New Challenges to Global Security

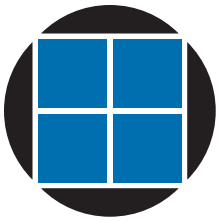
From Russia post-Crimea to Cyber Security post-Snowden

PROCEEDINGS OF THE 31*st* INTERNATIONAL WORKSHOP ON GLOBAL SECURITY

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

Dr. Roger Weissinger-Baylon
Workshop Chairman

Anne D. Baylon
Editor



31*st*
international workshop
on global security

Proceedings of the 31st International Workshop on Global Security

Anne D. Baylon, *Editor*

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

THEME
New Challenges to Global Security
From Russia post-Crimea to Cyber Security post-Snowden

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)

PRINCIPAL SPONSORS
French Ministry of Defense

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

North Atlantic Treaty Organization
Public Diplomacy

MAJOR SPONSORS
Lockheed-Martin · McAfee, a part of Intel Security · Microsoft
MITRE · Fortinet · Tiversa · Area SpA · Dyn · Tenable
Network Security

ASSOCIATE SPONSORS
Kaspersky Lab · FireEye · URS
Quantum Research International
Middlebury Institute of International Studies

Cover: Dôme of the Hôtel National des Invalides

Photography: Jean Lee (lee@meanjean.com)

This work has been funded in part by a multi-year grant from the Office of the U.S. Secretary of Defense (Office of the Director of Net Assessment – Contract Number HQ0034-13-P-0081) and by a grant from the North Atlantic Treaty Organization (Public Diplomacy Division) with additional fiancial support from Lockheed-Martin, McAfee - a part of Intel Security, Microsoft, MITRE, Fortinet, Tiversa, Area SpA, Dyn, Tenable Network Security, Kaspersky Lab, FireEye, and URS. The views presented in this book are entirely those of the editors and authors and do not reflect the official positions of any of the above organizations.

ISBN: 1-890664-21-9

Published by the Center for Strategic Decision Research | Strategic Decisions Press
2456 Sharon Oaks Drive Menlo Park, CA 94025 USA

website: www.csdr.org

contacts:
Anne D. Baylon, editor anne@csdr.org
Dr. Roger Weissinger-Baylon, chairman roger@csdr.org

Workshop Patron

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

Table of Contents

The *31st International Workshop on Global Security* is presented by the Center for Strategic Decision Research (CSDR) and Institut des hautes études de défense nationale (IHEDN), with the Patronage of Defense Minister Jean-Yves Le Drian and the sponsorship of the following organizations:

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE LA DÉFENSE

UNITED STATES DEPARTMENT OF DEFENSE
Net Assessment

NATO OTAN
PUBLIC DIPLOMACY

Center for Strategic Decision Research

IHEDN

MAJOR SPONSORS

LOCKHEED MARTIN

intel Security

Microsoft

MITRE

FORTINET

TIVERSA

AREA

Dyn

tenable network security

ASSOCIATE SPONSORS

KASPERSKY

URS

FireEye

QUANTUM RESEARCH INTERNATIONAL

Monterey Institute of International Studies
A Graduate School of Middlebury College

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

TOP PHOTO: *Courtyard of the Invalides, view from the King's Council Chamber.* BOTTOM PHOTO: *Lieutenant General Bernard de Courrèges d'Ustou, Director of the Institute of Higher Defense Studies (IHEDN) delivers the Opening Remarks of the 31st International Workshop on Global Security. At left, Ambassador Terry Stamatopoulous, NATO Assistant Secretary General for Political Affairs and Security Policy.*

Welcoming Remarks to the 31st International Workshop on Global Security

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

Ministers, Your Excellencies, Mr. Chairman, Fellow Officers,

Good morning and welcome to the Invalides, a place of history and heritage, to discuss the New Challenges to Global Security. It is with great pleasure that, as the director of the Institut des hautes études de défense nationale, I welcome today, for the fifth time in Paris, the International Workshop on Global Security, at the invitation of the Minister of Defense, Mr. Jean-Yves Le Drian. The IHEDN is co-organizing this Parisian edition of the seminar with Mr. Roger Weissinger-Baylon, the chairman and founder of the Center for Strategic Decision Research.

