full-scale Western policy of deterrence against Russia, backed up by economic sanctions, the cutoff of numerous channels of regular dialogue, and information warfare. Elements of a military bloc, whose collective defence spending outnumbers Russia's by a ratio of 17 to 1, have been deployed directly to my country's borders. I will not mince words. These actions are changing military reality on the ground. They are reducing political options for reengagement at a time when our common interests dictate that our nations stand together in tackling terrorism and instability in the Middle East and North Africa.

As a result of the ongoing NATO buildup in the Baltics, we will inevitably regard them as a potential military theater with its risks and threats.

Take the Baltics, which since the 1990s have been largely a militarily benign region—to the extent that back in 1999 they were even excluded for that reason from the area of application of the adapted CFE Treaty. Now, as a result of the ongoing NATO buildup, we will inevitably regard them as a potential military theater with its risks and threats. Consequently, our armed forces will need to adapt to decisions of the NATO Warsaw Summit regarding the so-called "continuous military presence" in the region. The same applies to other cases of NATO hyperactivity along our borders: a fourfold increase of NATO Baltic air patrols, forays of US cruise missile destroyers in the vicinity of Kaliningrad and Crimea or the largest NATO war games since 1989 "Anaconda-2016." This unprecedented militarization of the so-called "Eastern flank" is, in my view, hardly a cause for self-congratulatory assertions by NATO officials. Maybe some modesty would have been helpful because NATO actions basically confirm what we have been saying all along—that there is indeed an acute and systemic crisis of the European security architecture.

This leads me to my next point. The crisis did not start with Ukraine, just as NATO's military outstretch into its "Eastern flank" did not start with the Wales or Warsaw Summits. Its origins lie in the fateful decisions taken in the mid-90s that, in our view, favoured the eastward proliferation of NATO-centric security arrangements over a more concerted effort to construct an inclusive Euro-Atlantic security platform under the auspices of the OSCE. This process, while unhelpful on its own, was compounded by steps that have over time resulted in a significant erosion of the legal framework of European security.

The origins of the crisis lie in the fateful decisions taken in the mid-90s that favoured the eastward proliferation of NATO-centric security arrangements.

This year, for example, marked the activation of the American SM-3 missile and radar site in Romania. I think I don't need to remind you that it was back in 2002 when the US walked

out of the 1972 ABM Treaty and embarked on its controversial ballistic missile defence projects in Eastern Europe. Our attempts to convince our US partners to engage in this work together in a constructive spirit fell on deaf ears. The US kept substantiating its actions by citing the need to shield its European Allies from the "Iranian missile threat." By now, especially after the conclusion of the Iranian nuclear deal last year, these arguments have become as renowned as Colin Powell's famous vial of white powder. By the way, whenever I hear yet another media piece that speaks of "mounting evidence" against Russia, that vial is the first thing that comes to mind.

Likewise, when today NATO officials bemoan the absence of formidable arms control arrangements in Europe, they have only themselves to thank. It has after all been a concerted NATO position since 1999 to link the ratification of the adapted CFE Treaty to the resolution of protracted conflicts outside Russia's borders. Russia did ratify that treaty, by the way, and so did Belarus, Kazakhstan and Ukraine.

The list goes on. Numerous opportunities have been wasted. Just think of Russian ideas on OSCE reform, the European Security Treaty or, closer to the Russia-EU context, the Meseberg initiative. But the bottom line is this. Today the relationship between Russia and the West is increasingly held hostage by regional crises—first in Ukraine, now in Syria. But these differences should not obscure the underlying fundamental problem, namely the structural deficits of the European security architecture. Almost 30 years after the end of the Cold War, in spite of the absence of former ideological barricades, we continue to inhabit a continent of dividing lines, uneven levels of security and confrontational military planning. Mushrooming superiority complexes are, apparently, preventing some of us from hearing each other out and having faith, at least, in the reality of our interests and concerns. An "outlast" mentality is taking hold. Some are deluding themselves into thinking that the other side is on a waning path economically, demographically and politically, and that consequently time is working in their favour. As trust has plummeted, suppression of dissent and "witch hunts" for supposed Russian sympathizers are back in vogue.

Today, the relationship between Russia and the West is increasingly held hostage by regional crises—first in Ukraine, now in Syria.

These problems are political…they cannot be resolved through purely military decisions on enhancing one's own resilience or capabilities for force projection.

Make no mistake. These problems are political in nature. They cannot be resolved through purely military decisions on enhancing one's own resilience or capabilities for force projection. A negotiated political solution needs to be identified, which, in our view, should be based on international law, respect legitimate mutual interests and ensure the indivisibility of security for all states from Vancouver to Vladivostok in line with the 1999 Istanbul Charter for European Security. Either that or we may continue to "sleepwalk" towards new intended and unintended risks and challenges in our relations. This distinguished audience is well positioned (and hopefully well prepared) to manage the necessary wake-up call and shift our discussions from a pattern of mutual recriminations to a genuine and honest dialogue.

Why the Internal and External Aspects of Terrorism Are Increasingly Intertwined

Ambassador Miguel Aguirre de Carcer
Permanent Representative of Spain to NATO

Our panel on Daesh/ISIL deals with the terrorist threat. I would like to share three comments that are drawn from Spain's national experience.

First, terrorism from Daesh is, in my view, today's major global threat. No country or society can feel immune from it and the less prepared we are to confront this terrorism in any country, the greater the risk of being targeted.

Second, in order to confront Daesh's terrorism, we need to employ a myriad of tools and instruments. We require intelligence analysis tools, policing tools, adequate legal frameworks, financial surveillance mechanisms, knowledge and insights of the communities from where Daesh terrorists are drawn from, social media surveillance, political understanding and awareness of the phenomenon, military capabilities etc. So this vast array of actions obliges our state structures to maintain an extremely close coordination and I would say that countries with insufficient internal coordination will allow terrorist networks, cells, or individuals, to take advantage of these gaps.

We require intelligence analysis tools, policing tools, legal frameworks, financial surveillance mechanisms, knowledge and insights of the communities from which Daesh terrorists are drawn.

Third, in my view, international cooperation is more important than ever to fight against terrorism. All those tools and instruments I mentioned above also have an external dimension and today, both internal and external dimensions of terrorism are completely intertwined. In order to be effective, it is crucial to have close cooperation with other relevant countries to obtain the necessary information, to be able to act early on and to prevent an attack from occurring. And here again, as with internal coordination, without effective international cooperation, terrorists, network cells, or individuals will clearly take advantage of the perceived gaps. Whether we are thinking in terms of the open borders of the Schengen area, the borderless extent of the Sahel region, or the problems of effective border controls in many other regions, we must be aware that the times of closing out any country from the rest of its neighbors are forever gone. Possibly the current greatest challenge is the conflict in Syria. Without effective cooperation among all countries concerned, it will remain very difficult to prevent Daesh from using the Syrian conflict to its own advantage.

It is crucial to have close cooperation with other relevant countries to obtain the necessary information, …to act early on, and to prevent an attack.

To summarize:

- Daesh/ISIL is a major global threat and no country should believe that terrorism is somebody else's problem. This mistake might turn out to be very painful for their societies.
- Terrorism must be confronted with multiple and closely coordinated internal tools and instruments because terrorists will exploit gaps and deficiencies.
- Daesh's terrorism takes place in a globalized world and it is essential to strengthen an effective international cooperation to defeat it.

Facing an Enduring Threat of Extremist Salafi-Jihadist Regional And Global Violence

Mr. Pjer Šimunović
Director, Office of the National Security Council of the Republic of Croatia
Former Ambassador to Israel

While the territory controlled by *Daesh* contracts and its manpower and resources are depleted, the 'Caliphate now' narrative is losing ground. Yet there seems to be no end in sight for the extremist Salafi-Jihadism in general, spreading militancy, violence and terrorism. With the fight most likely shifting back underground, *Daesh* and *Daesh*-inspired terrorism presents an immediate danger both in the region and globally. In the continuously shifting sands of the Middle East and amid this orgy of violence, a new power vacuum is in the making with bitter rivals racing to fill it.

Daesh 'Down but Not Out'

After an initial strategic surprise created by *Daesh's* arrival on the international scene and its rapid conquest of territories in Iraq, Syria, and Afghanistan (the Islamic State of Khorasan), the Islamic State's expansion was not only stopped but also reversed as a result of a successful offensive by internal and external actors converging on the key extremist nodes of Mosul and Raqqa. *Daesh*'s manpower and war *materiel* are now reduced, limiting the organization's options for holding and running the conquered territory. According to experts, over the past 18 months *Daesh* may have lost over one-third of its fighting force from roughly 25,000 to 15,000 men, with the monthly rate of incoming foreign fighters declining from 2,000 to 200. The organization's assets and finances are depleted, with limited options for re-supply; oil income is estimated to have been cut in half to $250-$350 million in 2016 from $600-$700 million in 2015 (oil income represented half of *Daesh's* income in 2015). Salaries for fighters and soldiers have been cut down, while the critical leadership is getting eliminated (such as Abu Mohammad al-Adnani, spokesman and a key field commander, who was killed last August). As a result, life under *Daesh* is becoming extraordinarily difficult, exacerbating repression and poverty, leading to a drastic rise in taxation to make up for the loss of oil income, increasing the likelihood of population dissent, and impacting upon *Daesh*'s recruitment and overall hold on power. *Daesh* is self-destructively too extreme, ultimately generating too many enemies.

Simply facing too many enemies, Daesh is self-destructing… The question is, "What will become of the current Daesh, or what will replace it or merge with it, taking the banner of extremist Jihadism?"

However, while *Daesh* may be 'down', it cannot be counted 'out' yet. If nothing else, it demonstrates a grim determination to fight all the way to an apocalyptic end. With a 'Caliphate now' narrative losing ground literally, together with its credibility and appeal, depriving *Daesh* of its most concrete promise to its followers, and of its most distinctive feature within the global jihadi movement, the question is, 'What will become of the current

Daesh, or what will replace it or merge with it, taking the banner of extremist jihadism?' Anyhow, there is no end of violence in sight—with the existing, critical level of militancy, hatred and upheaval, the fight will go on, in all likelihood reverting back to the underground, in a more fluid form, to *guerrilla* warfare and terrorism, and also surviving in a well-developed digital domain.

Within the violent jihadism universe, *Al-Qaeda* and the *Taliban* may have a more enduring presence because they are either not running the risk of holding and governing a concrete, high-value and ultimately vulnerable state-like territory, remaining instead a harder-to-hit, fluid, terror network (*Al-Qaeda*), or they are having some inherent territorial and specific ethnic, Pashtu roots (the *Taliban*). Unique circumstances created a 'perfect storm' for *Daesh,* an opportunistic outgrowth, to come into being. *Daesh's* sensational upward trajectory was made possible when the global jihad landed on the fertile ground of the fragmented wastelands and devastated cities and villages of Syria and Iraq, cracked wide open by the preceding wars and other ongoing conflicts.

Daesh's sensational trajectory and its zenith are now passed. Amid the violence and bloodshed that opposes bitter political and religious rivals, a new power vacuum is in the making.

This latest turn of events has multiple implications. In the Middle East region itself—amid the violence and bloodshed that opposes bitter political and religious rivals, a new power vacuum is in the making. It has started a race for survival and supremacy between different factions that are eager to fill the space liberated from *Daesh* territorially and politically. Calm is therefore unlikely to return any time soon. The conflict keeps shifting *tous azimuts*, depending upon the time and place: Sunnis *vs* Shi'ites, Sunnis *vs* Sunnis, Shi'ites *vs* Shi'ites, regional and outside powers with their local allies *vs* different inside forces. As a predictable consequence of these developments, *Daesh* is seeking to prove its continuing relevance by conducting high-profile terrorist attacks in the region and globally that are either *Daesh*-run or *Daesh*-inspired. A high level of threat is also stemming from returning foreign fighters who can conduct direct actions back home or in other countries, and engage in spreading radicalization and recruitment among local Muslim populations and recent immigrants. The number of foreign fighters is disturbing: if we single out as an example the Western Balkans region, (Bosnia-Herzegovina, Serbia, Macedonia, Kosovo, Montenegro, Albania) which is not the largest contributor, around 1,000 people have joined *Daesh* and other Islamic extremist groups, mainly in Syria, since 2012; some 350 have returned, with around 400 still remaining in the Middle East.

There is another distinct danger to watch. Faced with reversals on the battlefield, *Daesh* has been trying to make up for the manpower losses by increasingly recruiting children for combat activities, including for terrorist suicide attacks. There are about 4,000 children-soldiers currently in Iraq and Syria, and their number is on the rise. The children are exposed to a systematic extremist Islamist brainwashing from a very young age. *Daesh*'s 'education' serves as a voluntary and forced vector of radicalization and recruitment. Families are also sacrificing children for a desperate economic gain. This early and profound

brutalization inflicts a lasting and fundamental injury to a person, and in the longer term creates a most serious human and security challenge.

'A War of Ideas, Bombs and Binary Codes'

The world's response to the threats *Daesh* and other violent jihadi organizations should aim to counter both the motivation of terrorism and its operational capability. To begin with, it is imperative to understand the nature of the threat as it gets proclaimed and materialized by itself: extremist Salafi-Jihadism, by the most violent means available, seeks global supremacy and the replacement of any other Islamic, Western or other influence with its most rigid, totalitarian Caliphate. A multi-dimensional counter-terrorism effort should keep hitting the conceptual and material centres of gravity of this threat, including its vectors of transmission, in 'a war of ideas, bombs and binary codes'.

The Muslim community must take the lead in this effort and be backed by a wider support. At stake is the extremists' ability to control territory, to finance, support and conduct operations and terrorism.

Extremists' ideology needs to be targeted, their willingness to use and justify the use of violence, and their ability to attract and recruit. The Muslim community must take the lead in this effort, backed by a wider support. What needs to be targeted is the extremists' ability to control territory, and to finance, support and conduct operations and terrorism. Their ability to exploit our vulnerabilities must be neutralized. To do this requires a seamless use of offense/defense and building up strong resilience; having in place all necessary national and international resources at our disposal to use in a joint, simultaneous, well-proportioned and judicious way. This encompasses the police, military, intelligence, diplomacy, judiciary, education, development and public relations domains. It is a sensitive balancing act among security, practicality, legality and the morality of our action. Finally, our action would be far more efficient without an unfortunate structural deficiency consisting of conflicting interests and mutual mistrust among the various regional and global actors.

DAESH/ISIS—Dealing with the Spreading Threat

Ambassador Fatih Ceylan
Permanent Representative of Turkey to NATO

It is fascinating to see at this workshop such a diversity of backgrounds and perspectives. Yet I believe we all share the same ultimate goal for our countries: security, stability and prosperity for all. These three fundamental ambitions, however, have been hampered by DAESH, a quotidian plague in the world. To borrow a math term, DAESH represents a *negative exponent* in our times. In order to have the right exponent, we must first turn the numbers "upside down" to understand the root causes of DAESH and address them. All of us have different means to attain that goal. In order to give you Turkey's perspective—the perspective of a country that is not only inside the region but has been exposed to various kinds and forms of terrorism for many years, I will:

- First, look at the root causes, i.e., the developments in the Middle East and North Africa that are related to the DAESH spillover.
- Second, focus on the measures and steps Turkey has been taking in order to help degrade and destroy DAESH.
- Last, briefly talk about what the next steps could be and the potential role that NATO could play.

The Root Causes

Turkey stands at the forefront of NATO's southeastern border in facing DAESH—a threat that tests our resolve, solidarity, and resilience. Beyond Turkey's borders lies an immense source of instability with a succession of conflicts affecting all of us negatively. That is also DAESH's place of birth. Philosophers say that life must be understood backwards. Before doing that, let me clarify an important issue: different terms are needed to analyze what DAESH means and its implications for the region, for Europe, and for the world at large. When we use these terms, we must be very familiar with the background because there are different interpretations of what certain words mean. I will take Jihad as an example. DAESH terrorists interpret Jihad in one way, but other Muslims interpret it in a completely opposite way. Jihad is not to invade and kill others, it is intended to invade your own soul to avoid excesses in your own life and submit yourself to God. This is our interpretation of Jihad, but DAESH's interpretation of Islam is totally wrong and must be addressed effectively, first and foremost by Muslims and also in cooperation with other communities and societies.

DAESH terrorists interpret Jihad in one way but other Muslims interpret it in a completely opposite way. Jihad is not to invade and kill others, it is intended to invade your own soul to avoid excesses in your own life and submit yourself to God.

Now, what are the developments in the Middle East and North Africa? Failed and failing states, beleaguered and oppressed societies, alienated communities that have been replaced by state-like terrorist entities and unpleasant regimes have created a vacuum in the Middle

East and North Africa Region (MENA). Meanwhile, sectarian policies stretching from Iraq to Syria and championed by revisionist actors are adversely impacting the socio-political strata in the region that were still intact.

Syria. In Syria, the Assad regime, in its desperate drive to retain power at all costs created a significant breeding ground for DAESH. The rise of DAESH in Syria needs to be well studied. As evidence emerges about it, the regime started in 2012 to release extremists from prison to deliberately subvert a peaceful uprising and exacerbate radicalism in order to make itself the lesser evil for the international community and Syrians alike. Here, let me emphasize one point. In 2011, the number of DAESH militants was around 400 to 500 men, but in a matter of 4 years, it was estimated that over 27,000 foreign fighters had travelled to Iraq and Syria. Without giving up our efforts to defeat DAESH, it is critically important to have a political solution—the sooner the better—on the basis of the Geneva Communiqué and to reinstate stability and security in Syria. For us, the protection of the territorial integrity of Syria, the establishment of a multicultural secular and democratic structure and the prevention of sectarian and divisive policies are a must. We are trying to build up on this.

For Turkey, the protection of the territorial integrity of Syria, the establishment of a multicultural secular and democratic structure and the prevention of sectarian and divisive policies are a must.

Aleppo. What is happening in Aleppo? Aleppo has a long history of peaceful coexistence among different religions, ethnicities and cultures. Now, the city is desperately seeking a respite from its suffering: tens of thousands of innocent people have been besieged by the regime and its supporters and the city has been brought to the brink of total destruction. It is not only the civilians that are being bombed, maimed, starved or forced to displace. The moderate, peaceful and pluralistic future of Syria is also being targeted and, in this case, standing by is just letting radicalism, extremism, hatred and militancy take root. If Aleppo falls, there will be many repercussions. We will no longer be able to speak about a multicultural or non-sectarian Syria. The worst outcome will be our total loss of credibility. The more we stand idle against the spread of horror by the Syrian regime and its supporters in cities like Aleppo, the less chances we will have to defeat terrorists like DAESH since the destruction of the peaceful coexistence is their breeding ground.

Mosul. Mosul is another microcosm of the region. The Mosul operation should serve as a bridging factor, not the other way around, which will trigger sectarian clashes and stiffen DAESH resistance. If this balance is not established during the liberation of Mosul, it will not be possible to establish it afterwards. There is still no political consensus on how Mosul will be governed after the operation. Unless the framework of a compromise is put in place fairly soon, establishing order will be very difficult. An inclusive and representative governance, based on the constitutional principles of power and revenue sharing, should be the cornerstone of such a political agenda. The Mosul operation should continue to ensure that DAESH and other extremists will not find it a fertile ground to exploit in the future.

Iraq. What is the situation in Iraq? This country has been continuously in crisis for years. DAESH is just the latest episode in this drama and probably the most complicated one. Iraq was plunged into crisis simply because of the sectarian and oppressive policies of the previous government. This means that either we will reach out to these oppressed people and regain their trust and confidence or we will lose them to DAESH. It is again the international community's duty to remind the Iraqi government that it needs to do more for winning the "hearts and minds of every segment of the Iraqi society." Turkey will keep to provide political, military and humanitarian support to Iraq and is ready to increase it if Iraq so wishes.

In Iraq, either we will reach out to these oppressed people and regain their trust and confidence or we will lose them to DAESH.

Libya, Yemen, Egypt. Finally, we should not lose sight of the risks and challenges posed by the developments in Libya, Yemen and Egypt, as well as in the Sahel region and Somalia in terms of creating fertile grounds for DAESH. Libya still risks to be a springboard for further DAESH expansion in North Africa. The Libyan Political Agreement (LPA) must be fully implemented and a Libyan-led and Libyan-owned process is a must. The Libyan Government of National Accord (GNA) in general, and the Presidential Council in particular, should be duly assisted.

Turkey's Steps to Help Degrade and Destroy DAESH

I will briefly touch upon what we have been doing so far in this battle against DAESH. We strongly support the Coalition of which Turkey has been a member from the beginning. Actions speak louder than words of course: we granted thousands of over-flight permissions and opened our bases for Coalition aircraft. We co-chaired the Coalition's sub-working groups. We contributed militarily to the Coalition operations. We provided humanitarian support for stabilizing efforts. In fact, outlining each and every aspect of Turkey's contributions to fight DAESH could easily be another topic for a possible future meeting. I will just give two striking examples:

On the humanitarian side. In addition to the ruthless deeds of the Syrian regime, the current terror cycle has caused refugees to amass in and around Turkey. We are now hosting over 3 million people from Syria and Iraq combined. Our official expenditures have exceeded 12 billion dollars. If you combine this with unofficial expenditures, you reach the figure of 20 to 25 billion dollars so far, whereas we have only received 400 million dollars worth of support from the international community. Some of these Syrian and Iraqi refugees fled DAESH as well as YPG terrorism in Syria. We did not discriminate amongst them when opening our doors. Being Arab, Kurd, Turkoman, Yezidi, Christian, Assyrian, Sunni or Shia makes no difference for Turkey, which is doing its best to help them.

On the military and security side. The moderate Syrian opposition has seized the northern Syrian town of Dabiq with the backing of the Turkish Armed Forces. Dabiq was considered central to DAESH's propaganda, which locates the town as the place of Armageddon where the infidels (non Muslims) will be defeated. In fact, Operation Euphrates Shield has pushed

DAESH away from the positions they control along our borders. So far, a 98 km stretch of our borders from Azaz to Jarablus has been sealed off and we have cleared over 1,300 square kilometers from DAESH. Euphrates Shield has also created a strong momentum to put DAESH on the defensive elsewhere in Syria, like in Raqqa and Al Bab. We are determined to continue the destruction of DAESH and other terrorist targets in our vicinity.

We are also doing our part to stop the flow of foreign terrorist fighters and have taken all necessary measures. We have set up a no-entry list of 12,800 people and deported 1,300 people in this context. On the other hand, there is no scarcity of terrorist organizations at our periphery. DAESH, PKK and its affiliate YPG in Syria continue to impose their sick and archaic agendas and ideology by perpetrating indiscriminate bombings, ethnic cleansing and intimidation. We are obviously taking the necessary measures and believe it is our right to expect from the international community the same care and attention against these violent extremists. In view of the plethora of crises in the region, Turkey has always displayed proactive engagement and advocated the need to build inclusive societies as a way of defeating sectarianism and terrorism of all kinds. On the bright side, since it is the duty of a diplomat to be optimistic, Tunisia has made a remarkable stride towards democracy. This must certainly be supported.

Is There a Role for NATO in this Struggle?

Let's not forget that NATO's Afghanistan operation was launched following a terrorist attack against an ally. While maintaining a stronger collective defense with a 360 degree-approach for its members, the Alliance can and should leverage its toolkit for adapted crisis management and conflict prevention efforts as a way to project stability and build resilience in NATO's neighborhood. NATO's motto has always been "solidarity and indivisibility of security." Now is the time to demonstrate this against terrorism. To attain this goal, NATO needs a modern and visionary approach against terrorism that is faster, flexible, adaptable, scalable and affordable. This will require developing a more robust NATO in defense and related capacity building, enhanced readiness, early warning and indications, strategic communications, with synergies between and among political, economic and military courses of action. Intelligence and information sharing is also a *sine quo non*.

Turkey is not merely at the frontline of this full-fledged instability and insecurity; it represents the last stronghold, particularly for the rest of Europe.

To sum up, it should be clear to everyone that Turkey is not solely at the frontline of this full-fledged instability and insecurity; it represents the last stronghold, particularly for the rest of Europe. Eliminating DAESH is not an issue Turkey can solve on its own. We need more international cooperation. All in all, DAESH must be defeated on the ground. Yet, removing the root causes of the problem must not be deferred or overlooked. Illegitimate regimes, sectarian governments, or terrorists like DAESH, PKK, and aaits affiliates or Hezbollah cannot be remedies. The genuine support of the peoples of the region must be obtained. This is what will allow us to prevail over the forces of terror and eradicate DAESH.

Europe Needs to Toughen Up on its Saudi Ally and on Iran, Too

Ms. Marietje Schaake
Member of the European Parliament

We meet on a very interesting week and a very interesting day—the presidential election in the US—where politics, the consequences of a lack of trust, and the emergence of new voices and forces on the political stage could quickly change almost everything we have been talking about and our whole perspective. This brings to mind the impact of these new political forces including the anti-terror legislation as well as the risk of what I would call "do something politics." I will focus on this because this sort of "knee-jerk reaction" that we often see in light of the very serious threat of terrorism is something to be careful about. There has been a preference to look at what impact technology has instead of looking at the offline reality, focusing on the short-term rather than the long-term, looking at what is domestically important instead of looking at foreign policy and the global perspective, and focusing on the immediate security impact instead of the long-term fundamental freedoms. So I think it is time to connect the dots and when we look at the confrontation with Daesh, or the so-called Islamic State, a lot of these challenges are actually exposed in Europe. It is crucial to ensure that we protect, safeguard and make our open societies more resilient and not only defend ourselves, our people, our values against attacks from the outside but also from an erosion from within.

In the US presidential election, politics, the consequences of a lack of trust, and the emergence of new voices and forces on the political stage could quickly change …our whole perspective.

The whole question of terrorism— a global phenomenon like Daesh and the so-called Islamic State—hit home for us in European institutions when we found out with relief that our staff had made it to work safely on the Brussels subway after the attacks and our colleagues had been largely spared from the devastating violence at Brussels airport. The terrorists had used encryption and bought their guns on the internet or the dark web. The initial responses, calling for breaking the encryption or hacking back to catch the terrorists, have proven to be shortsighted. Efforts by the government were at the expense of actual security and, although I know that cybersecurity has been discussed a lot at the workshop, we should be careful about giving it too much attention. These efforts have also led to focus away from the need to invest in human intelligence and knowledge about phenomena that may, in the long and short-term, threaten our open societies. Simplifying profiling in minority communities also risks eroding the trust of the very people that law-enforcement authorities need to get help from. Of course, we learned later that the simple ordering of a large number of pizzas through a landline revealed more than any encrypted app could have concealed. So, instead of mass surveillance, which is never proportionate, we should think about what good and up-to-date intelligence can do and this should go hand-in-hand with the appropriate democratic and judicial oversight.

Instead of mass surveillance, we should think about what good and up-to-date intelligence can do and this should go hand-in-hand with the appropriate democratic and judicial oversight.

Last week, in response to parliamentary questions, my party leader asked the Dutch parliament about a Jihadist who was able to travel from the Netherlands back to Syria for the second time, even after having been caught and registered. The government's answer was that at the time when this individual was traveling and at the time when the high alert had come, the phone lines had coincidentally gone down, which supposedly explained why the government had not intervened. Over the weekend, Belgium chose to expel an Imam because he had incited hatred and decided that he could just be brought to the Netherlands. With the threat of everyday terrorism, this "pass the buck" approach or not even having the most basic infrastructure in order is actually quite shocking. It really erodes the trust that the people have in government and law enforcement authorities and does not help stem the fear that people have and that is exploited. Trust is not only a problem between people and government, but also between states. It is certainly lacking in Europe and we discovered it after a French suspect in a terror attack was able to travel to Belgium with hardly any sharing of intelligence. We observe the same attitude of moving the problem across borders when we see the lack of common border protection and the absence of shared responsibility or solidarity when it comes to registering and sheltering refugees and asylum seekers. I recall the Prime Minister of my country, the Netherlands, saying years ago when the first refugees were drowning and arriving in Italy, "Tough luck for Lampedusa being located where it is. It is not our problem." But of course we are only as strong as our weakest link. We are incredibly mutually dependent and need to start acting in that direction too.

Trust is not only a problem between people and government, but also between states. It is certainly lacking in Europe.

Regarding the question of domestic and foreign policy, some of you have talked about the fact that the lines are blurring and I could not agree more. I also think that for a long time European governments collectively and societies as well have been a little bit too naïve. The approach to immigrant communities and the hope that they would quickly find their place in our societies through social upward mobility did not always work as planned. Ignoring social economic challenges was actually a big mistake and it has created an environment in which people who experience challenges at home can be too easily recruited and exploited by people with criminal track records. When we ignored problems, others quickly jumped into the vacuum. The recruiting also happened through religious institutions and mosques as well as in after-school programs where a lot of financing has been coming from abroad with very little public debate and scrutiny. I think that we are now paying a price for this. It would have been a perfectly reasonable question to ask why foreign governments or individuals from countries such as Saudi Arabia were spending this kind of money to export their very conservative and potentially very impactful ideology to Europe and elsewhere. People who become radicalized and violent are actually the exception but, given the grave impact of their actions, we should look at the worst-case scenario. I think that there is also some confusion in the debate about what risks and developments are going on in our societies. Of course, we must respect freedom of

The approach to immigrant communities and the hope that they would quickly find their place in our societies through social upward mobility did not always work as planned.

expression, freedom of religion, but we should also feel free and equipped to address the impact of the different strands of the political Islam's agenda. When Islam moves from an individual matter of belief and conviction to a political agenda, it can be challenged in the political arena, but I see a sort of hesitation, sometimes confusion and lack of confidence by mainstream political parties in addressing some of these political agendas. In my own party, we might find it easier to address the agenda of conservative or ultra-conservative Christian parties where, for example, there is one in the Netherlands that does not allow women to serve in public office, but we would have a harder time addressing the agendas of people who base their views on the Koran or at least claim to do so. Of course, it is not about banning ideas. I am a firm believer in maximum freedom of expression and having a very open debate, but we must have an open and well-informed debate, and transparency about what is at stake. That includes working with communities to address their role and place as part of open societies. It should not be solely a question of whether parts of expression should be banned or not banned. So often, when politicians address questions of diversity, integration, Islam in the West, the question will be: are you proposing to ban this or that? Are you proposing to ban the burka? Are you proposing to ban an azan—a cult of prayer being called out loud by mosques—etc. We should not reduce this discussion to what should be banned and not banned, to legislate or not to legislate. We should have a much more open discussion, ensure that it is inclusive and that we talk with the people, not just about them. This is because, unfortunately, the notion of exclusion from the debates and the inevitable exclusion of societies is a fertile ground for recruitment. So doing the right thing to protect the open society but sticking to principles is key.

I am a firm believer in maximum freedom of expression and having a very open debate but we must have an open and well-informed debate, and transparency about what is at stake.

The same goes for our role on the global stage. Syria is a key issue and one of the most difficult issues for me to deal with, having been in a position of responsibility without being able to do much about this problem. It is a huge embarrassment and a disgrace for the EU and international community to see this war getting to where it is and having made so many victims. The European Union and others in the international community left a vacuum that was quickly filled by others. Lack of action on the ground has led to immense suffering and has also led to the recruitment by extremist radical Jihadist groups of people who were desperate after having lost half of their family and feeling that nobody cared. I do think we have to address the role of the Assad regime in fueling extremist groups in order to create more legitimacy for its government, and the unfortunate fact that too many countries in the international community are stepping into this frame. As a consequence, I am afraid that we have less of a role model on the ground but also at the negotiating table and I think that this must change. I am encouraged by the fact that EU High Representative Federica Mogherini has now spoken to both Saudi Arabia and the Islamic Republic of Iran. I do believe that the EU should have more of an even hand or balanced approach with these major players in the region and that, where sponsoring of terrorism occurs or where repression of human rights occurs, we must act even-handedly.

The EU needs a clear strategy toward Syria and, more broadly, a much stronger Common and Foreign Security Policy. It is baffling that, considering the grave crisis that the Syrian war has also had in Europe, EU member states still do not have a common position vis-à-vis Syria. I find that very difficult to understand. Of course, the Common Foreign and Security Policy's hard power should only be a last resort, but I do not think we should treat soft power as second tier, as an after thought, or as the byline of what we should be doing because we pay the price in the long term. We have seen years of budget cuts to international media programs right at a time when propaganda is hitting Europe harder than it has for a long time; we have seen budget cuts in our defense spending without member states seeking an approach for a more common defense which could be much more effective with relatively fewer resources; and we are seeing a compromise on human rights—a central tenet of our policies—by European governments eager to manage migration and create an anti-terror policy that will protect their interests. I think this is a real problem when a young generation of people growing up in the Middle East and North Africa sees that Europe is not standing up for their rights while it claims at the same time that these rights are universal. Last, I think the EU should get out of its mode of just being in crisis management and look at where the next threats could emerge. The EU could, for instance, engage with states like Indonesia or Nigeria, but also be more involved in aspects of transition, international law and justice. If we want to have an even-handed and principle-based long-term approach where we can be credible, this is the only way. I am afraid that right now, Europe runs the risk of letting the long-term perspective be completely overshadowed by short-term interests and this could fatally undermine its effectiveness and credibility on the global stage. This would very much affect the way we deal with terrorism coming from Daesh with consequences that would be felt much more broadly.

This is a real problem when a young generation of people growing up in the Middle East and North Africa sees that Europe is not standing up for their rights while it claims at the same time that these rights are universal.

Opportunities for Terrorism in Cyberspace

General Marc Watin-Augouard
Founder of the Forum International de la Cyber Security (FIC);
Director, Center for Research, Officer School of the Gendarmerie Nationale

The relationship between terrorism and cyberspace is drawing attention because of Daesh, but this kind of terrorism began years ago—not only in France but in other countries, too. During the 1980s, terrorism was already very serious in France. We saw hostage taking, selective murders which were actually assassinations, aircraft hijackings, and bombs in the metro and in the public transportation system. At that time, however, terrorism was conducted in what we might call the "real world."

When the digital space began to develop, we wondered whether terrorists would be active in this new space of potential conflict, just as they had been in the spaces of land, air and sea. At least in France, the first question that we asked was whether terrorists would be able to penetrate our vital systems. Would they be able to damage them, modify their functions, or steal data? Would they act with the intent of causing grave public harm, intimidation, spreading terror, or simply creating so much disorder that it would amount to a veritable chaos? One could imagine such attacks on SCADA systems, the systems of command and control that permit the functioning of most of our industrial systems including our critical infrastructure.

As of now, we have not actually attributed a cyber attack to a terrorist group in France. The question we have asked is whether Daesh would use cyberspace for its own purposes, for administrative requirements, political purposes, or financial purposes. In fact, we have already seen a certain number of attacks where the terrorists used cyberspace to transmit information, orders, and instructions, or to finance their activities. On several occasions, we have seen that counterfeiting has been used to finance terrorist movements. Thanks to the internet, counterfeiting for the financing of terrorism is increasing.

We have seen a third way of utilizing cyber space: to influence global public opinion—with images of decapitations, women being raped, and a Jordanian pilot burned alive.

Recently, we have seen a third way of utilizing cyber space: to influence global public opinion with images of decapitations, women being raped, and a Jordanian pilot burned alive. The internet is now extremely well developed, with an enormous number of connected computers across the world—more than 10 billion. Daesh is able to exploit the internet for terrorism and it has become its most powerful and effective tool. This was a revelation for us after the Paris attacks on 13 January 2015 when 19,000 websites of towns, municipalities, and government offices were defaced. Their home pages were modified and replaced with Daesh messages. While it is not certain that Daesh was actually behind all of this and even though the defacing of home pages is not necessarily a proof, it is clear that we have seen a powerful utilization of cyberspace for communication, propaganda, and inciting terrorism.

In France, one of our first questions was whether these attacks were covered by the laws covering liberty of expression and freedom of the press. It was a real debate, because press law is a very old and important one that protects not only journalists but victims as well, and it seeks to achieve an appropriate balance for a procedure that is different from that of common law. The first measure taken in France was to say that expressions of terrorism were not a matter of free speech or freedom of the press but of combat and war. The second measure was to place under criminal law any provocation, apology or defense of terrorism. Also, such provocations or apologies, even in a non-public space, are covered by the law. In addition, we have criminalized the behavior of all those who create, possess, export, or alter content for terrorist purposes.

Our first question was whether terrorist attacks were covered by the laws covering liberty of expression and freedom of the press.

The third measure concerns individuals who do not incite terrorism but, instead, may habitually consult terrorist sites. It is not an issue of criminalizing someone who might consult such a site on a single occasion but rather someone who does so frequently. In this case, the French position was originally quite divided. In 2014, the initial decision was to say "no," we will not actually criminalize such consultations—but the fact of habitually consulting a terrorist site could be considered as one of the material elements that would be used to define a terrorist, notably an individual terrorist, or "lone wolf" who acts by himself. In the face of the enormous harm caused by terrorists, France decided on 3 June 2016 to actually criminalize the habitual consultation of a terrorist site.

In the face of the enormous harm caused by terrorists, France decided on 3 June 2016 to actually criminalize the habitual consultation of a terrorist site.

In this way, both the production and utilization of terrorist materials are now considered to be criminal activities. These are important steps because they have given necessary tools to our authorities, but nonetheless we can see very quickly that there are limits to their effectiveness. This is because the fight against cyber criminality, in other countries as well as in ours, must face two obstacles: the first challenge is attribution—who is actually behind a cyber attack? We all know that this can be extremely difficult, partly because the attackers use widely-known means or groups to attack you. This makes it necessary to trace back not only to the source of the attack, but to find who is behind the attack. With this level of difficulty, in order to effectively fight against cyber crime, you need to be more than one, you need an international effort.

The November 2001 convention of the European Council of Budapest on the fight against cyber criminals has only been ratified by 49 countries.

An international convention that is extremely restrictive concerning the fight against cyber criminals is the November 2001 Convention on Cybercrime of the Council of Europe, known as the Budapest Convention, which has only been ratified by 49 countries. Of course, African countries have signed the Malabo Convention on Cyber Security. Nonetheless, we are

confronted with problems that are diplomatic as well as technical, because we can only deal with countries that agree to cooperate.

Finally, we are now trying to work "upstream" before the actions are committed, which means moving from the judicial world to the world of prevention. In France, we voted a law concerning intelligence in July 2015. It legalizes the actions of the intelligence community, which were completely hidden until now. We have given administrative authority and responsibility, which is not under the control of a judge, but is covered *a posteriori* by the control of an administrative judge. This includes a shift of our efforts "upstream" including algorithms placed with the suppliers, which detect weak signals and meta-information.

I don't want to embarrass our American friends, but speaking of the Snowden affair, we are told that we are doing in France exactly the same things that our American friends have done—namely that we are creating a true mass surveillance system, which will certainly present problems. We cannot rely exclusively on our intelligence services, it can only be done together with private actors, making it necessary to work with Apple, Amazon, Facebook, and others—developers, internet service providers, and website hosts. It is a common challenge, so let us share it. It is important for international security, but it is also important for the credibility of industry. Perhaps you will be criticized tomorrow for doing business at the expense of innocent people by accepting information that they provide. The work that must be done today is to dereference, remove, and block harmful content. This exercise is not always simple, as we know from confronting pedophilia content: fortunately, images of pedophilia speak for themselves and they are easy to recognize. But consider an image of the Bataclan, the site of a horrible terrorist attack, which was spread widely—only the image by itself and without commentary. Was this a provocation? Or was it an apology? Would there need to be an accompanying text for such images to constitute provocation or apology? No. On the other hand, sites where we wanted to remove such content did not do so, because we did not have the proof that it was really something to be concerned about. This is another element of the new kinds of difficulties that we must face today.

Consider an image of the Bataclan, the site of a horrible terrorist attack. Such images were spread widely—but only the images, by themselves and without commentary. Was this a provocation or an apology?

There are two big problems concerning messages and terrorism. The first is the debate between security and liberty. The debate is essential because the internet was created on the basis of liberty, with the technical contributions of Silicon Valley, and security, with support from DARPA and the Pentagon. These twin poles of liberty and security are what make the internet viable and this leads to another difficulty: the more we try to work "upstream" in a preventive manner, the more we intrude into private life. At what point does the intrusion into private life become more harmful than the risk of the terrorist act that we want to prevent? We are in a debate concerning our entire society.

The second debate that we are having in France—and you have it in the US with Apple versus the FBI—is over encryption. For us, encryption is an element of confidence, it permits an enormous number of commercial transactions and exchange of other data that we consider to be confidential. If we want to be able to break encryption, we would need to have backdoors and these backdoors could be utilized by others. If we insist on being able to break encryption, we risk losing the war of confidence. In France, we have Telegram, for example, which provides end-to-end encryption.

If we insist on being able to break encryption—with backdoors, for example, we risk losing the war of confidence.

My last point is more philosophical—it has to do with the power of the "verb," the power of the image, and the power of the discourse. We see that on the ground with the coalition against Daesh in Syria, which is necessary, in Mali, where it is also necessary. How can we hope to have a final victory if our discourse is not heard by the entire world, by all the countries in the world. As long as we cannot succeed in the battle of meaning, in the battle of ideas, everything else that we may do will be in vain.

Invited Address

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

The structure and purpose of the agency that I direct, the National Cybersecurity Agency of France (ANSSI), may seem unusual compared to models in some other countries. If I compare the models, it is not to criticize but to explain that France has made the choice of separating the missions of attack and defense, as well as the mission of intelligence from the mission of protecting the victims. Without pretending that we have chosen the best way to do it, I am convinced of the advantages of this model for France that clearly establishes the missions for everyone without prohibiting any of the actors from communicating and working together intelligently.

Cyber security is important not only to the ministries of defense and interior but also to foreign affairs and economics, and probably, to a majority of all the departments of the government.

The other particularity of this model is that it positions close to the Prime Minister the agency in charge of the protection of information systems. This permits effective cooperation with all the ministries since cyber security is of importance not only to the ministries that are oriented toward security—especially the ministries of defense and interior—but also the ministries of foreign affairs, economics, and probably in the near future to a large majority of all the departments of the government.

Since I am speaking to experts, I will not try to describe in detail the threat, which you already know. Instead, I will limit myself to a few observations that we have made within our agency and which concern the effects on victims. In 95% of the cases, the attacks are intended to steal information for economic purposes. In general, such attacks target large national or international industrial groups. As to the timelines, the attacker has often been there for months, or even for several years. In fact, we are dealing at the end of 2016 with attacks that were initiated in 2012, in 2013, or even earlier. For many victims, it is not even possible to say when the initial infections occurred. All this is extremely worrisome, and it demonstrates the lack of maturity of the players, notably the economic ones.

Even more worrisome are the risks that affect our critical infrastructures, that is to say all of our large networks—the electrical grid, the transport networks, the telecommunications networks, the water supply networks, and all their associated industries. This risk, which we are addressing at the international level, is not new, but the threat to our critical infrastructures is becoming more and more dangerous. I will offer two examples: the first concerns the terrorist risk, which is becoming very real. The second is the situation that we see today in the United States during the heated environment of their national elections, notably the threats—as one can read in the press—to the structure of American democracy.

Terrorism. Often, I am asked if terrorists have cyber attack capabilities or if Daesh would be able to develop the capabilities necessary for such attacks. This is a subject of very real

concern, which arises directly from the terrorist attacks that France experienced in January 2015 against the newspaper *Charlie Hebdo*, and which led to a wave of disfiguration and modification of websites. This has influenced the attitudes of decision makers and of public opinion, and it has caused cyber to be associated psychologically with terrorism. Obviously, the risk is not large at this time, even though it is something that we must deal with. The real risk lies in the question, "In the future, will terrorists be able to use digital means to attack critical infrastructure for purposes of terrorism and create serious panic by attacking networks, transportation, etc.?"

"In the future, will terrorists be able to use digital means to attack critical infrastructure for purposes of terrorism and create serious panic by attacking networks?"

Do terrorists have the competence to do it? At the present time, I observe that certain groups are certainly thinking about it. Who are they? These are often people associated with mafias, with groups associated with organized crime, and they are sometimes protected by states. Such criminal groups that are capable of creating violent attacks by digital means already exist without doubt. On the other hand, there are also those who have the means, are clearly hostile to our country, and have few scruples about paying cyber mercenaries to lead these violent attacks. The probability of these two groups coming together, if it has not already happened, is therefore extremely high. It is evident to me that, in the future, we will have a form of cyber terrorism. We must fight against this kind of problem in a very complex context, because we are likely to have groups claiming responsibility, but we will have considerable difficulty in discovering which groups are actually responsible.

The Situation in the United States. The other troublesome situation concerns events that are now occurring in the United States. The American electoral campaign has been highly perturbed by various revelations and intrusions into information systems, principally to obtain private correspondence linked to political figures. Analysts are blaming groups such as APT28, which is well known in France and seems to have been behind the *TV5 Monde* attack. This group may also be behind the attacks against the German parliament, and it seems to have links with Russia. I will be extremely prudent on this subject, however, because all of this would need to be proved—which we do not know how to do at the present time, even though we have strong suspicions. I have a feeling that we are entering the era of an arms race and preparation for war that makes me extremely uneasy.

To my great surprise, NBC News announced on 4 November that US government hackers had prepared some kind of counter attack that would be used against Russian systems in case of problems during the US elections.

In response to these threats and the rising concerns, we have made an important choice in France concerning the protection of critical infrastructure, which is to rely on law and regulations in order to impose security on those who are considered to be operators of vital national importance. This choice was made in 2012 and became law in December 2013. After a fairly long process of building confidence with the operators, we have now published in the "Official Journal" of the French Republic the obligatory security rules that are

imposed on the operators of vital importance. A very positive point is that this work has been accomplished with the close cooperation of the operators themselves. The idea was not to impose inadequate regulations on them, but to help them. By assisting the operators of vital importance, we help the nation, which is the objective of the agency that I direct.

This essential work depends on the availability of security solutions and suppliers capable of performing the work. Some of the rules cover organization and governance; others are more technical in nature because they must protect the network with appropriate architectures to detect attacks, and to respond to these attacks. All these things depend on true professionals who are specialized in these areas and on whom we depend to protect all the critical infrastructures. We evaluate and certify those private suppliers on the basis of public repositories. This effort to protect critical infrastructures is therefore well underway, and I salute the work done by all those, public and private, who are engaged in this undertaking. It represents an acknowledgement of the danger and a desire for protection, since the threat is no longer hypothetical—it is today's reality.

Until now, we have worked for the most part at the national level, because we are concerned with the protection of the nation, but we have been aware from the beginning and we recognize from our daily experience that there are limits to what can be achieved at the national level. These limits are very real, because the protection of those whom we need to defend does not stop at the borders of France. We must work with our partners, including multilaterally within NATO. Above all, we must work with Europe in order to develop cyber security in the most consistent manner possible over the entire continent. To be very clear, when I speak of Europe, it is continental Europe, which I hope, includes the United Kingdom. At the European level, interesting efforts are underway which permit optimism. The NIS (Network and Information Security) directive concerning the security of networks builds on the main themes that we have achieved in France for the protection of the critical infrastructures. This is an extremely positive element that will permit an effort larger than that we would be able to have only in France or only in Germany or only in the UK. We have a public/private cyber partnership (cPPP) for research at the European level led by the European Commission, which will permit the allocation of about 450 million euros for the coming years in order to develop research on cybersecurity and the corresponding industrial development. It is also very positive that cybersecurity is from now on included in the European research programs. More generally, we have a capacity development with the different countries of Europe (which, it must be recognized, are at very unequal levels of development) notably through the European ENISA agency. ENISA is doing very interesting work developing and assisting countries that no longer have a choice but to develop true capabilities in cybersecurity because they are required to do so by the NIS directive.

Above all, we must work with Europe in order to develop cyber security in the most consistent manner possible over the entire continent.

We want to make sure that, in the name of free trade, these treaties do not interfere with the ability to regulate.

All this is very positive, but there are a few areas where preoccupation and vigilance are necessary on our part, notably concerning economic treaties such as the TTIP, TISA, and NAFTA. We want to make sure that, in the name of free trade, these treaties do not interfere with the ability to regulate. This applies especially in two areas:

- *The ability to evaluate security products.* We would like to continue to be able to evaluate security products at the appropriate level, so that the products can inspire confidence. That can be complicated; it can take time; and it might even require access to confidential data such as source code. Therefore, the economic treaties potentially pose a real issue.
- *The ability to control the localization of data.* There are cases where data do not need to be localized at all; there are other cases, where one would like them to be localized in Europe; and there are cases involving data that are especially sensitive, where one would like the data to remain on national territory. We consider that the ability to regulate localization is necessary. Of course, it must be done properly, but above all it must not be considered as a form of protectionism, because this is not the case.

In conclusion, I have the impression that we are increasingly living in a kind of digital Far West, rather like the images that we have all seen of cowboys in the so-called Western films. There are more and more actors who are promenading around with a Colt revolver on their belt, showing that they are armed, ready to defend against attacks, and ready to respond. This presents real problems, especially given the fact that the attribution of attacks can be extremely complicated and difficult. We are accustomed to hearing that "If you want peace, prepare for war," but I have the impression that—at the present time—many actors are operating in a manner that might be more correctly described as "If you want war, prepare for war." This concerns me enormously, because the notion that "If you want peace, prepare for peace" is not being sufficiently considered today and we are increasingly in an armaments race. Without being alarmist, I have a feeling that we are in a situation that our countries all experienced in the dawn of the 1914 conflict, when countries were showing their muscles and excessively developing their offensive capabilities without asking the question, "And afterwards, what are we going to do with all that?" Beyond the development of offensive capabilities, it is essential that all of the actors address the question, "What must we do to live in peace in cyberspace?"

I have the impression that…many actors are operating in a manner that might be more correctly described as "If you want war, prepare for war."

Invited Address

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

Le modèle de l'agence que je dirige, l'ANSSI, peut sembler original comparé à d'autres modèles. Si je compare les modèles, ce n'est pas pour les critiquer mais plutôt pour expliquer le choix qui a été fait en France de séparer les missions d'attaque des missions de défense, et les missions de renseignement des missions de protection des victimes. Sans prétendre que nous avons la meilleure manière de faire, je suis convaincu de l'intérêt de ce modèle pour la France qui établit clairement les missions des uns et des autres sans empêcher les différents acteurs de se parler et de travailler intelligemment ensemble.

L'autre particularité de ce modèle est qu'il positionne auprès du Premier Ministre l'agence en charge de la protection des systèmes d'information, chargée d'actions purement défensives. Cela nous permet d'avoir une coopération efficace avec l'ensemble des ministères puisqu' aujourd'hui, la cyber sécurité intéresse non seulement les ministères portés sur la sécurité—ministères de la défense et de l'intérieur en tête—mais aussi les autres ministères—affaires étrangères, économie, et demain probablement la très grande majorité des départements ministériels.

La cybersécurité intéresse non seulement les ministères portés sur la sécurité mais aussi les autres ministères..et demain..la très grande majorité des départements ministeriels.

Comme je m'adresse à des experts, je ne vais pas revenir en détail sur la menace, que vous connaissez, et me bornerai à quelques observations que nous faisons aujourd'hui au sein de notre agence en ce qui concerne le traitement des victimes. Dans 95% des cas, il s'agit encore d'attaques qui visent à voler de l'information à des fins économiques. C'est la réalité du terrain aujourd'hui. En général, ces attaques ciblent de grands industriels nationaux ou internationaux. En terme de positionnement dans le temps de ces attaques, l'attaquant est très souvent là depuis plusieurs mois, voire plusieurs années, et nous déplorons le fait que nous traitons aujourd'hui fin 2016 des attaques qui ont été initiées en 2012, 2013, voire même avant dans certains cas. Pour de nombreuses victimes, il ne nous est pas possible de dire à quand remontent les infections initiales. Il s'agit donc de quelque chose d'extrêmement inquiétant, qui montre un manque de maturité de la part des acteurs, notamment de la part d'acteurs économiques.

Aujourd'hui la menace qui pèse sur nos infrastructures critiques se fait de plus en plus pressante.

Plus inquiétants encore sont les risques qui pèsent sur nos infrastructures critiques, c'est-à-dire tous les réseaux que nous connaissons—réseaux d'électricité, de transport, de télécom, d'eau, ainsi que toute l'industrie qui va avec. Ce sujet, dont on parle au niveau international, n'est pas nouveau mais aujourd'hui la menace qui pèse sur nos infrastructures critiques se fait de plus en plus pressante. Je vais prendre deux exemples, deux cas d'application : le premier

concerne le risque terroriste qui devient bien réel. Le second, c'est ce que l'on peut observer aujourd'hui aux Etats-Unis dans cette actualité brûlante liée aux élections américaines, notamment les menaces que l'on peut lire dans la presse qui semblent peser sur le mécanisme démocratique américain.

Le terrorisme. On me demande souvent si les terroristes ont des capacités d'attaque informatique ou si Daesh pourrait développer des capacités d'attaque informatique ? C'est un sujet d'inquiétude bien réel qui est directement lié aux attentats terroristes que la France a connus en janvier 2015 contre le journal Charlie Hebdo, et qui ont donné lieu à une vague de défiguration et de modifications de sites internet. Cela a beaucoup marqué les esprits, à la fois des décideurs et de l'opinion publique, et créé le premier lien entre cyber et terrorisme. Bien évidemment, le risque n'est pas là, même si c'est quelque chose qu'il faut traiter. Le vrai risque est dans la question: « Est-ce que demain des terroristes pourront utiliser des moyens numériques pour être capables d'attaquer des infrastructure critiques à des fins de terrorisme et créer une véritable panique en s'attaquant à des réseaux, de transport ou autres ? »

La question de savoir si demain nous aurons une sorte de cyber terrorisme est une évidence.

Les terroristes ont-ils la compétence pour le faire ? J'observe aujourd'hui que manifestement des groupes s'affairent. Où sont-ils? C'est un problème, quoi que l'on s'en doute un peu. Ce sont souvent des gens associés à des mafias, à des groupes liés à la criminalité organisée, parfois protégés par des états. Donc ces groupes qui sont capables de mener des attaques violentes par le biais du numérique existent aujourd'hui à n'en pas douter. D'un autre côté, il y a également des gens qui ont des moyens, en veulent clairement à nos pays, et n'auront pas beaucoup de scrupules à payer des cyber mercenaires pour mener des actions violentes. La probabilité que ces deux groupes se rencontrent, si ce n'est déjà fait, est évidemment extrêmement forte. Donc, pour moi, la question de savoir si demain nous aurons une sorte de cyber terrorisme est une évidence. Nous devrons lutter contre ce genre de problèmes dans un contexte très complexe parce que nous aurons peut-être des revendications mais nous aurons du mal à savoir qui a réellement tenu l'arme.

La situations aux Etats-Unis. L'autre situation inquiétante concerne ce qui se passe aux Etats-Unis. La campagne électorale américaine a été grandement perturbée par diverses révélations et intrusions dans les systèmes d'information, notamment pour récupérer de la correspondance privée liée aux différents responsables. Les analystes pointent du doigt des groupes comme APT28, bien connu en France, qui semble être derrière l'attaque contre TV5. Ce groupe, qui se fait régulièrement remarquer, pourrait aussi être derrière les attaques contre le parlement allemand et semble avoir des liens avec la Russie. Je suis extrêmement prudent sur ce sujet parce que tout cela mériterait d'être prouvé, ce que l'on ne sait pas faire aujourd'hui même s'il y a de fortes présomptions. J'ai le sentiment que nous entrons dans une ère de course aux armements et de préparation à la guerre qui me laisse particulièrement inquiet.

Au-delà de ces menaces et de cette montée des inquiétudes, on a fait le choix en France en matière de protection des infrastructures critiques de passer par la réglementation pour imposer la sécurité à ce que l'on appelle les opérateurs d'importance vitale. Ce choix a été fait en 2012. Il s'est concrétisé dans la loi de décembre 2013 et, après un assez long processus pour établir la confiance avec ces opérateurs, nous publions aujourd'hui dans le Journal Officiel de la République Française les règles obligatoires de sécurité qui s'imposeront aux opérateurs d'importance vitale. Le point très positif est que ce travail a été fait en coopération étroite avec les opérateurs eux-mêmes. L'idée n'est pas de piéger les opérateurs, de leur imposer une réglementation inadaptée ou inutile, mais de les aider, et en aidant les opérateurs d'importance vitale, on aide la nation, ce qui est l'objectif d'une agence comme celle que je dirige.

On a fait le choix en France… de passer par la réglementation pour imposer la sécurité …aux opérateurs d'importance vitale.

Ce travail essentiel repose aussi sur la disponibilité de solutions de sécurité et de prestataires de sécurité capables de faire le travail. En effet, un certain nombre de ces règles sont liées à l'organisation et à la gouvernance, d'autres sont des règles plus techniques puisqu'il faut bien être capable de protéger les réseaux, de les architecturer autrement, de détecter les attaques et de réagir à ces attaques. Toutes ces choses relèvent du niveau de véritables professionnels qui ne font que cela et sur lesquels nous comptons pour protéger l'ensemble des infrastructures critiques. Nous évaluons et qualifions ces prestataires privés sur la base de référentiels publics. Cette démarche de protection des infrastructures critiques est donc bien engagée et je salue le travail fait par l'ensemble des acteurs publics et privés dans ce domaine. Il y a une véritable prise de conscience, une volonté de se protéger car la menace n'est plus hypothétique—elle est bien la réalité d'aujourd'hui.

Jusqu'à maintenant, nous avons beaucoup travaillé au niveau national puisque nous sommes bien sur des questions de protection de la nation, mais nous savions dès le départ et nous l'expérimentons au quotidien, que ce travail national trouve ses limites. Il trouve ses limites parce que la protection des gens que nous voulons protéger ne s'arrête pas aux frontières de la France. Nous devons travailler avec nos partenaires, en multilatéral au sein de l'OTAN dans un contexte bien particulier. Nous devons surtout travailler au sein de l'Europe de manière à développer la cyber sécurité la plus homogène possible sur la plaque continentale. Pour être très clair, lorsque je parle de l'Europe, c'est la plaque continentale européenne qui, je l'espère, inclut le Royaume Uni. Au niveau Européen, des démarches intéressantes sont en cours qui rendent optimiste. La démarche de la directive NIS (Network and Information Security) sur la sécurité des réseaux reprend les grandes idées de ce que nous avons pu faire en France sur la protection de l'architecture critique. C'est un élément extrêmement positif qui va nous permettre d'avoir une démarche plus large que ce que nous faisons simplement en France ou que ce que font les Allemands de leur côté en Allemagne. Nous avons un travail de partenariat cyber public/privé (PPP) pour des travaux de recherche au niveau de l'Europe portés par la Commission Européenne, ce qui va permettre d'allouer environ 450 millions

Nous avons un travail de partenariat cyber public/privé pour des travaux de recherche au niveau de l'Europe portés par la Commission Européenne.

d'euros dans les années à venir au développement de la recherche en cyber sécurité et le développement industriel qui va avec. Il est également très positif que la cyber sécurité soit dorénavant incluse dans les programmes de recherche européens. Plus généralement, nous avons un développement capacitaire avec les différents pays d'Europe (qui, il faut bien le reconnaître, sont aujourd'hui à des niveaux très variables) notamment en nous appuyant sur l'agence Européenne ENISA. ENISA fait un travail intéressant de développement et d'assistance aux pays qui ont envie ou qui n'ont même plus trop le choix de développer de vraies capacités en cyber sécurité puisque la directive NIS le leur impose.

Tout cela est très positif avec toutefois quelques sujets de préoccupation et de vigilance de notre part, notamment autour des traités économiques transatlantiques en cours comme le TTIP, TISA, et NAFTA. Nous veillons à ce que, au nom du libre-échange, ces traités ne viennent pas mettre à mal des dispositifs de capacité à réglementer. Cela s'applique particulièrement à deux domaines :

- *La capacité à évaluer les produits de sécurité.* Nous souhaitons pouvoir continuer à évaluer les produits au bon niveau pour donner confiance et cela peut être compliqué, prendre du temps, et même nécessiter l'accès à des données sensibles comme les codes source. Donc, c'est un vrai sujet que l'on peut retrouver dans les traités économiques.
- *la capacité à réglementer sur la localisation des données.* Il y a des cas où les données n'ont pas besoin d'être localisées, et il y a des cas où on peut être amené à vouloir qu'elles soient localisées en Europe. Et puis il y a des cas plus forts de données particulièrement sensibles où l'on peut vouloir que les données restent sur le territoire national. Nous considérons cette capacité à réglementer comme étant nécessaire. Elle doit être bien utilisée, mais surtout ne pas être vue comme une forme de protectionnisme parce que ce n'est pas le cas.

En conclusion, j'ai quand même l'impression qu'aujourd'hui nous sommes de plus en plus dans une sorte de Far West numérique avec cette image que nous avons des Westerns et des cowboys. Il y a de plus en plus d'acteurs qui se promènent avec le colt à la ceinture et qui montrent qu'ils sont armés et prêts à se défendre et à répondre aux attaques. Cela pose de vrais problèmes, notamment du fait que l'attribution même des attaques reste un sujet extrêmement compliqué. Nous avons l'habitude de dire que « qui veut la paix prépare la guerre », mais j'ai l'impression qu'en ce moment, beaucoup d'acteurs sont plus dans le mode de « qui veut la guerre prépare la guerre ». Cela m'inquiète énormément car la notion de « qui veut la paix prépare la paix » me semble assez peu traitée aujourd'hui et nous sommes plus dans une démarche de course aux armements. Sans être trop alarmiste, j'ai un peu le sentiment que nous sommes dans la situation que nos pays connaissaient à l'aube de 1914 à un moment où chacun montrait ses muscles et développait ses capacités offensives à outrance sans trop se poser la question de « Et après, qu'allons nous faire de tout cela ? » Au delà des travaux offensifs, il est essentiel aujourd'hui que l'ensemble des acteurs se posent la question « Comment allons nous faire pour vivre en paix dans le cyber espace ? »

Cybersecurity for a World of Rapidly Intensifying Cyberwarfare

Mr. Marty Roesch
Vice President and Chief Architect
Security Business Group, Cisco

We are living in interesting times. I have worked on cyber security for about 20 years, beginning as an engineer. In 1998, I wrote a program called *Snort* that became a part of the foundation for the analysis of network traffic and intrusion detection. *Snort* grew into a company called Sourcefire, which was acquired by Cisco in 2013. Today I am the chief architect for security at Cisco, and my role is to bring together all of Cisco's security technologies into a cohesive architecture that we can offer to our customers. When you do this sort of work, you don't do it in a vacuum but in the context of current trends in cyber security.

Most recently, these trends have been fascinating to watch, and challenging to keep up with. We have seen a lot of politically motivated hacking of the US election. We have also seen interesting developments in the area of Internet of Things (IoT), which is turning into a weapons platform: one hundred thousand IP-connected cameras were used to mount one of the largest denial-of-service attacks in history. So yes, we are living in interesting times because these ideas that we thought were still under development are already playing out. Attacks against political campaigns are particularly fascinating because they are essentially "influence operations," that we see happening almost in real time. And to paraphrase Carl von Clausewitz, the Prussian military theorist from the 1800s, cyber war feels like the continuation of politics by other means. Since many networks are running on Cisco gear, we want to be able to help our customers manage the risk of these emerging trends.

One hundred thousand IP-connected cameras were used to mount one of the largest denial-of-service attacks in history.

There are a lot of people working on these problems. There exists a vast cyber security industry that has grown up over the past 20 years and, in a lot of ways, gotten out of control. Today, there are about fifteen hundred security vendors offering fifteen hundred different solutions that frequently overlap. I can guarantee that there are not fifteen hundred ways of doing security. So, instead of the standard approach to security—which consists of buying a lot of products that you believe are best of breed and trying to figure out a way to get them to work together—we need to find a center of gravity to build around.

This approach to security has not been working well and you can see it in the news. The compliance regimes and mechanisms for ensuring the functionality and security of the devices on the market—whether government-sponsored or sponsored by industry bodies—are often featured by companies that you are reading about because they have been hacked from top to bottom.

Because cyber security is so complicated, people often lack the conceptual or intellectual anchors to move forward with their plans for security purchases or architectures. To facilitate the conversation, Cisco has built four principles that we use to talk about cyber security.

1. Security Must Enable the Safety, Growth and Prosperity of Global Citizens and Nations

Security must be there for everyone in order to enable an organization's growth and prosperity. According to David Goeckeler, SVP of Networking and Security at Cisco, good, bug-free software actually enables innovation. By securing the foundations of your organization, you are able to innovate, move forward, and grow more quickly because you can trust and build upon what is behind you. The flip side is that security cannot be a roadblock that prevents you from moving forward.

According to my boss at Cisco, David Goeckeler, good, bug-free software enables innovation.

Security professionals must proactively engage government organizations to make sure that the compliance regimes —rules and regulations that are brought forth by governments — are in line with the existing security realities and necessities. The security field is quite broad, with some people focusing on cryptosystems and others on reverse engineering, while I focus on threat-centric security. In order to maintain the integrity of operational environments to find, localize and defeat hackers, I need to be able to understand the unique challenges faced by other teams. When something like the Wassenaar Arrangement is announced for the control of vital cyber security exports, the reverse engineering and research communities tend to complain because they don't feel that they have had an opportunity to be listened to or to express their concerns. Since the policies would be much better if these communities could be consulted ahead of time, security professionals need to take proactive steps in order to have a seat at the table as we innovate and as we bring more digital future to governments and organizations.

2. Security Must Work with Existing Architecture and Be Usable

We are entering an era of trusted platforms: the iPad and the Chromebook are trusted platforms. They operate on what we call "walled gardens," where the systems manufacturers curate what is available to the systems; they have very discrete control over the hardware elements with which they are built; and they try to produce a secure execution environment that does not contain malware and limits the opportunities for attackers to get in. Trusted platforms like the iPad and the Chromebook are great, and, in a lot of ways, they are the future, but they are not part of the past 35 years during which our computing infrastructure has been deployed.

We have to work on what has been deployed as well as on what things will look like moving forward. Think of the Internet of Things and the very obvious security issues that it brings. When my family complains about not being able to get to a website, I have to tell them

about how one hundred thousand IP-enabled cameras were hacked and used to blow them off the internet. As it stands now, anybody can make any device they want, plug it into the public internet, and it is supposed to be okay. But maybe it is not okay. Perhaps there needs to be a kind of regulatory compliance regime for the IoT so that it can interoperate with the legacy architectures that are already in use without posing a danger to those architectures and to all of us as well. The recent IoT attack against Dyn, which took down part of the Internet, was a drop in the bucket compared to what could be coming. Right now, we have terabit/second denial-of-service attacks on the internet. If a terabit/second is possible now, ten terabits/second cannot be far behind. Beyond that level of attack, who knows how the ability of the internet to move packets would be impacted. Instead of a DNS service going down, which just happened with the IoT attack on Dyn, perhaps a large segment of backbone could go down.

Perhaps, there needs to be a kind of regulatory compliance regime for the IoT so that it can interoperate with the legacy architectures.

That is a scary notion, and we need to find a way to deal with it. It is challenging since organizations with pre-existing architectures have to be able to secure themselves in this new world. Moreover, security architectures have to blend right in. If this doesn't happen, people will simply find ways to go around them. I know of security professionals inside my own organization who are circumventing these security controls, because they simply do not like the way these security controls are done and think that they can do better.

3. Security Must be Simple, Open and Automated to be Effective

Currently, organizations deploy very complex security architectures. We go out and buy one of everything that seems to be needed in the best of breed systems, bring it back to our shop and try to make it all work together. But because nothing was really built to work together, it does not work well. Next, we take the data these systems generate, and we dump them into a data management platform, cross our fingers, and try to figure out what is happening. We use that information for the next configuration of the infrastructure that is deployed.

This model for doing security is failing over and over again. If we are going to build real security in the future, we need something that permits automated information sharing and radically improves security intelligence. I know that people care about information sharing because every government conference I have gone to for the past 15 years has had at least one track on "How do we share information?"

We are building systems…capable of collecting metadata… such as files that possibly contain malware, or which IP addresses and domains people are going to.

Fortunately, we have taken a step toward making the infrastructure share information automatically. We are building systems with points of presence on networks and devices that are capable of collecting metadata about discreet things that we are interested in, such as files that possibly contain malware, or which IP addresses and domains people are going

to. We take that information, stream it up to a cloud back-end and then look at it holistically and globally across the entire deployed footprint of collectors.

The collectors do more than collect information—they are also control points. If a file shipped up to a cloud turns out to be a bad file, I shut that file down and whoever is plugged into that cloud will no longer be able to run that file. Essentially, I just did information sharing by fiat of the system's architecture. This is the current state-of the-art that is incorporated in actual products that we are shipping today. From my standpoint, this is one of the most exciting things that I have seen in the last twenty years. We are building real information sharing architectures that integrate end points, networks and cloud capabilities together under one roof that automatically share information without human involvement. Humans get involved and alerted when things go off the rails, but this information-sharing infrastructure has such a high degree of automation that it really breaks out of the mold of everything that I mentioned earlier.

One-third of the world's emails go through our email security gateways. We see about 5% of the world DNS traffic and sandbox about 1.5 million samples of previously unseen malware every day.

Since we are able to do this and tie it to global threat intelligence, we can do some really interesting things. At Cisco, we have an impressive dataset that we operate on a day-to-day basis. My side job is with Talos, Cisco's threat intelligence team. Talos deals with all the threat intelligence that we get in through our systems. Everyday, about one-third of the world's emails go through our email security gateways. We see about 5% of the world DNS traffic and sandbox about 1.5 million samples of previously unseen malware every day. With this data, we are pulling out the intrinsics, i.e., IP addresses, domain names, URLs, file identification and metadata. We bring all that together, normalize it and then push it back out to our security infrastructure, our web security gateways, our email security gateways, our Intrusion Prevention Systems (IPS), and our advanced malware Systems. We are doing this transparently and automatically, so that information sharing is a side effect of the architecture of the system.

We want to achieve "networked defenses"—where defenses themselves are networked together, automatically share information, and are aware of the global security picture.

This is exciting for a number of reasons: first, it recaptures growth in our business and second, it is changing the way people do security. We need an architecture that achieves what we have been trying to achieve manually for decades, and we are making progress. At the end of the day, we really want to achieve "networked defenses"—where defenses themselves are networked together, automatically share information, and are aware of the global security picture.

4. Security Must Enable Visibility and Appropriate Action

Traditionally, we use our security infrastructure to provide visibility and control through the intrusion prevention system and vulnerability management system. Today, a whole new layer of visibility and control is being built and deployed everywhere—it even includes

those smart light bulbs on the ceiling, one of which may be IP-enabled. The Internet of Things is a visibility and control network for our interactions with the real world, and it is vitally important that it should be secure in order to be usable and not pose a threat to societies, cities, or even mankind.

Integrity must be the foundation: if you cannot maintain the integrity of the environment of the systems you operate with, you cannot get good security. When I talk about integrity, I talk about this infosec mindset in which the integrity of the system is required to perform high-level security functions. If you cannot control what is executed on the CPUs, the contents of the RAM, how they utilize the network, or if you let the network be under someone else's control, then you cannot do security. High-level functions like cryptosystems do not work once somebody has control of the CPU: you may think everything is encrypted but it is not encrypted against the person you are actually trying to hide the data from. So a very important, high-level goal is to be able to maintain the integrity of our operating environment or re-establish this integrity in the wake of an attack.

High-level functions like cryptosystems do not work once somebody has control of the CPU.

The Challenges

Encryption. There are two additional challenges: our relationship with cryptography and with the Internet of Things. Cryptography, like any good tool, can be used for good or for evil. It can secure the communications of terrorists, but it can also be the foundation that is required to build a secure automated software update system. One of the biggest advances in security over the last 15 years has been automated software updates. Now we can automatically update software on devices in such a way that every Microsoft Tuesday you get the latest set of patches that incrementally make that windows system run more securely. Periodically, I get updates on my iPhone that make my phone more secure. My Tesla car now gets software updates and it keeps getting more secure and faster.

One of the biggest advances in security over the last 15 years has been automated software updates.

In order to do these things, we need a strong cryptography capable of guaranteeing the trust and integrity of the software that is being deployed on our devices. Without that, we cannot trust automated software updates. Unfortunately, the roots of trust for automated software updates capable of giving us better software safety across all the devices we use are the exact same foundations that allow people like Julian Assange to safely move data from point A to point B to embarrass governments, corporations, or whomever is on his hit list. We need to have a conversation about that.

During our regular discussions with the FBI, the Director has mentioned that we need to build backdoors in these systems. This would fundamentally undermine the trustworthiness of the systems and, if we are going to do that, who could be trusted to hold

It is like saying: "Trust us, we are the government. We will hold your keys for you. Why won't you trust us?"

the keys and not lose them? Given all the leaks that we have had lately coming out of places that are never supposed to leak—the FBI, the NSA, etc.—this is a big problem. It is like saying: "Trust us, we are the government. We will hold your keys for you. Why won't you trust us?" Well, I can give you a list of reasons. We need to have a more mature conversation about what we are willing to live with. It is about being able to get metadata about terrorists' conversations as well as conversations themselves. Law enforcement is to the point where they mostly track metadata of the communications that take place and it is the same with intelligence agencies. They track metadata as opposed to trying to be in the conversation. This is challenge number one. We as a civilization need to figure out the rules of war for cyber—what needs to be off limits and what is okay—and we also need to figure out the rules for cryptosystems.

The Internet of Things. The other challenge is the Internet of Things, which has so much promise. I love having IP-enabled light bulbs in my house that I can talk to individually; I love being able to reset my thermostat while I am at the airport, because I forgot to turn it off before leaving my house. But I hate not being able to get to Twitter because someone launched a gigantic attack against a DNS service and the attack was made possible because some manufacturer has not done the basic security to make sure that their IoT devices could not be used as part of a botnet.

Some things can be done. The same mechanisms that are used to curate walled gardens for things like iPads and Chromebooks can be used for the Internet of Things to provide and revoke keys that could operate on trusted platform modules on these devices. When they are at the point where they pose a global threat to the internet, the keys could be revoked and these devices could be disarmed or deactivated. This would be to the dissatisfaction of those who bought them on the one hand, but, on the other hand, it would be for the greater good. Now obviously, you would need some sort of classification system because it would be fine to turn off my IP-enabled light bulb, it would not be fine to turn off my IP-enabled pacemaker. Those sorts of things need to be hammered out.

Mechanisms used for things like iPads and Chromebooks can be used to provide and revoke keys on IoT devices…. where they pose a global threat to the internet.

In summary, the principles that I have outlined offer an excellent approach that can be built upon for securing the entirety of the environments that we are trying to protect today. They are also relevant to dealing with the ever-expanding world of cyber warfare and pervasiveness of internet-connected devices.

Cyber Influence Opérations—DAESH Propaganda, Manipulating Elections, and Influencing Public Information

Ingénieur Général Daniel Argenson
Deputy Director, Institut des hautes études de défense nationale (IHEDN)

Since the workshop has been focusing on strategic disruptions this year, it makes a lot of sense to have a panel on this important issue. I would like to thank CDSR for having scheduled it and having asked me to be the moderator.

Are we facing a disruption? Is there something new concerning strategic disruptions? Information wars and manipulation of information have always existed. During the Cold War, it was called disinformation. According to the free dictionary website, disinformation means "deliberately misleading information announced publicly or leaked by a government or especially by an intelligence agency in order to influence public opinion or the government in another nation." A new paradigm is emerging from the massive use of the connected world and the fact that it ignores state borders. This is presenting an unexpected new dimension, sometimes called the 4th industrial revolution, which may benefit mankind but at the same time makes our democracies more vulnerable. This panel will focus on the dark face of this, commonly called the dark web.

At the recent Warsaw summit, NATO declared cyberspace to be a full dimension of armed conflicts, which means that article 5 of the North Atlantic Treaty can be invoked in case of a cyber attack, but also that cyber is fully part of military operations. Jamie Shea will address the strategic threat of cyber operations and how NATO and the Allies are responding. In recent years, we have also witnessed the growing use of cyber for propaganda and recruitment and the difficulties we have in countering this situation and preserving our democratic values. Last year, we had a workshop roundtable focusing on this issue. Despite the fact that ISIS is close to losing its territory, the cancer has been spreading and we will face its consequences for years. We increasingly talk about cybercrime and again about the difficulty of tracking it and punishing those who are responsible. More recently, the US election campaign has shown the expanding and even disrupting role of information or disinformation and called democracies' attention to that. Frédérick Douzet will address this problem.

The US election campaign has shown the expanding and even disrupting role of information or disinformation and called democracies' attention to that.

We can imagine many other examples of cyber influence, such as in the stock market. All show the huge leverage effect of cyberspace, which was unpredicted a few years ago, and the associated risk of escalation due to major countries' mutual accusations and misunderstanding. That is why it could be interesting today to compare the Russian perception of cyberspace with ours. Kevin Limonier will share his experience with us.

The Strategic Threat of Cyber Operations and How NATO And the Allies are Responding

Mr. Jamie Shea
NATO Deputy Assistant Secretary General for Emerging Security Challenges

The objective of this panel on Cyber Influence Operations—Daesh Propaganda, Manipulating Elections, and Influencing Public Opinion is to look at the exploitation of the web for malicious purposes, whether at state level or at the ISIL level. Just to do something a little bit different, I thought I would tackle the idea of cyber terrorism and provide some thoughts on that.

Five Considerations on Cyber Terrorism

First, what is cyber terrorism? Frankly, we do not know. Just as it has proved impossible despite 30 years of efforts in the UN to have a definition of terrorism, we have not come up with a definition of cyber terrorism either. For example, does it have to be an attack similar to the way a cyber attack could be considered in NATO as a potential Article 5? Does it have to have a degree of damage, or even death or destruction, before it can be considered as the equivalent of terrorism in the physical domain? Or is it enough to use the internet to spread fear, to intimidate, to coerce, to propagandize, or to recruit? We need to do some more work in order to have a clear idea. Cyber terrorism is still too much associated with cyber vandalism. As such, it does not communicate a set of political objectives and can come across as disruptive for it own sake. So as long as we, even within our NATO countries, are confused about this, it is going to be difficult for us to act together.

Second, do Jihadists actually want to carry out cyber attacks? So far, the evidence is no. Is this because they do not have the capabilities? I would say probably not. The glory of cyber is that you can attack anybody from anywhere anytime and with a minimum of effort. And even if you cannot do the attack yourself, for $1,000, you can hire someone in cyberspace who will carry out an extremely good 400 gigabyte per second denial of service attack for you and, for another $1,000, that person will give you the after sales service of repeating that attack every five minutes for as long as you want. So there is no sort of physical limit to the ability of Jihadist organizations to carry out at least basic attacks if they choose to do so. But a lot of evidence suggests that they do not want to go down that road. Of course, there are threats that are facilitated by the internet and threats that exist because of the internet and I would argue that the ratio is definitely in the second category since our business model is increasingly based on internet functionality. If the internet does not work, ISIL cannot work. ISIL probably has as much to lose from a war in cyberspace as anyone else.

Third, attribution is notoriously difficult. After the attack on TV5 Monde in France last year, there was a great deal of confusion for quite a while and there is still no evidence as to who was behind it. First the finger was pointed at ISIL and later at the Russian intelligence services. Therefore, in a confused world there are indications, if not evidence, but it is not so

easy for Jihadists to actually put on an authentic label proving that they were truly behind the attack. It is much easier to do if they are actually behind a physical terrorist attack.

Fourth, "if it bleeds, it leads." It is obvious that it will be much easier to gain attention with sensational killings and a lot of blood than with cyber attacks. Also, at least from a terrorist point of view, cyber attacks could become devalued since newspapers report increasingly severe cyber attacks almost daily and terrorists look for the unusual, the rare, or the sensational to get publicity. Is it in their interest to invest in something that is becoming rather common? There is also the fact that the public is becoming resigned to cyber attacks; and many entities are reluctant to admit that they have been attacked in the first place.

Fifth, terrorism is incredibly cheap. Most of the lone wolf attacks that we have experienced cost between $200 and $1,500 maximum. A rudimentary cyber attack is still going to be inexpensive vis-à-vis, for example, investment in chemical capabilities or weapons of mass destruction, but it is nonetheless more expensive. So for the time being, terrorists are likely to keep looking at the internet more for propaganda, radicalization, recruitment, financing, command and control and operations, rather than for disruption. On the other hand, terrorists often have to target important symbols of state power to gain traction and governments will inevitably start wising up to cyber threats and harden their critical infrastructure. In the United States, critical infrastructure also includes elections systems, voting machines and voter rolls. Then it will not be so easy, even for terrorist organizations, to attack these types of targets. Concerning cyber attacks, I see terrorism going more in the direction of raising money. There is a long association between organized crime and terrorism; in my country, the IRA was the best bank robber. As ISIL loses many of its traditional funding instruments— the ability to tax six million people within the caliphate, to commercialize art treasures, to explore oil resources—it may, like many other terrorist organizations, start looking more towards classic robbery and banks are an easy target. Yesterday, we woke up in the UK to the sensational news that the Tesco Bank had been hacked over the weekend and twenty thousand Tesco customers had lost their money. So Jihadists are likely to look increasingly to those kinds of attacks in order to raise funds.

As ISIL loses many of its traditional funding instruments… I see terrorism going more in the direction of raising money.

We Need a Coalition to Combat the Use of the Web by Terrorists And Jihadist Organizations

My second set of remarks is that we need a coalition of governments, private citizens, internet service providers, information technology companies, NGOs etc. to combat the use of the web by terrorists and Jihadists organizations. Here, the good news is that there is finally some progress. The US State Department has set up a Global Engagement Center, the EU has set up an Internet Forum, Europol already has an Internet Referral Unit and claims that, through this referral unit, 15,000 items of Jihadist propaganda have been removed from the internet so far. The European Commission is devoting its own efforts to strengthen the Internet Forum with a financial endowment of 10 million euros. In another good sign,

technology companies are increasingly recognizing their responsibility to take down Jihadist websites and propaganda. For example, Twitter claims that since the middle of 2015, it has taken down about 360,000 propaganda items. It is good news but, according to the sources that I consult, this is only removing about 40% of the material on line. Also, how do we deal with the fact that, as soon as we take down the material, the groups can either move to the Dark Web, or to different sites like Telegram or WhatsApp, to greater encryption, or they can simply replicate with reach by having 40 to 60 Twitter handles alone replicated elsewhere? This is not a long-term solution to the problem of radicalization online. We have to get better at it and it is good that companies like Google with its Jigsaw initiative are actively searching what they can do to promote an effective counter-narrative. The counter-narrative side ultimately is going to be more rewarding than simply the censorship side.

We have to understand what drives ISIL's propaganda. Only 20%, believe it or not, is based on religion and religious messages and only about 20% on violent images of beheadings. Interestingly, the overwhelming evidence of this propaganda's attraction is based on images of utopia. It is similar to the Israeli kibbutz of my student years, where the kibbutz was the archetype of the model society, the building of the new world, the egalitarian welfare state. The overwhelming material that ISIS has been putting out is images that attract young people and women, not just bloodthirsty people who want to cut someone's head. It is a totally false and artificial picture of a world that does not exist. This utopia points to the absolute necessity to deprive ISIL of its caliphate because it is neither the violence nor even the religious messages that are the great recruiting cause. It is this notion that this egalitarian ideal society actually exists to which people can contribute. The end of the caliphate, I believe, will remove the single most important propaganda instrument that ISIL could use.

ISIS has been putting out images that attract young people and women… It is this notion that this egalitarian ideal society actually exists to which people can contribute.

We also need to look into the international legal aspects of criminalizing terrorist behavior. Where do we draw the line when it comes to freedom of speech? Can we feed in to international conventions like, for example, the Budapest Convention, the Council of Europe on Cybercrime, elements about terrorist behavior as well? I think this is something that we need to look at as well. And finally, to what degree are our own cyber instruments useful in taking the offensive against terrorist groups? The Pentagon has been on the record recently for the first time, in what is normally a very covert area, actually admitting openly that it has been using cyber effects to disrupt ISIL's command and control and operations, and to spoof some of its messages to create confusion. How effective are these kinds of instruments? To what degree would they also have a side effect, perhaps of prompting cyber retaliation on behalf of ISIL? I think further research needs to be done on this.

In conclusion, social media are not the root cause of radicalization, which existed before social media were created, but they are powerful instruments to spread the message and explain why ISIL attracted recruits from 100 countries. The answer is that we have to deal

with the root causes of radicalization and not believe that simply through social media manipulation or control or censorship, we will be able to deal with this issue. As a final point, to what degree is internet radicalization based on what is now called the age of vitriol, the age of rage, the general sort of feeling that we are now living in fragmented societies where social media have produced a temptation for the human being to reveal his darker side with perfect anonymity and express rage or frustration against the elite, the evil establishment? To what degree therefore are we going to have to have this sort of social debate about the role of social media, Twitter, the US elections campaign, the Brexit debate in the UK, many examples of clearly where we are seeing the decline of the traditional media with its sensible focus on the objectivity of facts, of civility in discourse. A disagreement is not a criminal offense. We can have disagreements. But to what degree therefore is this going to grow, this sort of reliance on social media, not only producing terrorism but producing lots of other things that could equally undermine us, like populism and a lack of civility. It is a difficult issue but we ought to have that debate as well.

Hacking During the US Presidential Campaign

Dr. Frédérick Douzet
Castex Chair of Cyber Strategy, Institut des hautes études de défense nationale (IHEDN)

I have been asked to talk about the hacking of the Democratic National Committee (DNC) and the release of hacked emails by Wikileaks. The first question I want to ask is what is new about this? Spying on a foreign political organization is not something really new; manipulating an election is not really new either. What is new in this case is that the information was not only hacked by cyber means, but it was also released publicly. What is also new is that the US was the victim of the hacking in the context of a bizarre election where, according to last week's *New York Times* poll, 82% of the voters admitted that they were actually disgusted by the campaign.

What do we know about what has been going on? According to the FBI, cybersecurity companies like CrowdStrike and investigations by Thomas Rid from King's College in London, the DNC email servers were hacked by the Russian groups Fancy Bear and Cozy Bear via advanced persistent threats that the FBI linked to intelligence agencies. Technically, is this wrong? Of course, it is wrong, but it doesn't violate any norms since intelligence activities are not regulated. If we take the case of the Office of Personnel Management's hacking, it is not that much different from what has happened with the DNC hacking. The US is not happy about it, but some high officials have also mentioned that if they had the ability to do the same, they would probably do the same. Yet the fact that the information was publicly released makes the whole difference. The operation was a clear attempt to disrupt the election if we consider the timing of the content released by Wikileaks, which was just before the Democratic Convention. Julian Assange had threatened to reveal more information as the election was approaching, so there was also a pretty tense relationship between Julian Assange and Hillary Clinton. What we did not know at this point is how this information stolen by Russian services had been transmitted to Wikileaks. Who is the famous Guccifer? How was this information leaked, for what reason, and by whom?

The DNC hack was a clear attempt to disrupt the election if we consider the timing of the content release by Wikileaks, which was just before the Democratic Convention.

This leaked information… was a wake-up call on the cyber security of the electoral process in the United States.

What do we know about the consequences of this operation? There is no question that it had an influence on the authorities to start with, because it steered a panic movement about what could happen and how it could potentially affect the election. So the first important consequence was a wake-up call for the cyber security of the US electoral process. To some extent, we can wonder whether that was a service to American democracy, because a lot of experts had been warning about the vulnerabilities of the voting machines for years. Many of these machines are very old and their systems are not being updated. While it had just been a rhetorical threat until this year, the threat had suddenly become real. People realized that anybody can be hacked and that private conversations, even highly political ones, can

be leaked. This made it more real, not only in the United States but in other countries as well. For example, we have elections coming up in France, and I am not sure I would want to read what is being exchanged during the primaries here.

In a sense, it was a success for influence operations, because it triggered fears, both among the US authorities and the electorate, that it was possible to manipulate the voting registration rolls and that these data were actually not very well protected. Admiral Michael Rogers, the director of the NSA, said in September that if he had been asked a year ago about what constitutes critical infrastructure, he would have said that it was the power grid, transportation systems, etc. But he now indicates that perhaps some data should also be considered as part of the critical infrastructure. So this has definitely raised concerns about whether these voting data and the integrity of the voting process were seriously protected. Ironically, the whole process may be best protected, not by cybersecurity, but by the extreme decentralization of the system because there are so many different machines, operating systems, ways of voting, and processes.

This might underline the need for a diversity of systems to avoid any kind of massive attack or any systemic effect of an attack. The attacks also come in a weird context where one candidate, Donald Trump, claims that the election is rigged, and this raises another threat because it would not take much for him to claim that the election was hacked, and therefore stolen, if there were a single incident that could be attributed to some cyber operation. At best, it could trigger the issue of the election's legitimacy if the integrity of the electoral process were altered. At worse, it could incite violence, although violence following election results could be sparked without a cyber attack. The second irony of all this is that maybe the electoral process can be saved by the archaism of the electoral college, because differences across states can be so significant that, even if there is an incident in one state, it could undermine the "rigged election" argument if the results are consistent across other states.

There was also a wake-up call on the risks of manipulating an election through cyber means and whether that did a service to the American democracy or not.

The second big consequence was a wake-up call for the risks of manipulating an election through cyber means. Whether that did a service to the American democracy or not is another story. That is something that Roger Weissinger-Baylon wanted me to discuss. Clearly, the biggest fear of the authorities following the release of the emails was that Julian Assange or Russian services might be preparing an October surprise, i.e., the release of information that could really swing the election at the last minute. In the end, the emails that were released attracted attention to some problematic behavior and political maneuvers within the DNC, which was sort of expected, but there was not that much in the emails per se. They showed mostly politicians playing politics but did not show that Hillary Clinton was either a crook or a criminal and, if we look at the polls, they did not seem to have that much political effect. The real October surprise did not come from Julian Assange and from the Russians, it came from the letter that the Director of the FBI sent to Congress releasing little information, which raised suspicions about potential evidence of criminal behavior by Hillary Clinton. It also contributed to feed all kinds of conspiracy theories.

Conspiracy theories and the spread of fake news were also encouraged by the fragmentation of the media market and social media and this was a lot more disruptive if you look at the polls than anything that Wikileaks released. It was much closer to the election than the Wikileaks and in my opinion this was probably even more of a problem for the American democracy than what we have observed so far.

The third wake-up call was for the importance of defining rules of the road for cyberspace. Guillaume Poupard mentioned that we are moving towards a sort of Wild West. We have at the same time an arms race development with more offensive tools but also an effort within the UN Group of Governmental Experts to regulate and set up rules. The US has clearly attributed the attacks to the Russians. So what will happen afterwards? Barack Obama mentioned that there would be a proportional response, but we do not know yet what it will be. This situation is similar to what occurred with Sony Pictures where, for a while, the White House debated what they should call the attack. It was not serious enough to be a cyberwar, and it was more serious than a cybercrime, so they called it cyber vandalism.

How do you build legitimacy to respond following such an attack? ...so far, there has been a lot of restraint for fear of causing a conflict escalation so close to the election.

Yet, this raises more questions. Is attribution the business of one country and should we take its word for it? How do you build legitimacy to respond following such an attack? What is the right level of confidence? What evidence can be shared and should be shared before there is a response? What are the options for a response? Technically, it can go from sanctions to covert operations. You can use the whole range, but so far, there has been a lot of restraint for fear of causing a conflict escalation so close to the election. Aside from the risk of conflict escalation, another concern maybe that the US is leading a huge effort to regulate the area. How do you craft a response that is consistent with the values you are pushing in trying to provide rules of the road and norms of responsible behavior for states? And how do you deter a country from meddling with an election? In this case, we are not even talking about a norm, because it is not clear that a norm has been violated, this is new territory. The US is facing behavior that they really do not like, but that does not necessarily legitimize a strong response. So there is no doubt that this kind of issue will be more and more on the table as more types of hybrid warfare occur. And in the absence of open conflicts, behavior will be increasingly offensive but below the level of what would trigger a war while gradually blurring the frontier between war and peace. This will require creative answers.

In the absence of open conflicts, behavior will be increasingly offensive but below the level of what would trigger a war while gradually blurring the frontier between war and peace.

Russian Strategies for Cyber Influence

Professor Kevin Limonier
Associate Professor, Université Paris VIII,
Institut Français de Géopolitique, Slavic Studies Department

Cyberspace is a Western concept, not a Russian one, and the Russian doctrine prefers the term "information space." This is not just a semantic difference: information space includes things like television, radio, etc. and information is the center of the scope, not the medium with all its technical aspects. In this perspective, the Russian representation of digital networks is more focused on the content, while the Western classical representation has long been focused on securing the content, even though this has changed now.

The 2015 Russian cybersecurity doctrine, which is called "Information Security Doctrine," considers that the main threat to the Russian Federation's digital networks is more political than technical. It relies on the "color revolutions" of Georgia and Ukraine and also on the Maidan revolution that took place in Kiev a few years ago to explain that foreign powers may try to destabilize the "near abroad" of the post Soviet era by using the internet's social networks and other political technologies. This doctrine, along with terrorist threats, inspired the strongly criticized Yarovaya Law that was voted by the Duma last year to strengthen government control over social networks such as VK, the number one social network in Russia.

Considering cyberspace as an information space implies a totally different way of thinking about cyber operations.

Of course, the doctrine is quite discrete about going offensive. But we know that the paradigm of considering cyberspace as an information space implies a totally different way of thinking about cyber operations. For example, Russia may prefer cyber operations that have a strong symbolic impact rather than seriously disruptive technical attacks. The first example is the famous 2007 DDOS-type cyber attack against Estonia, which had a strong geopolitical background because the attack was viewed as retaliation against the Estonian government's decision to move a Red Army memorial from the city center of Tallinn to the suburbs. This story was highly commented in Russia at the time. Another case is the spectacular hacking of a Ukrainian power plant last year although it caused almost no physical or concrete damages.

Moscow does not accept responsibility for the attacks on Estonia or Ukraine, which seem to have been conducted by independent hacking groups fighting for Russian interests.

So the symbol is important, even if Russia can also mobilize its heavy cyber weaponry as it did during the 2008 war against Georgia. But in that case, the Russian army conducted cyber operations in a military perspective. In the case of Estonia, Ukraine, or other similar cyber attacks, the Russian government seems not to have been directly involved. By that, I mean that we have no proof at all: Moscow does not claim these attacks, which seem to have been conducted by independent hacking groups. But these groups usually leave interesting clues, such as code

comments in Russian, or bots that are active only during work hours, Moscow time, except for weekends and days off. Of course, these clues are not fortuitous. They are signatures, not of the Russian government, but of independent groups fighting for Russian interests and this is a kind of proxy war where the link between these groups and the Russian government is totally hypothetical. This hypothetical dimension maintains a high level of fuzziness that can be quite discouraging for Western observers because the purpose of such attacks is not to destroy, but to discourage and in some cases to destabilize.

I think this is a legacy of old Soviet strategies like the Maskirovka doctrine that was designed in the 1920-1930s and massively used during the Cold War in many countries from Nicaragua to Mozambique. It consists in destabilizing the enemy by using non-regular fighters that are more or less involved in an ideological struggle on the side of Moscow. This ideological background is very important because it influences large parts of the Russian society today and, according to very popular thinkers in Russia like Aleksandr Dugin, it encourages the involvement of people against what is perceived as a threat from the West. This reminds me of a Russian military practice called "opolchenie." Russian speakers in the room may have recognized this old word used in Russia for centuries to designate irregular fighters fighting for patriotism. Opolchenie already existed at the time of Ivan the Terrible. They harassed Napoléon's Grande Armée in 1812, fought beyond Nazi lines during World War II and exist today in the separatist territories of Ukraine. They are also the ideological and patriotic fighters we may find beyond cyber attacks hypothetically committed by Russia. Hacking groups like the Dukes, who designed the Snake virus, can be considered as a new type of opolchenie. Their concrete links with the Russian government remains a mystery and this mix of official and non-official, ideological and non-ideological dimension is the most brilliant aspect of the Russian offensive cyber doctrine, because we do not even know if these groups are Russian. But, who cares? Attribution to Russia is in the interest of Moscow and it is also in the interest of other people, perhaps in Washington or Brussels, so I would say it is good for everybody.

Protecting Critical Infrastructure from Cyber Attack

Ms. Caroline Baylon
Information Security Research Lead, AXA (R&D)

Since I chaired this same panel on critical infrastructure at last year's workshop, it gave me an opportunity to reflect about what had changed over the past year. The first thing that stands out is that many predictions that were made last year are starting to be realized. Of course, there have been significant cyber attacks on critical infrastructure in the past, but we are now moving from predicting that these were going to occur on a broad scale to seeing them happening and the press is also mentioning them. The biggest incident was on December 2015 when the Black Energy cyber attack on Ukraine's power grid left 700,000 people without electricity for several hours—an attack that we think was the work of Russian-backed hackers. Another element that stands out concerns the things that many people either predicted or could have predicted that we did not pay attention to. We have been very focused on the vulnerabilities of industrial control systems but while we were very aware of these vulnerabilities, we were not necessarily thinking about the full destructive potential of botnets and DDOS attacks.

In December 2015… the Black Energy cyber attack on Ukraine's power grid left 700,000 people without electricity—an attack that we think was the work of Russian-backed hackers.

In the past few weeks, we have seen a series of DDOS attacks against Dyn, the DNS provider, that caused internet services' disruptions and another attack that took down the internet in the entire country of Liberia. We talked about IoT as a being the major culprit. It is important to remember that developing regions, and notably the African continent, are in the process of coming online. For instance, in the past five years Ghana has gone from having only one undersea internet cable to having five that connect the country to the rest of the world. Also, a lot of machines in developing countries are either unprotected or under-protected, many of them without antivirus, which makes them highly susceptible to being compromised and recruited into a botnet network.

At AXA, we are thinking about scenarios involving new forms of ransomware…with the rise of IoT, you might have to pay a ransom if you want to get in or out of your house or if you want your car to start.

So while it is very helpful for us to look back at how things have evolved, I think it is even more important for this panel to be looking toward the future. At AXA, we are working on cybersecurity futures and we are currently doing scenario planning. I notice that there has been a lot of talk about IoT at the workshop, but cloud computing has not been mentioned much. This is something that we think a lot about. A number of companies are increasingly moving to the cloud, a move that means an increase in efficiency and many benefits, but it comes with a large number of vulnerabilities as well. So we are working on both positive and negative scenarios involving the cloud. We are also thinking about scenarios involving new forms of ransomware attacks. For example, with the rise of IoT, you might have to pay a ransom if you want to get in or out of your

house or if you want your car to start. We have also raised some questions earlier today about the definition of critical infrastructure. If we do see these sorts of ransomware attacks starting to occur, does that mean that houses and cars should be part of our definition of critical infrastructure? And of course, we start to see the rise of smart cities. What about ransomware attacks that might involve shutting down public transport, for example?

To the extent that cyber challenges are predictable and that we can do proper planning, what can we do about these issues now since we are the ones in a better position to take action on them before it is too late? I would like to leave you with three questions to keep in mind for the questions and answers at the end of this panel:

- First, we predicted that attacks on critical infrastructure will become commonplace and this is in the process of becoming reality. What actions can we take today to mitigate this?
- Second, are there other things that we are simply not paying attention to? What do you see in the current landscape that may become a clear challenge in the future?
- Third, what are your predictions for 2017 and beyond?

The Importance of Best Operational Practices, from Life Cycle Management to the Positive Effects of Critical Infrastructure Regulation

Mr. Alain Fiocco
Senior Director, Chief Technology Officer
Head of Paris Innovation & Research Lab, Cisco

Attacks on Domain Name Systems (DNS)

Let me go back to basics and give you just a few data points. Since we have been talking about attacks on the Domain Name System (DNS) lately, I will use the internet as a critical infrastructure to give you examples. The DNS system is the system that allows you to type into your browser the name of the website or resource that you want to get to—such as www.cisco.com—and that system will return to you an IP address,[7] which might be something like 72.163.4.161, that you wish to connect to. It is very foundational but actually quite fragile and brittle. Years ago, the engineering community came up with ways of signing and securing zones and domains in the DNS system. The first domain was officially signed in 2003 and we are in 2016. Do you know what percentage of domains is actually signed on the internet? Only 14% of the domains are actually signed, which indicates that, even though there is no more critical infrastructure than the DNS system, it is lacking a minimum of basic hygiene. The entire internet is running on it and yet it is still completely unsecure. The hijacking of the domain resolution system is the reason why Dyn was attacked by a botnet a few days ago and a very large proportion of the internet users could not access the services that they wanted to get access to.

Hackers can steal your domain and redirect you to a website that, instead of being yours, is somebody else's website and they can steal a lot of critical information.

In Europe, we pride ourselves on doing a better job. 19% of the domains are signed and it is about the same number in the US. So 80% of the domains in the European internet are not even signed, which means that they are subject to attacks such as domain poisoning or similar things. Hackers can steal your domain and redirect you to a website that, instead of being yours, is somebody else's website and they can steal a lot of critical information. The same thing is true for all kinds of critical infrastructure systems, such as the routing system, which discovers topologies and makes the internet function as a packet switching mechanism. A routing best practices was published almost 15 years ago on how to best secure the routing system on the internet. The level of adoption of that basic technology is in the same range as for the DNS system, below 20%. So there are some very basic informational resources that need to be put in place. It is not a matter of technology necessarily. Sometimes it is just a matter of turning on and building the operational practices around those technologies.

For routing best practices, the level of adoption is in the same range as for the DNS system, below 20%.

[7] If you type the IP address 72.163.4.161 into the search box of your browser, it should bring you to the Cisco.com website. This is how the DNS system works.

Basic Hygiene for the Internet

Another issue, which few people talk about and also concerns basic hygiene, is how to do life cycle management. Let me give you another example. You may have heard that TV5 Monde[8], a French TV channel, got hacked about a year ago. The hackers hacked into the very core of the TV channel, which was the media production infrastructure where they were creating content, TV shows, and news. As it turned out, this company was actually using a media production server that was running on twelve-year-old software. This software had never been updated and the password had not been changed on the system. For the attackers, it was a very soft target. This is not how they got in, but it is what they targeted and they brought down the entire channel for several days. The message here is that we sometimes tend to think that attacks are very complicated things that are super sophisticated. In fact, most attacks target very weak and brittle infrastructure that has not been upgraded and does not have the best operational practices. Hygiene is the foundation and we tend to forget that far too often.

Most attacks target very weak and brittle infrastructure that has not been upgraded and does not have the best operational practices.

[8] This attack has been attributed to the Russian APT28 group, also known as Fancy Bear, which is believed to belong to the Russian Military Intelligence group GRU.

The Economics of Cybercrime

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

Cybercrime's Impact is More Important than "Who did it?" and "How?"

Last year, I talked about critical infrastructure, and I am happy to admit that I was actually quite wrong. At the time, we had a set of predictions showing that the probability of attacks on critical infrastructure was quite low, because we had only previously seen the attacks in Iran and in Germany. But on 23 December 2015, we saw a news report from the Ukraine about an attack taking down the power grid. We were subsequently able to get the malware samples and do research on them. What this demonstrated to me was that, as a community and as a society, we have failed to answer the fundamental questions associated with this new digital threat: whenever a major attack breaks news, the only two things that we generally care about are "who did it?" and "how did they get in?" The reality, however, is that these are not the fundamental questions that we should be asking. The biggest issue that should concern us today is the impact—and not only the impact on victims but equally on society as a whole.

Impacts on Customers, Profits, Health and Research

Earlier this year, when a major telecom in the United Kingdom was compromised, it lost 95,000 customers, which represented a significant economic impact on the organization. Last week, we had a ransomware attack against a UK hospital, and it had to cancel scheduled operations and transplants. This huge impact on operations and health is far more important to us as a society than "how did they get in?" or "what form of ransomware was used?" This morning, we have been chasing down a breach against a large United Kingdom bank: 40,000 customers seem to have been impacted with money stolen from their accounts. Yet, the only thing we worried about was "which email did somebody click on to allow them in?" We are actually seeing huge amounts of similar thefts across multiple industries and multiple verticals. In a research paper that I recently co-authored, we demonstrated and showcased the example of a major pharmaceutical company whose intellectual property is being stolen by actors whom we believe to be state sponsored in order to further another nation's economic interests related to oncology research. This is having a huge impact on such firms that are unable to realize the benefits and the opportunities that their research should permit. We call this the "lost opportunity impact." Not being first to market impacts these organizations' profitability as well as the amounts that they will be able to reinvest for research and development.

Cybercrime has a significant economic impact on organizations… we call that the "lost opportunity impact."

In fact, cybercrime has national impact. A few years ago, we did a report with CSIS in order to understand the economic impact of cybercrime on major countries across the world. It was remarkable that Germany came out on top of the list. Of course, you would not be

proud of being on the top of such a list, but the impact on the German economy was equivalent to 1.29 % of GDP, which is significant. Now what does this tell us? Is Germany targeted more than any other country? Or is it that Germany, unlike other countries, has a fairly robust reporting system for cybercrime. Of course, it is the latter and, in fact, another remarkable thing is that we found countries, such as Argentina, that fail to even report digital crime. The seemingly good news for Argentinians is that cyber crime represents 0% of GDP. The reality is that they are simply not reporting it. Perhaps our greatest concern was that we did not find a single country that had done studies to determine the economic impact that these digital threats are having upon their societies and upon their economies. While we often talk about cybercrime as more lucrative than the drug trade, there is scant evidence to show the actual size of cybercrime's impact.

Cybercrime has national impact… but there are countries, such as Argentina, that fail to even report digital crime.

Since no one really considers the impacts, we need to focus our efforts upon them because the threats that we witness are increasing exponentially. Caroline Baylon talked about the Mirai IoT botnet. This is remarkable, because we used to think of IoT as the attack target, and now it is the attack vector. The most telling thing about Mirai is that anyone of us can rent that botnet for about $7,500, which offers 100,000 compromised IoT systems that can be used to attack any infrastructure of your choice for an entire week. Caroline also talked about ransomware, and we actually highlighted and demonstrated the vulnerability of automobiles at Las Vegas this year. We actually introduced ransomware into connected cars. Yet, the scary thing was that, when we contacted the manufacturers of these vulnerable devices, they did not even respond. They failed to even acknowledge the fact that we had found vulnerabilities in their environment, despite the fact that the threat landscape is making it easier for anybody to conduct such attacks. When we did a study in the health field, we identified cases where medical data were being stolen by criminals. In fact, I asked my 11 year-old-daughter to go out and find some examples for me. That is how simple it has become: an 11 year-old child can go out and find stolen data.

The Economic Impact—the UK's Approach

The economic impact is what matters. The UK cyber security strategy was published last week, and they have announced that they want to ensure that the UK is the safest place for any business to operate. In other words, they see cyber security and a safer digital society as a key Unique Selling Proposition (USP) to attract new business onto their shores. It is a fact that the economic growth of any nation depends on its ability to safeguard its assets. Those assets may or not be digital, but they will be absolutely dependent upon digital services.

Protecting Critical Infrastructure from Cyber Attack

Dr. Lin Wells II
Advisor, Georgia Tech Research Institute
Former U.S. Assistant Secretary of Defense (acting)

When we talk about types of critical infrastructure, we often talk about power, water, transport, but the US actually recognizes 16 different critical types of infrastructure. They include things like food, security, critical manufacturing—which covers the 3D printing world—health care, financial services, and voting. However, the responsibility for protecting all these different types of infrastructure is allocated to different ministries, which means that they will be stove-piped. In the US, there is an infrastructure protection division within the Department of Homeland Security (DHS) that is trying to do this coordination. We found interdependencies and cascading casualties across infrastructures, particularly in the case of Hurricane Sandy, with power fuel and communications. For example in New Jersey, there were gasoline stations that had gasoline but no power to pump it; there were stations that had power but no fuel to pump; and there was no way to work across the infrastructures to know what the interconnections were and how to fix them.

The US recognizes 16 different critical types of infrastructure … but the responsibility to protect them is allocated to different ministries, which means they will be stove-piped.

How can we deal with those crosscutting issues? One thing to keep in mind is the velocity of technological change. If some parameter, for example computing power per unit cost, is doubling every eighteen months, in a year and a half, you will get 100% more capability, but in five years, it will be 900 % more capability. I do not know whether the velocity of technological change will continue to increase, whether it will level off, if it will accelerate, or whether there will be step functions through quantum computing. However, the point is that linear projections based on where we are today are not working—at least in the government programming, because they take where we are today and double it in a couple years, but it is not going to be that way.

Every year, I go to Black Hat and Defcon, the hacking convention in Las Vegas, and IoT has been a fairly important subject for the past two years. The problem with IoT is that there is no demand in the market place for security: it is all functionality and speed to market. I am reminded of where we were in 2005 and 2006 with the financial markets. A great deal of money was made in subprime lending and derivatives, with no one understanding the underlying risks. I think we need to think of this issue as almost society-wide, because it is really a fundamental problem. How can we do this? There has been some very interesting work done on planning and engineering for resilience. It points out, first of all, that this work needs to involve the whole society: it cannot be just the techie; it cannot be just the government. It has to be public/private, whole of government and transnational.

The problem with IoT is that there is no demand in the market place for security: it is all functionality and speed to market.

You have to deal across multiple domains—the physical domain, the cyber domain, the human domain—with the temporal dimension added to all this across those different dimensions.

Scenarios have to be thought of in the right context. It is not just the random hacker out there doing something. Threat, resources, political will and velocity of tech change are what you must consider in your analysis. If you think about the risk, look again at the interdependencies: what are those interdependencies? What are the pathways into the systems? At Defcon last summer, a demonstration showed 8 different pathways into a SCADA system, and the SCADA infrastructure worldwide is pretty much hopelessly broken. So how can you begin with a good base? Who are the stakeholders? What are the stakeholders' perceptions? Raj Samani pointed out the impact on societies: what are our populations' mental models for how they will respond to these various attacks? Will they think it is just hackers doing standard attacks or will they see these attacks as having a fundamental impact on their way of life? And when you work on these scenarios, you need to combine training, exercises, education, and incentives to change behaviors because, frankly, you never learn a lesson until your behavior changes. When a crisis comes up, you observe a lesson. For the next crisis, you re-observe the same lesson. How can you put together a combination of training, exercise, education, and incentives to cause people to do things differently? We say act early because the cost of doing something at the beginning is vastly less than the cost of remediation later.

When you work on these scenarios, you need to combine training, exercises, education, and incentives to change behaviors because, frankly, you never learn a lesson until your behavior changes.

Going back to some of the lessons from Defcon, there was a lot of emphasis on speed. At this workshop, someone mentioned earlier how long it takes to detect and to patch malware. Cisco has a really good mid-year security report in which they talk about 150 to 200 days to detect malware if you have it on your system. In some cases, approximately 20% of the devices Cisco looked at had malware that had been there since 2012. Also, once you detect the malware, it takes an equivalent amount of time to patch it. So it is not just finding the malware, it is getting the company to act to fix it once it has been found. Last year, I looked at hypervisors and the vulnerabilities of software to find radios and software to find networks. Caroline Baylon mentioned the Cloud. There are serious vulnerabilities, particularly in hardware, firmware and hypervisors that need to be thought through in terms of this new path to protect. This is a multi-faceted problem that has to be handled across many different domains. At the same time, there are opportunities. One thing that has really come out is this issue about boundary control points and segmented enclaves. Last year, Tesla offered up a model that they asked to be hacked. The hackers came back and said that the car had some vulnerabilities, although they thought it had actually one of the better security architecture they had seen. What they had done was to segregate the infotainment local area network from the controller area network that runs the car with an untrusting bridge to manage certificates and encryption to pass messages between; then, you can patch it over the air. It might be possible to put that kind of model as a wrapper around some of these vulnerable SCADA systems and other similar systems as well.

The United Nations Security Council and the Protection of Critical Infrastructure from Cyber Attack

Dr. Aníbal Villalba
Senior Adviser to the President, National Cybersecurity Council of Spain

I would like to present a different approach to cybersecurity and the protection of critical infrastructures within the United Nations system, especially within the UN Security Council. Several times during this workshop, we heard that the UN should have a leading role in cyberspace when cyberspace has an impact on international security. We fully agree with that. So far, the UN has made several efforts in that direction and Ambassador Martinon spoke about the work of the UN Group of Governmental Experts (GGE) that is going to meet for the year 2016-2017 and will provide a report. I feel very privileged to have worked in the last edition (2014-2015) of the GGE group. This is a great opportunity to exchange ideas, in a discreet manner, with important actors during meetings in Geneva and New York under the umbrella of the UN and to discuss the impact of cybersecurity on state behavior. It is also fantastic to come to an agreement and to have a common understanding of things as important as the conclusion that international law is applicable to cyberspace. This is a major step. The way the UN works is that it selects countries—20 countries in the last edition and 25 countries for this one. Each country in turn selects a Governmental Expert that is supported by his/her government to provide a report that should be independent because it is signed by each one of the experts, not by the governments. The report then goes to the UN Secretary General, normally by summertime, and the Secretary General presents it to the UN General Assembly during its annual session in autumn.

The UN Group of Governmental Experts (GGE) is an opportunity to … discuss the impact of cybersecurity on state behavior.

Spain supported this approach of incorporating cybersecurity in the UN system with the thought of going one step further and finding a way to involve the Security Council, which has the leading role on international security for that. We will finish our membership in the Security Council as a non-permanent member by the end of the year, and our agenda includes the plan to bring cybersecurity to the Security Council's agenda. We talked to different members, US security members, EU members as well as other officials and actors, and proposed a meeting that will take place on November 28 under the umbrella of the Security Council. It is an informal meeting and our chosen topic, which was accepted by the Security Council, was the protection of critical infrastructure from cyber attacks. This agenda was accepted for a number of reasons. First, critical infrastructure protection was included in the report of the GGE 2015 as one of the major threats to international security. Second, we also discussed with different actors the fact that cyber attacks to critical infrastructure do not come from hackers or hacktivists or even terrorist groups. These are very complex attacks with advanced persistent threats (APTs) that can only be supported by states and, of course, they have an impact on the behavior of states, which is the core business of the UN. So we proposed an "Arria Formula

Spain's goal is to bring cybersecurity to the Security Council's agenda.

meeting"—Arria was a diplomat from Venezuela who, when he was chairing the Security Council, used a different approach to talk about topics that other actors were not willing to discuss formally within the Security Council. Thanks to this format, you can talk freely, there are no records kept, but you can discuss sensitive subjects such as terrorism before they go to the Security Council.

The meeting is open to every UN member. We also want to include organizations like the OSCE because they are working on cybersecurity confidence-building measures, and the European Union in particular because of its July 2016 Directive on the Security of Networks and Information Systems (the NIS Directive) that European Union countries have to implement in the near future. This directive, which requires member states to establish a network of Computer Security Incident Response Teams (CSIRTS) with the obligation to share information, is quite revolutionary and will completely change the map of cybersecurity within Europe.

Cyber Warfare as the Fifth Battlespace

Mr. Don Proctor
Former Senior Vice President, Cisco

"Cyber Warfare as the Fifth Battlespace" has come up several times over the course of the workshop. I would like to return to two comments that were made yesterday. General de Courrèges d'Ustou talked about "strategic disruptions" and we are certainly living in a world of strategic disruption, not only in the world of cyber security, but in the real world too as the tragic events in Paris, Brussels, Madrid, London and other places over the years have shown us. I also learned a new term during Admiral Coustillière's presentation. He used several times the term "espace numérique"—or digital space—something that we are talking about today. Since the esteemed panelists following me are the subject matter experts on this topic and have prepared their remarks, I will just submit a couple of seed questions:

- My first question is intentionally a bit provocative: is cyberspace truly the fifth domain? We seem to take it almost for granted that it is the fifth domain, but is it something different? We know that cyberspace is borderless in many ways. Is it a commons or is it something that is more closely tied to national sovereignty? While cyberspace itself is generally borderless, the equipment, the routers, computers and switches that make up cyberspace are physically located in countries around the world. So, there is an interesting interplay between whether it is a new domain or whether it is an extension of an existing domain.

Is cyberspace truly the fifth domain? And is cyber warfare still distinct from kinetic warfare?

- The second question is whether cyber warfare is still distinct from kinetic warfare? I have heard the term "hybrid warfare" several times in this conference, and we are perhaps living in a world of hybrid warfare where you may have kinetic responses to cyber attacks or cyber attacks that precede kinetic attacks, and it strikes me that the lines are starting to blur.

Finally, we may be able to talk about a question that came up in the last panel: "Are we collectively and independently organized properly for both defense and offense in cyberspace?" This question led to an interesting dialogue about law enforcement versus national security.

Cyber Warfare as the Fifth Battle Space

Ambassador Jiri Sedivy
Permanent Representative of the Czech Republic to NATO, former Minister of Defense

When the very first NATO cyber security policy was drafted and adopted in Tallinn in 2008, I was the NATO Assistant Secretary General for Defense Policy Planning, chairing the working group that was responsible for cyber. We visited the embryonic NATO Cooperative Cyber Defence Centre of Excellence that Sven Sakkov now directs, and we were briefed on the cyber attack against Estonia the year before. This helped finalize the NATO cyber security policy, but it was only a general framework. It defined terms—such as "cyber security" or "cyber defense," and it was a "soft" but important initial step toward the institutionalization of cyber defense in NATO. In fact, the mere mention of collective defense or article 5 in the context of cyber security was completely new. This point is worth emphasizing, because it illustrates how fast cyber has been developing in NATO.

Despite the agreement that a cyber attack could possibly trigger article 5, there is still no clear definition of what this could mean.

Despite the agreement that a cyber attack could possibly trigger article 5, there is still no clear definition of what this could mean. NATO experiences some 200 million incidents on its networks daily and faces perhaps millions of various attempts of cyber harassment, with around 200 intrusion attempts monthly that are even more serious. China and Russia are the main sources. At the same time, I would not say that we are necessarily on the verge of a cyber war. Our adversaries are trying to get into our networks and to compromise the security of our information but, above all, I believe that they are testing us and seeking vulnerabilities. The Warsaw Summit gave a great push by adopting the Cyber Defense Pledge and recognizing cyberspace as an operational domain, in which NATO will plan, train, operate and develop capabilities, and defend itself in that area.

The Importance of Cyber within NATO's Deterrence and Defense Posture

The NATO cyber mandate is above all defensive; NATO as such is not going to develop its own collective cyber capability to conduct proactive operations in cyberspace. However, the Alliance will integrate cyber defense capabilities into the NATO Force Structure through the NATO Defense Planning Process (NDPP). This means tasking the Allies to develop appropriate cyber capabilities on the national level and also integrating cyber into planning for joint operations across all other domains. It also means integrating cyber operations into our deterrence posture. Ultimately, I believe that the Allies need to change their binary way of looking at cyber and see it as a vital deterrence tool. What kind of deterrence effects can individual allies achieve through coordinated operations in cyberspace? I do not think that a cyber attack always requires an identical counter-cyber attack. Deterrence is not limited to the movement and staging of troops and physical assets. The use of offensive cyber operations remains, however, subject to constraints. They are mainly legal—similar to the use of any kind of military force, but also specific to the cyber domain: any proactive cyber

capability is basically a tool for one-time-use since it involves disclosure of the exploited vulnerability. Eventually, NATO will have to consider the development of a comprehensive Cyber Defense Military Doctrine, which will assure the integration and usability of cyber defense capabilities across all domains.

The Development of Capabilities at the National Level

Since NATO has no collective cyber defense capacities, it relies heavily on the capabilities provided by individual Allies, including offensive capabilities. Approximately 95% of the NATO capabilities are developed in the nations and owned by the nations. It is the responsibility of individual allies, in line with Article 3 of the Washington Treaty. The defense ministers have recently adopted metrics to measure the implementation of the Cyber Defence Pledge, which will be reviewed on an annual basis. The first assessment's results will be known at about this time next year. Only then will we have the first data on national cyber progress—or lack thereof. These results will be important because, on the one hand, there is a group of nations that have well developed and developing capacities, including proactive or offensive ones; on the other hand, some nations are not eager to invest in this area and are free riders, but no one should rely on the Alliance or allies to do their job.

Some nations are not eager to invest in cyber defense and are free riders, but no one should rely on the Alliance or allies to do their job.

NATO–EU Cooperation in Cyber

The good news is that the NATO–EU cyber relations are not starting from scratch. Since 2010, high-level staff-to-staff cyber defence consultations and informal meetings have taken place annually. The National Criminal Intelligence Resource Center (NCIRC) and the Computer Emergency Response Team-Europa (CERT-EU) have been cooperating since the creation of CERT-EU in 2011 recently signed a technical arrangement that establishes a critical response and coordination link. The EU has also been observing the NATO annual cyber defence exercise, "Cyber Coalition." Several informal cooperation initiatives have taken place between the NATO Cooperative Cyber Defence Centre of Excellence and EU agencies, namely the European Defense Agency, which has a robust training program in the cyber domain. We should encourage closer cyber cooperation between NATO and the EU, especially in the area of training, exercises, simulations and decision-making. Another critical area will be cooperation in cyber research and innovation: NATO in the area of capability development and planning and the EU in the area of training and R&T cooperation. This will also be an opportunity to strengthen ties with industry and the private sector, which is an important "cyber-stakeholder."

NATO after Warsaw: Don't Get Lost in Cyberspace

Mr. Sven Sakkov
Director, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)

Is cyber is a domain? This issue has been discussed by Dr. Patrick Allen and Dennis Gilbert[9] who suggest that a domain should meet six conditions:

- First, unique ability is required to operate in that domain
- Second, the domain is not fully encompassed by any other domain
- Third, a shared presence of friendly and opposing capabilities is possible in the domain
- Fourth, control can be exerted over the domain
- Fifth, a domain provides the opportunity for synergy with other domains
- Sixth, a domain provides the opportunity for asymmetric actions across domains

While this is a work done at the request of our CCDCOE center in 2009, I would like to comment on one of their points: even though cyberspace is in a sense borderless and limitless, its infrastructure falls within sovereign jurisdictions. So calling cyberspace a domain is actually not all that simple.

Observations on a Future Cyber War

At this point, I would like to offer a few points of my own, and then make some observations on the way forward.

- There will be future wars between cyber actors.
- It is unlikely that such future wars will take place only in cyberspace, although it might begin with a cyber attack.
- In any future war between capable adversaries, at least part of a war will be played out in cyberspace.
- In order to achieve our goals, we would want to be able to use all the various levels at our disposal including offensive cyber.
- There will be a pressure to use warfighting methods that are the least likely to result in civilian casualties and destruction. This is a political imperative.
- We would want to minimize risk to our pilots and special operators and, if possible, we would like to use methods that spare us from some of the risks.
- The West will fight in a coalition and the most likely coalition will be NATO, if it is a real fight. It is very hard to imagine that the UK or Italy, for example, would have their own independent military campaign without NATO and/or EU allies to partner.

[9] Dr. Patrick D. Allen, Johns Hopkins University, and Dennis P. Gilbert, Booz Allen Hamilton.

- If it is to be a NATO coalition, we want to have a coordinated effort across all domains of warfare between allies.
- To achieve that coordination in wartime, we need to prepare for it in peacetime.
- That means that we have to work out all the many related issues including conceptual ones. For example, is there such a thing as deterrence in cyberspace? I personally believe that deterrence is possible, but it works differently. It depends on (a) resilience, which is deterrence by denial; (b) the ability to attribute attacks and (c) the ability to retaliate i.e. to actually do something about it.[10]
- As has been said many times, we need to mainstream and operationalize our approach to cyber defence. As to the Alliance, what do we need to do?
- How does the decision to recognize cyber as an operational domain affect doctrine, organization, training, exercise and material, leadership, education, facilities and so forth.

Suggestions for the Way Forward

Strengthen CCDCOE. Although I may be biased, I believe that the first step should be to strengthen CCDCOE, which would be enormously valuable. At CCDCOE, we have representatives of seventeen allies and three partner nations, so eleven allies do not contribute to our centralized NATO research training, education and exercises. Of these seventeen allies who do contribute, eleven only provide a single researcher. This means that there is room for improvement, especially since the role of CCDCOE is not just to engage researchers, but, together with Allied Command Transformation (ACT) and several nations, we are developing NATO's cyber operation doctrine. We are also running the important legal framework project called the Tallinn Manual, and Tallinn Manual II will be launched in February. It is a study in international law and its applicability in cyberspace, which will inform EU and GGE discussions as well. We are a major training provider for NATO nations, and we are conducting the largest most technically complex international live fire exercises, called Lock Shields. This year, we had twenty teams, with about 16-18 people per team. Altogether, about 600 people were involved in this live fire technical exercise.

Improve Information Sharing among Allies. After strengthening CCDCOE, the next step should be to improve information sharing among the NATO allies. It is a touchy subject, but the NATO Intelligence Fusion Center (NIFC) in England already offers a successful example. In the intelligence field, people working together and building trust on a day-by-day basis (and having a pint after work) show that you can build trust and effectively share intelligence, which can then be fused and pushed out to NATO customers.

---

[10] As to attribution and deterrence, there appears to have been a remarkable drop in the Chinese commercial espionage against the U.S. over the past year, which seems to be the result of two developments: a US attorney attributed some of the attacks not just to China, but specifically to Shanghai Unit 61398 and four specific individuals. Another factor was the U.S. declaration in 2010 that it would reserve its rights to respond to a cyber attack in a time and manner of its own choosing, which would not necessarily be in cyberspace. Finally, Chinese commercial hacking against US companies stopped the moment the US government threatened to consider such cyber attacks as potentially constituting a trade war with China.

A Future Cyber Command. Eventually, we should consider whether there is a need for a cyber command. Dutch Ambassador Marjanne de Kwaasteniet alluded to this yesterday. The Warsaw Summit Communiqué recognizes cyberspace as a domain "where NATO will defend itself as effectively as it does in land and in the air and sea." In order for this to have real meaning, cyber will have to be done by someone and somewhere—which may require organizations and facilities. Of course, it will take many years, but we should all understand that another facet of warfare is being added. A cyber command will not be a silver bullet. War will still be messy. We will still need GIs in the mud and foreign legionnaires in the sand somewhere, but we need to understand that if we are to be relevant as an organization in NATO in the cyber field, we will eventually need something like a cyber command. In fact, our daily lives are more and more dependent on the internet and cyber, which amounts to a digital revolution that is disrupting societies. Today, the US elections are being held, with a lot of talk about the influence of angry, white, uneducated men. We can only imagine what the world is going to be like in twenty years, or even ten years. The US has 3.5 million truck drivers, 600,000 bus drivers and 300,000 taxi drivers. They will all lose their jobs to self-driving cars and trucks, but they are not going to blame themselves for losing their jobs, they will blame someone else.

The Need for an Adult Conversation on Cyber. In the future, cyber will continue to be disruptive and it will change societies. Cyber will change war, although not radically, and war will still be messy. This is why we need to have a normal adult conversation about cyber issues—including cyber offense. Cyber is not something that can be fired like tomahawk missiles, and code cannot be paraded like troops or tanks. When it comes to cyber offense capabilities, moreover, nations are likely to say that they don't do that or deny any knowledge of having such capabilities. Why? It is partly for deterrence and the desire to keep your adversary from knowing that you have certain capabilities that you can use to actually harm him if he harms you. Still, I think that these issues need to be on the table, and we should not shy away from discussing them.

The Challenges Facing NATO for Multi-Domain Operations (Integrating Space, Air, Cyber, etc. for Lethal and Non-Lethal Effects)

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

Several weeks ago, the U.S. Deputy Secretary of Defense commented about our dropping cyber bombs on ISIS, which amounts to an assertion that we are having a cyber effect on such things as ISIS's command and control. However, what he did not say is that we are seamlessly integrating cyber effects with our air and ground kinetic operations. This is a complex integration that is seldom achieved—and it is this challenge of multi-domain integration that I would like to discuss. Some of the comments made yesterday were *à propos:* Admiral Coustillière talked about the need for strategy, understanding, response, and freedom of action, and for responding with the elements of power. By that, I mean all the levers of government and international power and the levers of NATO. He talked about NATO's collective cyber defense, recognition of future requirements, and the blurring of lines in cyber for both civil and military infrastructure. The Dutch Ambassador to NATO spoke of cyber within hybrid war, NATO's aide to allies through hybrid activity, and SACEUR's reliance on members to deliver effects in collective defense. Moreover, we see that new connections and capabilities must be available for the active cyber defense of this alliance in militarily constrained operations or what we might call our new reality of Phase-Zero-plus. In US parlance, the active cyber defense activities in this phase will include Defensive Cyber Operations-Response Actions (DCO-RA), wherein the rules of engagement and policies for responding with a cyber effect against an adversary activity are the same as those for generating your own cyber offensive capabilities. Therefore, defensive cyber operations-response actions follow the same precepts as offensive cyber operations; both are challenging to execute because they are seldom practiced and have significant consequences if there is a "misfire."

Defensive cyber operations - response actions follow the same rules as offensive cyber operations; both are challenging to execute because they are seldom practiced and have significant consequences if there is a "misfire."

Getting back to today's panel, we must recognize that NATO must develop, integrate, and execute multi-domain activities. Cyber effects do not operate alone and SACEUR's intent, particularly when it comes to non-lethal effects, will require a coalition construct: bringing together member nation cyber capabilities and more importantly, varied national policies that afford their employment. From what I have experienced in command and control of these sorts of multi-domain activities, you physically join together in a single operations center, sharing a common operating picture, integrating capabilities—planning—execution, and sustaining the timing and tempo for commander decision. So, whether the headquarters for this sort of activity would be in Mons at SHAPE or at the Comprehensive Crisis and Operations Management Center (CCOMC), the way NATO comprehends militarily key cyber terrain and commands maneuver is very important. This is because you are going to need to

employ big data analytics to have the analyst-to-intelligence-officer-to-commander discussions about your courses of action, all of which are built on clear communication and confidence in your information.

As to Don Proctor's question, "Is this a domain or not?" there is always a place where we are in contact with an adversary. We are in sustained contact in cyber space and in our intelligence surveillance and reconnaissance, watching each other. We are also in contact at sea and, increasingly, in contact in the air, too often with "near miss" poor airmanship. And we are in contact via information—what we are saying to influence the adversary. It could appear that the only place where we are not bumping up into each other is on the ground, but the rotation of a Brigade Combat Team is certainly meant to send a message. The notion of domains notwithstanding, it is more useful to think of cyber as a cross-domain arena of overt and clandestine or stealthy contact.

At a recent CSIS forum in Washington, Secretary of Defense Carter wanted to talk about the significance of the "third offset." The third offset is not just about autonomy in our personal intelligence. It is also about operational innovation as well as technical innovation that permit full spectrum capabilities to be employed during a conflict. We are set to work with NATO to adapt a new playbook to address the challenge of hybrid war. When LtGen "Rooster" Schmidle was deputy commander of U.S. Cyber Command, he drove practical innovation by melding new operational concepts with useful technology—fortified by strong leadership intent. This is an acute advantage in cyber effects if we bring together an operational concept and new technology and accept a DevOps culture of rapid prototyping and fielding. Speed and agility are easy to say but hard to achieve—because often we are changing someone's way of doing acquisition. In making a shift, you do not necessarily require more resources since the stress of not having enough money is very good at driving innovation and the up-cycling of current technology.

Bringing together an operational concept and new technology for cyber also involves cultural change because you are going to change someone's way of doing acquisition.

Our discussion of cyber today has been almost in isolation, but it is a part of other activities—seeing each other, surveillance, signaling, messaging—all those things that go on every day. To deliver cyber effects, the fundamental requirement for NATO or its partner nations is deep technical understanding of intelligence on systems. In fact, it is now a matter of systems of systems: if we are talking about going against an adversary's systems to defend our own systems, it is not just network on network, or what they call "on-net" activity. More likely it is "off-net." In the US, we have separate cultures steeped in electronic warfare, electro-magnetic spectrum, and cyber. In pathfinder efforts, leaders are working together to characterize the landscape of cyber and influence campaigns, which they must do to either defend or deliver effects on the systems that we may need to affect in either non-lethal or lethal aspects. Also, there must be

To deliver cyber effects, the fundamental requirement for NATO or its partner nations is deep technical understanding of intelligence on systems.

knowledge about the adversary's tactics and, more importantly, the way the adversary thinks. Unfortunately, we have been lacking in understanding intent and messaging. Per recent studies on US-Iran relationship over the past twenty years, these was an inaccurate understanding of leadership intentions and how our "messaging" was understood by the foreign government and population. It hampered our diplomacy and international relations. We did not have a clear view of how they were thinking and, when they heard us, they may have completely misunderstood our message. Successful messaging depends on timing and the continuous assessment of whether it is having the effectiveness that you want to achieve.

A successful cyber effect operation depends on building trust with commanders who understand the risk equation and the level of confidence, as well as the battle damage assessment.

Similarly, a successful cyber effect operation depends on building trust with commanders who understand the risk equation and the level of confidence, as well as the battle damage assessment (and if it can be measured) of meeting the commander's intent. Or was there unintended collateral damage? More importantly, did it meet the overall intent of the military campaign? This kind of follow-through should be advanced because, to-date, we have not seen maturity in the cyber domain that is comparable to that of the physical domain. In fact, synchronization and integration of effects that intertwine and reinforce each other are very difficult. There are issues of the timing needed for the non-lethal effects that require greater finesse in our intelligence planning, our understanding of the target, and the deliberateness of an effect. You want to know if it is fungible, of limited duration, hard kill, or soft kill. All those things need to be identified because you don't want to overshoot or have needless overmatch.

Because the employment of multi-domain operations is still maturing, it is an opportune time for NATO to jump into the breach and look at how NATO will exercise these requirements. (I mean field exercises, not modeling and simulation due to the many assumptions made in simulation data sets.) The aforementioned examples also apply to NATO's use of flexible deterrent options, de-escalation and conflict, the ability to predict and red team the impact, and the likely response to activities. These opportunities are very complex. Being aware of the complexity helps us recognize what NATO will need to do to operate with multi-domain effects and speed-of-decision in command and control.

This analysis also applies to NATO's use of flexible deterrent options, de-escalation and conflict, the ability to predict and red team the impact, and the likely responses.

The Way Ahead for Europe and the Relationship with Russia

Ambassador Imants Liegis
Ambassador of Latvia to France; former Minister of Defense of Latvia

In order to focus on the geostrategic situation, I would like to move away from the important cyber issues that we have been discussing. We are living in a period of instability and uncertainty that has not been witnessed since the tumultuous changes between 1989 and 1991. To address these issues, our panel will look at two fundamental questions: (a) Europe's future and (b) our relations with Russia. Before handing over to our main speakers, let me say a couple of words to kick off the topics.

Europe

At the Bratislava Summit on 16 September, the twenty-seven European Union leaders met to consider the way ahead. In a challenging geopolitical environment for European Security and Defense, the objective is to strengthen EU cooperation on external security and defense. In December, the European Council will decide on a concrete implementation plan for security and defense including how to better use the options in the treaties, especially capabilities and how to start implementing the joint declaration with NATO immediately.

Various contributions towards these ideas have been put forward by different formats, such as the Visegrad 4, or the German-French "motor" (both with and without Italy). On security and defense topics, we have had joint démarches by both French and German Foreign Ministers and both Defense Ministers. While future decisions should of course be made by all twenty-seven Member States, there clearly needs to be a strengthening of EU internal security and steps are already underway to strengthen the management and control of external borders.

It will benefit all parties if the cooperation between the EU and NATO remains high on the agenda concerning issues such as cyber security, strategic communication and other ongoing hybrid threats. At the NATO Warsaw Summit, the EU and NATO placed cooperation as a strategic priority and the Presidents of the EU Commission and Council signed an unprecedented agreement with the NATO Secretary General about future areas of cooperation. However, there should be no duplication of EU and NATO work and the EU will of course continue to avoid engagement in collective defense, which remains the prerogative of NATO. The basis of European security must involve retaining the Transatlantic link.

Relations with Russia

Despite Ambassador Chizhov's arguments to the contrary, the root of today's problems lie in Russia's military intervention by annexing Crimea and continuing its actions in East Ukraine. These actions, as Assistant Secretary General Camille Grand stressed, have radically transformed the nature of the relationship and they have been exacerbated by

multiple large-scale exercises, sometimes unannounced, sometimes including nuclear elements, and often displaying a wide scale of capabilities on NATO's doorstep. President Putin has been able to surprise by acting with speed, as we saw both in Crimea and Syria, and Russia has the capabilities to conduct military actions simultaneously in Europe's East and South. Under the circumstances, the only premise for a return to some sort of business with Russia must be the full implementation of the Minsk accords and the return of illegally annexed Crimea to Ukraine.

The way ahead needs to be based on defense and deterrence as well as dialogue… but a dialogue should not necessarily be the only policy option.

The efforts of the Normandy Format have been welcome, but elections in France and Germany next year mean uncertainty vis-à-vis the continuation of the process. A united approach by the EU and NATO should be maintained and the consensus on sanctions between the US and the EU will be crucial. In any case, the way ahead needs to be based on defense and deterrence as well as dialogue. No efforts should be spared to maintain a dialogue so as to search for ways to reduce risks and build confidence. Nonetheless, a dialogue should not necessarily be the only policy option.

The Common Foreign and Security Policy after Brexit

Dr. Ioan Mircea Pascu
Vice President of the European Parliament
Former Minister for Defense of Romania

Post-Brexit, the EU's Common Foreign and Security Policy (CSDP) is evolving, but for many reasons in addition to the Brexit vote. The new security challenges, by their very nature, are bringing external and internal security much closer together. At the same time, the EU appears to be shifting away from its long-time focus on operations, the management of conflict and crisis management, in order to develop a true and authentic common security policy which will necessarily mean working more closely and effectively with NATO.

For hundreds of years, the major tenet of Britain's security has been to control developments on the European continent so as to prevent threats to its own territory and interests. As a result of the Brexit vote, however, Britain has stepped away from a splendid framework within the EU from which it benefited tremendously for a long time. It will lose a great deal of its influence, which implies the abandonment of its principal tenet. Most likely, the "Brexiteers" were hoping for a "good run" and to make a strong political statement, but they were not seeking victory or even desiring one, and they were caught by surprise when it actually happened. Unfortunately, this brings to mind an old saying, "When the gods wish to punish someone, they answer our prayers." I would like to be clear that am I not judging, but simply pointing out the actual facts.

Brexit brings to mind an old saying, "When the gods wish to punish someone, they answer our prayers."

There are already unintended consequences, including many that will not be apparent for some time. It is a fact that the Brexit vote has already affected the TTIP trade negotiations with the US—even though we Europeans had been negotiating with the City, London's financial district, in mind. Brexit has also weakened the ability of Europe to present a united front on sanctions against Russia. Militarily, the UK's departure reduces Europe's military capability by 25%, since Britain has the EU's largest and most capable defense capabilities. Fortunately, there is also a positive side: the Common Security and Defense Policy (CSDP) may be able to advance more easily since Britain's presence in the EU has been the largest single obstacle to progress. Now the CSDP has to become truly a CSDP.

Militarily, the UK's departure reduces Europe's military capability by 25%, since Britain has the EU's largest and most capable defense capabilities.

Until now, CSDP has been mainly "crisis management" operations and only France and Britain have been "expeditionary" powers by excellence—which was required by their history as colonial powers. Fortunately, France can be expected to maintain it expeditionary dimension, and Germany is steadily—but slowly—increasing its defense expenditures and commitments. Yet, Germany will remain, like Poland, a continental power. They may substitute somewhat for the loss of Britain. Italy, of course, is a Mediterranean and naval

power, rather than a truly continental one, which means that it will need to focus on the continuing refugee crisis, a major challenge, and it will be less interested in development in Ukraine or even the relationship towards Russia. With luck, we can expect a balance between the expeditionary and continental ambitions and capabilities of the EU countries.

Britain is expected to make up its "loss" by getting more involved in European affairs through NATO. For example, the UK—after completely neglecting Eastern Europe for a very long time—will station fighter planes in Romania for four months starting in 2017. One question, however, concerns the future attitude of Britain towards increased cooperation between NATO and the EU. Given the EU's hard negotiating stance over Brexit, Britain can hardly be expected to be generous in providing military support to the EU. Will it play a role similar to Turkey's—by being in NATO but not in the EU? What will matter a great deal is the way the divorce negotiations take place in defining the future relations between the EU and Britain, and there are two schools of thought: either rapid or slow negotiations.

Given the EU's hard negotiating stance over Brexit, Britain can hardly be expected to be generous in providing military support to the EU.

In any case, we should all realize that Britain's departure from the EU will weaken Europe, but it won't make the UK stronger—quite the contrary. As to the EU, a greater defense effort will be necessary. Fortunately, there are two promising developments, which may appear small by themselves, but are actually quite important since they signal fundamental change and progress. One important step is the EU defense fund (the pilot project run by the European Defense Agency and the Instrument contributing to Stability and Peace (IcSP) which will provide support for essential research and procurement. Another is the decision that EU funds, under strict conditions, will be able to support armed forces when EU goals cannot be achieved without security. These are important steps forward.

The Future Relationship with Russia: "To Contain or to Refrain" Is that the Question?

Ambassador Boris Grigić
Permanent Representative of Croatia to NATO

First, let me emphasize that I am speaking here on my own behalf although the fact that I have been sitting on the North Atlantic Council for over four years may have somewhat influenced my thoughts.

I will paraphrase an old saying from the Balkans to describe the actual relations between Russia and the West: it is not the Cold War but the roses are not blossoming. We know how we arrived at that point. What started with armed and masked green men without insignia who took control of Crimea's public buildings ended with the Russian Federation's illegal annexation of Crimea. It continued almost immediately with actions by Russian forces in Eastern Ukraine that created yet another conflict with good chances of becoming frozen. This kind of activities is nothing new when it comes to Russia. What happened in 2008 in Georgia and before that in Moldova is very similar.

President Putin openly stated that the collapse of the Soviet Union was "the greatest geopolitical catastrophe of the [20th] century." Everything after that can be seen as Russia's concerted efforts to regain global power status.

None of this should come as a surprise. In early 2005, President Putin openly stated that the collapse of the Soviet Union was "the greatest geopolitical catastrophe of the (20th) century." Everything after that can be seen as Russia's concerted efforts to regain global status power, gain control over its neighbors, and even regain some territories that belonged to the USSR. Russia calls it "near abroad" or "zone of exclusive interest." The fact that it is talking about sovereign states does not seem to bother it too much. At the same time, Russia is accusing the West of "not taking Russia's interests into account," be it in Eastern Europe or in the Western Balkans, and thus of automatically being against Russia. It is as if what Russia declares as its interest should automatically become a Holy Grail or a "don't touch" zone. So, if Russia does not like the EU enlargement, there should be no EU enlargement? Or, if Russia does not like the NATO enlargement, there should be no NATO enlargement?

The West does not think in terms of "near abroad," "spheres of influence," "right to dominate," "right to dictate alliances," etc. The NATO and EU goals are not to create their spheres of influence, they are not claiming exclusive rights over any country or region, either in the near abroad or farther. Their goal is to create a sphere without anyone's "influence," a sphere of the shared values of freedom, rule of law and human rights. All those who so decide can embrace and implement these values. And that goal by definition cannot be directed against Russia or anyone else. These values and ideas are behind NATO's enlargement policy. Every European democracy should be in a position to freely choose to join NATO. Since the fall of the Berlin Wall, many have chosen to do so, including Croatia. Some, mostly in Croatia's neighborhood of the so-called Western Balkans, are still on the

road towards NATO and the EU. All Croatian governments have strongly supported their choice to join the NATO family of shared values. It is in Croatia's best interest and Croatia is helping them to meet the standards and conditions for membership. That is also why we are concerned when we see external influences attempting to stop or slow down those processes with questionable means and methods.

Unfortunately, as I stated above, Russia has a different view. The Western Balkans is one of the areas in Europe in which Russia is in geopolitical competition with the West. The 2013 Russian foreign policy concept mentions the Western Balkans as a region of strategic importance for the transit of Russian energy to Europe. The main reason for Russia's interest, however, is the wish to project itself as a "great power" able to compete with the EU and the US, and to spoil Western plans. Russia is not in a position to offer a credible alternative to EU and NATO memberships but it tries to slow down projects that would bring countries from this region closer to the EU and NATO, and eventually make all the countries of the Western Balkans EU and NATO members. Russia questions and challenges the West's values, projects and ability to deliver on its promises; although its ambitions in this region are not the same as in its "near abroad," the methods are similar. And there is a problem with the methods Russia uses.

Serbs and Serbia

The main axis around which Russia is building its network of influence in the Western Balkans is its strategic alliance with Serbian people—in Serbia, Bosnia and Herzegovina, Montenegro, Kosovo or Macedonia. As the Mother state of Serbs, Serbia is Russia's most important ally. Russian links with some political parties in Serbia are strong and Serbia uses Russian help in dealing with the thorny issue of Kosovo's independence. Russian influence in media and civil society circles is carefully planned and managed, shaping public opinion favorable to Russian interests and spreading the "Russian truth." Cooperation between the two countries' intelligence structures is deep-rooted.

As the Mother state of Serbs, Serbia is Russia's most important ally… Cooperation between the two countries' intelligence structures is deep-rooted.

Before 2012 Russia and Serbia had very little or no joint military activities. Then in 2013 they signed a Declaration on Strategic Partnership and a bilateral military cooperation plan focused on improved military to military relations, increased exercise activities and procurement cooperation. The first joint military exercise was "SREM-2014" that was held in parallel with the Russian occupation and illegal annexation of Crimea. In 2015, exercise "Slavic Brotherhood 2015" took place in Novorossiysk with the participation of Belarus and in 2016, the Slavic Brotherhood exercise took place in Serbia with the same participants. These exercises are geographically the westernmost excursions of the Russian military. They should not be considered as a military threat to NATO or to its member states, but they are certainly a very strong signal. Russia is signaling that they have friends and influence in the Western Balkans, a region that is oriented—or considered to be oriented—only towards the EU and to a lesser extent to NATO. It is not quite clear how we should be

reading the signal Serbia is sending with such policy: as a sign that the West is not its only option or just as a bargaining chip in its slow rapprochement with the EU, which is burdened with the problem of Kosovo's independence and a rejection of facing the truth about what happened in the Balkans in the nineties? Interestingly, Serbia's increased military cooperation with Russia started more or less at the same time as its negotiations with the EU. Obviously, it has something to do with the geopolitical competition in the Western Balkans. What is also interesting is that both military exercises contain the word "brotherhood." Russia is clearly trying to exploit the traditional cultural, religious, historical and Slavic elements that connect two peoples and two states. Serbia is the strongest link in Russia's "soft campaign" in the Western Balkans.

Both Russia and Serbia see themselves as "protectors" of their peoples living in neighboring countries—even to the extent that they are ready to attack, occupy and, if possible, annex parts of other countries.

There is another similarity between Russia and Serbia that is not mentioned very often but is very important in this context. Both countries see themselves as pivotal, dominant in their surroundings. Russia sees itself as a global power and Serbia sees itself as a regional power. Both countries see themselves as "protectors" of parts of their peoples living in other, especially neighboring, countries even to the extent that they are ready to attack, occupy and, if possible, annex parts of other countries on the pretext of protecting their "brothers and sisters."

Bosnia and Herzegovina

In Bosnia and Herzegovina, Russia exploits the same traditional links as in Serbia. Through the Republika Srpska, Russia is manipulating Bosnia and Herzegovina's road towards the EU and NATO. Due to the very complicated Dayton structure of BH, each of the three constituent peoples—Bosniaks, Serbs and Croats—can stop or complicate every decision required to implement the reforms that would bring the country closer to the EU and/or NATO. And Republika Srpska can stop political or economic decisions that could be against Russia's interest such as the decision to join international sanctions against Russia because of its illegal annexation of Crimea and its activities in the Donbass region. The latest example of the political manipulation in BH is a referendum on Republika Srpska Day that was called by President Milorad Dodik. Despite a ban of the referendum by the BH Constitutional Court and objections by the EU and the West, the referendum was held with strong political support from Russia. Just a few days before the referendum, President Dodik had been received by President Putin in Moscow. This failure to prevent the referendum could be seen as a worrying sign of Western decreasing influence and Russian stronger infiltration/influence in BH. It reinforced Russia's image as the protector of the Serbian people, wherever they are. Unsurprisingly, Russia owns a big part of the gas and oil business in Republika Srpska and has significant investments in other sectors. All that is accompanied by close cooperation between Russian and Serbian intelligence and security services.

Montenegro

In Montenegro, which is now firmly on its NATO and EU path, Russia tried different tactics. Being the smallest of the Western Balkan countries, Montenegro may have looked at first like an easy prey. It had very close relations with Serbia shortly after the beginning of the dissolution of the Socialist Federal Republic of Yugoslavia ; an important population of ethnic Serbs (29% versus 49% Montenegrins) living in Montenegro; and the fact that these ethnic Serbs were mostly "unitarists," very attached to their Mother nation state, could only add to that impression. Russia significantly participated in the privatization of the Montenegrin economy and Russians bought a large number of immovable properties, especially on the Adriatic coast but they could not buy Montenegro. Then Russia offered one billion US dollars to get access for its military ships into Boka Kotorska bay, but Montenegro rejected the offer. Russia also financed anti-NATO NGOs during Montenegro's alignment process with NATO standards but the public opinion slowly grew more favorable to the membership in NATO. Russia's last action took place on 16 October 2016, on the day of parliamentary elections in Montenegro. Two Russians stationed in Serbia seemingly organized a coup attempt in Montenegro and/or planned to kill outgoing Prime Minister Milo Đukanović. They had recruited around twenty-five Serbs from Serbia to do the job. After the plot was discovered, the coup organizers were held in Belgrade under the control of Serbian services but they were allowed to return to Moscow after a visit to the Serbian capital late last month by Nikolai Patrushev, the head of Mr. Putin's Security Council and a former head of Russia's F.S.B. security service. No one has officially connected this action with Russian officials or services but the story is very disturbing.

Let me finally come to my starting point, the question of *"To Contain or To Refrain?"* I will answer this question with four points.

- First, although I was inspired by the verse from the famous English play, the question fortunately does not amount to the original one: *To be or not to be*, neither for the Alliance nor for Russia.
- Second, *To Refrain* - is out of the question, because that would betray the basic principles on which the Alliance is founded.
- Third, *To Contain* - to a certain extent it is already happening through different kinds of bilateral and multilateral sanctions, through different NATO activities and through different national activities in many countries that see themselves (indirectly) described in Russian policies.
- Fourth, the solution for today's situation can only be a political one. So, political dialogue between NATO and Russia, both focused and meaningful, should continue. To be effective, it has to be combined with NATO's strong deterrence and defense capabilities.

Cyber Intelligence—The Challenge of Determining Attribution in Cyber Space, while Balancing the Digital economy, Privacy, Security and International Public/Private Cooperation

Mr. Andrea Formenti
Founder & CEO, Area SpA

Experience with a recent Italian national security internet investigation highlights the limitations of our existing capability of attributing the actions of suspects in the cyber domain. The purely technical challenge can be solved using innovative and creative approaches and unconventional technology. Yet, efforts to make these capabilities available on a daily basis to the whole national security community—intelligence and law enforcement agencies—reveal a large and complex institutional gap that still needs to be filled.

First, I will say a few words about our company. Since 1996, we have been developing in-house cyber intelligence software-based solutions exclusively for national security, intelligence and law enforcement agencies. We have a strong background in Lawful Interception and Communication Data Retention Systems. One hundred percent of our technical portfolio is forensic proof; this means that it includes embedded capabilities and specific features in order to generate, not just actionable information, but technical evidence usable in a court of law. In Italy, thanks to our leading market position, every year a significant part of all the technical operations in criminal and national security investigation are performed by the national legal prosecutor offices using our systems.

A Recent Internet Investigation

In a recent internet investigation, we were told by the national authorities that they needed to have access not just to WhatsApp and Telegram but even to Zello conversations. Zello was developed more than a decade ago in Texas and is still relatively unknown in the United States. The application combines social media with telephone and push-to-talk (PTT) walkie-talkie radio functions. Bill Moore, the Chief Executive Officer of Zello, recently pointed out that "One of the features of the app is that it's anonymous, so of course it is also used by criminals and bad guys." At the present time, it is still nontrivial and perhaps impossible for an Italian legal prosecutor or the judicial police to have direct access to the communication contents generated through the Over The Top (OTT) application providers. It is even extremely difficult just to attribute a portion of IP traffic to a specific network subscriber or communication device, because neither the metadata nor communication data of the OTTs are available to the Law Enforcement Agencies. Additionally, the technique of sharing a single IP address among many users, which is implemented by internet service providers using carrier grade network address translation (CGNAT), can make it very difficult for the Internet Service

It is nontrivial for an Italian legal prosecutor to have direct access to content generated through the Over The Top (OTT) application providers … or just to attribute a portion of IP traffic to a specific network subscriber or device.

Providers (ISPs) themselves to respond to legal requests for logged or captured traffic. Usually those requirements are met by retaining traffic information to/from a specific IP address for a period of time according to the law. With IP address sharing, however, there is no unique user identification through a single IP address and this compromises the attribution process.

Therefore, we have studied and proposed a solution that can generate detailed IP metadata specifically intended for IP address resolution and backward correlation of subscribers' identity. It offers self-consistent information through a single, centralized device able to provide coherent and reliable data respecting the privacy in the resolution/process and including forensic proof data management and archiving. Our system is also technically capable of performing context awareness filtering and logging with dynamic recognition and detection of 200+ applications, but the existing national law framework still does not permit the use of this real time data processing feature.

Lessons Learned

In many cases, the lack of an integrated long-term strategy and the national budget constraints of some countries impose a simple reactive approach—merely case by case. Paradoxically, this sometimes facilitates the use of intrusive techniques and the exploitation of software vulnerabilities. Current laws too often limit innovative capabilities, not just because of privacy rights, but mainly because of the latency between the time it takes to make laws and the rapid evolution of the digital economy. Awareness and competence are key factors that are not always taken into proper consideration. Accordingly, I would like to propose several questions that we need to answer: is a company that sells vulnerable software legally liable? Is the zero-day exploit market illegal? Are fake news illegal? Are fake social network profiles illegal? Is there such a thing as an "Internet Jurisdiction"?

The Way Ahead

During this workshop, one of the most frequently heard words has been "attribution," the capacity to attribute actions to specific subjects in the cyber domain. We believe that the experiences and solutions developed during criminal investigations may contribute to the attribution requirement in the military context as well. As Sven Sakkov mentioned, there is increasing interest in the entire chain of evidence acquisition in the cyber domain in order to make an attribution reasonably credible before a court or a jury. Technically speaking, for example, passively monitoring IP backbones and collecting intelligent metadata may combine privacy issues with the growing needs of cyber security. On a higher level, we should start thinking of common rules for "Security and Privacy by Design," keeping in mind that the digital economy will continue to grow and evolve in years to come. Serious, structured and internationally regulated cooperation between partner nations and between the public and private sectors may mitigate today's cyber chaos.

We should be thinking of common rules for "Security and Privacy by Design," since the digital economy will continue to grow.

The Way Ahead for Countering the Growing Cyber Threat

Colonel Eric Freyssinet
Advisor to the Prefect in charge of the fight against cyber threats
French Ministry of the Interior

In our panel, we are considering future cyber threats. Several times during this workshop, we talked about Mirai, the malware that turns computer systems into botnets for large-scale network attacks. Mirai in Japanese means "the future" and it is symbolic that cyber criminals are thinking of the future, while we tend to look more at the present. We need to consider the future for countering cyber threats in general, because cyber threats are not only growing, as the title of our panel indicates, but they are also moving, evolving, etc. It is a dynamic domain and we need to find solutions that, from my point of view in the Interior Ministry, will lead to the arrest of the suspect of cyber crimes. With the help of all actors, we need to find practical, technical and legal solutions. Our panelists will try to address some of these solutions but, before turning over to them, let me say a few words on three different aspects of the problem.

Attribution. Of course, you cannot mix cyber warfare and criminal investigation, but, as was mentioned yesterday, most cyber attacks are actually criminal matters and there has never been a war based on cyber attacks. Criminal cases involving cyber have been in the news recently, for instance with the hacking of the US Democratic party for which a criminal investigation is ongoing. While the FBI is working with the intelligence services, it is the FBI that is actually working the case. We have the same situation in France, where there is also an ongoing criminal investigation on the hacking of TV5 Monde. In these investigations, we have several different issues to consider: where should we look, what should we point to, what should we be thinking about, and who should be the one to talk publicly about it. I am not sure the political level is always the best solution for communicating about the problem. A good example is the case of TV5 Monde; the prosecutor of Paris is the one who made a statement and his statement was quite balanced in the sense that he was not pointing at a specific country but pointing at a number of potential directions.

Most cyber attacks are actually criminal matters and there has never been a war based on cyber attacks.

Different Types of Actors. Over the past few years, there has been an evolution in the way that people view cyber threats. People used to point to countries such as China, Russia, North Korea, etc. as being responsible for hacking attacks. Now they are indicating specific actors inside some of these countries—or perhaps hackers working on behalf of an interest that is related to a country. This is a very different approach, which means that we are looking at different types of actors, and they are more typically related to organized crime. This means that the questions are the same as for criminal investigations. The whole process for

Instead of pointing to China, Russia, or North Korea as being responsible for hacking attacks…they are indicating specific actors inside some of these countries.

obtaining proof is exactly the one that we follow all the time. We have clues that lead us to pursue a number of potential directions; then we investigate these various directions and find more evidence; and, once everything is combined, we have a case. This means that if we have traces that point to potential groups of suspects, we will be fully convinced only once we have the suspects, their computers, as well as more information that tracks back to our case. It is not enough to have information pointing to them, because this information pointing to them could also come from others trying to point to them, and it could be another issue.

The use of intelligence. In criminal investigations, we can use intelligence and there is actually a whole arena of our activity called Intelligence-led Policing that is based on what we observe on the internet. We want to be able to look at malware as it is being distributed before there are victims, and we are targeting those distribution vectors, namely the people distributing malware before their malware causes actual victims. This is because it is really too late if you arrive further down the line. That line of thinking has helped us develop a strategy that we think is going to prevent crime rather than wait for a crime to occur and then investigate it, which is going to be too late.

We are developing a strategy that we think is going to prevent crime—rather than wait for a crime to occur and then investigate it, which is going to be too late.

Cyber Security—The Urgent Need for International Quality Standards In Source Code Writing

Mr. Daniel Maly
Senior Vice President and Country Manager, Cast Software

In my former role at Microsoft, I sponsored this event several times in the past. Currently, I am a Senior Vice President for Cast, a leader in structural software analysis that is looking at the structure and architecture of applications and software and finding the vulnerabilities and issues.

Software is like pieces of modules: think about a wall, which has bricks and cement. Usually, when developers work on an application, they only look at one brick but they do not see the entire wall or the cement in-between the bricks. What happens then is that you may be able to use certain tools to look at a specific code but you are missing the big picture. In 84% of the time hackers do not look at the bricks, they focus on the cement and structure of the wall, i.e., they look at the connections between the modules and the software. For example at your bank, an application can go from your android phone or your iPhone to a database in the background, and data flows from your device all the way through the bank into the back and verifies who you are. The vulnerability is not at this point sometimes, but in the transaction, and finding where those vulnerabilities are is what the hackers are looking for. It is that connection piece where humans have to make some modifications, just like a welder welds the pieces of metal together, that is where the vulnerabilities are. And it is very pervasive because if you remember earlier comments about the Las Vegas Black Hat convention where a 10-year old girl was able to find an exploit and got a prize for it, this is affecting Microsoft, Adobe, Google and all these multi-billion dollar companies who hired the best engineers and bought the best security and yet, they remain vulnerable. Now, imagine that you are a bank, you are the ministry of defense, or you are the automotive industry. You are buying SAP, Microsoft etc. and you are using system integrators to help you combine those. The system integrators mention that they have really good engineers who are expensive, but they also have 70% of their engineers offshore in India or Central and Eastern Europe. Without being disrespectful, the quality of the standards there is a less than in the West. So there is a trade-off between cost and accessibility and the reason why there are so many vulnerabilities is due to a lack of international standards for software quality.

The reason why there are so many vulnerabilities is due to a lack of international standards for software quality.

The exploits that are developed are an industry. You can find them very easily on the black market for different prices…

The other important point to raise here is that the exploits that are developed are an industry. You can find them very easily on the black market for different prices, zero-day, one-day exploits etc. The fact that these vulnerabilities are there and generate an industry is a clear sign that the problem is quite serious and on a massive scale. So my warning is that the Emperor has no clothes! We are all vulnerable—not only ministries of defense but

society at large. The citizens are exposed on such a level that it would cause chaos if they really knew how vulnerable they are. I am mentioning this so that you are aware of it.

At our Rodin museum tour yesterday, we saw the hands, torsos, bits and pieces of sculpture that Rodin created. When he wanted to sell his work, his metal casters would make replicas of his women, men and children sculptures and put them together. This is how a lot of software is done because, in a world where we are moving towards Agile and DevOps, which calls for engineers to work quicker, the pressure is for speed at the expense of security and quality. When these developers use the same patterns, the same software, and copy it into different applications instead of slowing down and putting more effort into quality, they are trading time for poor security and poor quality. From our side, since I get to work with banks, with the military and with the automotive industry, I see the same failures over and over. This brings me to a call for action on your part to use industry standards when writing software. A number of companies like MITRE and McAfee provide guidelines but you need third party organizations. The one I would advocate would be the Consortium for IT Software Quality (CISQ). In collaboration with the Carnegie-Mellon institute, they are trying to formulate international standards that should be used by every country and every organization to bring common sense and some basic concepts for the practices in writing software—what you should not use so that you do not allow hackers to get in so easily. Those standards would protect all users, which would be a very practical way to address the threat on a massive scale and should be advocated in academies, in schools, in procurement processes, and overall management. Currently, these rules are being used by the US, DoD, Veterans Affairs, State Department, NSA, MoD of France etc.

In a world where we are moving towards Agile and DevOps, which calls for engineers to work quicker, the pressure is for speed at the expense of security and quality.

Most systems in the banking and insurance industries are 15 to 20 years old. They were written in Cobol, a very old programming language, and now banks and the insurance industries are being asked to introduce Microservices. Microservices are accessing those data that are an antiquated technology created by engineers who have all retired. The programmers do not know the architecture, they do not know the language, and they are being asked to put a layer of software on top of the existing one, which is a complete disaster. This is why they would need to move more slowly but they are trying to go very fast. I will give you another example. We have talked earlier about the automotive industry, embedded technologies and the ability to hack into them and blackmail people. You may feel that you are protected because you are using the government email system but if a hacker wants to attack you, he could come after you or maybe your family or children who are using Facebook, collect information and start blackmailing you; he could also go after your bank and collect your information from a different perspective, making you completely vulnerable on a personal level. So the government and your accounts might help you but, on a personal level, you will feel the effects of that blackmailing and hostage situation. Hackers may wonder what is more effective: a government-to-government attack or targeting specific people and influencing them so that they can be bent to their will? That is the real threat and that is what we are not addressing at all.

Cyber Security Must Address Horizontal Threats, too

Mr. Kurt Westerman
Vice President, Business Development, ARES Corporation

ARES is a Risk Management and Mission Assurance company with a strong focus on the security of high value and high consequence targets. We approach cyber security from a different point of view than the typical IT company. IT companies are focused on the delivery of content and, over the past decade, have seen a significant increase in the need for security. ARES is a security company that has seen an increase in the need to include cyber. This different perspective can provide valuable insight into how we address the issues of cyber security.

Cyber Vertical and Horizontal Domains

Most of the discussions throughout this workshop have focused on the "vertical domain" of cyber, where the target of cyber crime is the IT system or network. These attacks include:

- Denial of Service (DOS)
- Theft of data
- Theft of money (Ransomware)

These vertical domain discussions are indeed important, but there are other equally important cyber crimes where the target is not the IT system itself, but rather the organization or facility that is using the IT system. In other words, cyber is a component of a conventional or "kinetic" attack. It is therefore important to look at cyber security from a "horizontal perspective"— the interrelationships between cyber security and other elements of security such as physical security or information security. From this view, we address the "cyber component" of our overall security plan. ARES area of expertise is the intersection of cyber attack and kinetic attack.

In cyber's vertical domain, the target of cyber crime is the IT system or network…In cyber's horizontal domain, the target is the organization or facility that is using the IT system.

As Jamie Shea pointed out in his discussion earlier in the Workshop, terrorists often have little to gain from a cyber attack on a network or IT system. The results of these attacks are generally short-term—a few hours or perhaps days without service—but they rarely cause the level of damage necessary to draw world attention to their cause. However, terrorists can use cyber as an *enabling component* for a conventional attack that could cause the type of damage and publicity that terrorists seek. For example, suppose a terrorist group sought to bomb a nuclear power plant to breach the reactor vessel and spread radioactive contamination across the countryside. Such an attack would have far greater consequences and last much longer than an attack on a network. However, a kinetic attack of this nature could include a significant cyber component, such as disabling security sensors and cameras or modifying access files to enable the terrorists to get inside the facility.

Where Cyber Security Can Learn from Conventional Physical Security

By looking at cyber security from a horizontal rather than vertical perspective, we find areas where cyber security can learn from conventional physical security and vice versa:

- *Technology advances have made physical security systems more and more dependent on IT systems.* Most physical protection systems now operate through a network server that integrates sensors, cameras, and communications. Wired sensors and cameras have been replaced by wireless sensors and cameras. An adversary no longer has to locate and cut a hardened wire to defeat a sensor. These advances brought significant improvements to the overall physical security posture. For example, video signals can be sent directly to the response force and viewed on a smartphone, thus enabling the guard force to see an area before they rush in. However, a savvy adversary could intercept that signal and use it for his own intelligence. Adversaries can also attack the sensors and cameras via the internet, possibly remaining undetected when they do so. These vulnerabilities have required physical security companies to become smart about cyber security. We have seen similar needs develop in other areas of risk management and mission assurance such as the space industry where out satellites can become vulnerable to cyber attack.
- *The cyber security field can also learn from the conventional security field.* While we have talked in this workshop about network attacks from external adversaries, we must recognize that some of the most damaging cyber crimes have been perpetrated by *authorized users* within the organization—what we call the insider threat. If a network administrator becomes disillusioned at work or is recruited by a terrorist organization, he/she can access and divert sensitive data to an adversary. He/she could also take down network systems with a few keystrokes—destroying data and backup systems. Even a loyal employee could be coerced by an adversary who holds his/her family hostage into destroying network systems or data. In some cases, insiders have unknowingly aided adversaries by failing to follow proper security procedures. For example an employee could insert a USB "thumb drive" into his/her computer, not realizing that it contains malware or a virus. The conventional security business has been addressing an insider threat like this for many years and has much to share with their cyber security field in how to prevent such an attack.

The Way Ahead

The best way ahead for cyber security is to ensure that this threat is an integral element of an organization's overall security strategy and not a separate topic. Cyber security is not just the job of IT specialists. It must be a part of everyone's responsibilities and every member of the organization must be trained to recognize the dangers that they face. As we develop policies and procedures for cyber security, we must look at it from both the vertical and horizontal dimension in order to identify the interactions and interrelationships between cyber and other security elements.

Concluding Remarks

Ingénieur Général Daniel Argenson
Deputy Director, Institut des hautes études de défense nationale (IHEDN)

It is not easy to summarize in a few words the workshop on "Global Security in Crisis." When the workshop began, snow was falling on Paris and the weather was as cold as cold peace, but it ended with sunshine, which may be reason for optimism. A few months ago, when Roger and I discussed the choice of our theme, which is also the theme that the auditors at our IHEDN (Institute for High National Defense studies) have chosen, it quickly appeared that our choice was an obvious one given the new paradigm the world is facing. I thought at first that two days might be too long to cover this issue, but I must admit that it is not enough.

The new situation that we are confronting was somewhat anticipated in the recent White Papers on Defense and Security, including in my own country. The French White Paper had called attention to new risks by adding to the risk of military force, which still exists, the risk of state failures, and the defense and security continuum. Strategic disruptions are not limited to new antagonisms, but are characterized by a drift of the conflict toward other dimensions—military, societal, religious, economic, and technological. Even the notion of conflict is changing. During the workshop, we heard about cold peace instead of cold war and hybrid warfare has been reinvented. As French Prime Minister Manuel Valls pointed out, we are facing an enemy who is both overseas and on our territory, who uses our cities and towns, our infrastructure and resources, for perpetrating crimes, and who was even sometimes educated in our schools. Perhaps the most recent strategic disruption was the world's acquisition of nuclear weapons after World War II which led, from an ideology conflict between the two blocks, to a new world order that lasted for decades until the fall of the Berlin Wall.

…the notion of conflict is changing. During the workshop, we heard about cold peace instead of cold war and hybrid warfare has been reinvented.

Today's world is once again characterized by the emergence of new dimensions in conflicts. It is not by chance that most panels have highlighted a cyber dimension, which was a core element of this workshop. The fact that several cyber companies were sponsors, which is much appreciated, was less important than the fact that it is a day-to-day reality. In addition to this cyberspace dimension, the workshop also addressed most of the challenges that our democracies are facing today for their defense and their security. These challenges have the potential to affect the international order that the end of the cold war brought about: tomorrow will never be like yesterday. The workshop appropriately invited most of the actors involved in the resolution of the current situation—EU and NATO members, Asian countries, and Russia.

A new paradigm means a new order for tomorrow. I don't think anybody expected the workshop to give us an answer to that; we do not have a crystal ball and the world is so

sensitive to the "butterfly effect" that even the best experts cannot predict the results of the U.S. election tomorrow. I fear that we will have to live with unpredictability for years and we should be prepared for any situation. The new driver is that everything is possible. But throughout the workshop panels, I have noted some key words that could give us guidance for the new era in this insecure period: building trust, new international norms and rules, collective answers, patriotism, innovation, deterrence and defense, prevention-education-training, co-responsibility of public and private sectors… This provides much food for thought for future workshops. As an optimistic note in all this chaos, fewer and fewer people are dying from conflicts around the world. While there may be many good reasons to worry, there is also a chance that mankind is on its way to improving its ability to survive.

I fear that we will have to live with unpredictability for years and we should be prepared for any situation. The new driver is that everything is possible.

At this point, let me warmly thank the speakers and audience who placed the debate at a high level, the sponsors and partners who made the seminar possible, the military governor of Paris who hosted the workshop in this historic place, and of course CSDR, which made this 33rd IWGS a success. To conclude with an illustration of the difficulties in managing the new world, I will cite General de Gaulle's famous words during a press conference when he was France's President. Nobody remembers the journalist's question, but General de Gaulle's answer to it was: "How do you want to manage a country in which you can find more than three hundred different sorts of wines and cheeses." This will be the transition to the next and final step of this workshop that we are all waiting for, a "wine and cheese party." And with this, the workshop is now closed.

International Workshop Series on Global Security

PRESENTED BY

Center for Strategic Decision Research · Institut des hautes études de défense nationale

PRINCIPAL SPONSORS

French Ministry of Defense · United States Department of Defense · North Atlantic Treaty Organization · Cisco

MAJOR SPONSORS

McAfee | Intel Security · MITRE · Area SpA

ASSOCIATE SPONSORS

Cast Software · ARES · AXA

CENTER FOR STRATEGIC DECISION RESEARCH & STRATEGIC DECISIONS PRESS

2456 Sharon Oaks Drive | Menlo Park, California 94025 USA | www.csdr.org