A few words to explain what the IHEDN is. It is an inter-ministerial civilian and military platform which trains its members on strategic issues at national and regional level, and it is also a tool dedicated to European and international responsibility. This year, we are honored to welcome all of you, very distinguished participants including ministers, senators, deputy ministers, ambassadors and high-ranking generals.

During this thirty-first edition of the International Workshop on Global Security, you will be brainstorming for two days on the following subject: New Challenges to Global Security—including Russia post-Crimea and Cyber Security post-Snowden. On these crucial issues, you will benefit from the knowledge of the best experts in their fields during this workshop. I wish you a fruitful and constructive seminar.

General Patrick de Rousiers, Chairman of the European Union Military Committee and Military Advisor to the High Representative of the European Union for Foreign Affairs; Dr. Roger Weissinger-Baylon, Workshop Chairman and Co-Founder; Lieutenant General Bernard de Courrèges d'Ustou, Director of the Institute of Higher Defense Studies (IHEDN); Ambassador Terry Stamatopoulous, NATO Assistant Secretary General for Political Affairs and Security Policy (left to right).

New Challenges to Global Security
From Russia post-Crimea to Cyber Security post-Snowden

Overview

Dr. Roger Weissinger-Baylon
Workshop Chairman

INTRODUCTION

With the Patronage of French Defense Minister Jean-Yves Le Drian, and in partnership with the Institut des hautes études de défense nationale (IHEDN) within the French Prime Minister's organization, this year's *31st International Workshop on Global Security* was presented, once again, in the King's Council Chamber of the Hôtel National des Invalides on 27–29 October 2014. The Invalides, which were built by Louis XIV for his veteran soldiers and to provide a Chapel for the Royal Family, is one of Paris's great monuments. Approximately 80 senior speakers and participants—at the levels of minister of defense, former ministers, diplomats including ambassadors to NATO and the EU, generals, admirals, industry and academic leaders—were invited to address and discuss the theme of *New Challenges to Global Security—from Russia post-Crimea to Cyber Security post-Snowden* in a frank, open and not-for-attribution environment. Over the last few years, cyber security challenges have been growing so rapidly that the cyber threat has become a main workshop theme.

"The Invalides were built by Louis XIV for his veteran soldiers and to provide a Chapel for the Royal Family."

The workshop was presented with the sponsorship and other support of the French Defense Ministry, the U.S. Department of Defense, and the North Atlantic Treaty Organization (Public Diplomacy Division), with appreciation to the Military Governor of the Invalides, and our sponsoring organizations: Lockheed-Martin, McAfee, a part of Intel Security, Microsoft, MITRE, Fortinet, Tiversa, Area SpA, Dyn, Tenable Network Security, as well as Kaspersky Lab, FireEye, URS, Quantum Research International, and the Middlebury Institute of International Studies at Monterey. As our IHEDN partners have pointed out, this is the fifth time that the workshop has been welcomed to France.

Among the key speakers were Lieutenant General Bernard de Courrèges d'Ustou, Director of the Institut des hautes études de défense nationale (IHEDN); General Patrick de Rousiers, Chairman of the European Union Military Committee and Military Advisor to the High Representative of the European Union for Foreign Affairs; Ms. Marietje Schaake, MEP, Member of the European Parliament (The Netherlands); Ambassador Sorin Ducaru, NATO Assistant Secretary General for Emerging Security Challenges; Senator Alain Richard, French Senate (Val d'Oise), former Minister of Defense of France; Senator Jean-Marie Bockel, French Senate, Member of the Foreign Affairs, Defense and Armed Forces Committee and former Secretary of State for Defense; Mr. Chris Painter, Coordinator for Cyber Issues, U.S. Department of State; and Mr. Haden Land, Vice President, Research and Technology, Lockheed Martin Information Systems and Global Solutions.

While addressing the workshop themes of "Russia post-Crimea and Cyber Security post-Snowden" during the workshop, it was already clear that the challenges of the Russia-Ukraine conflict and the rapidly growing threat of cyber attacks are going to be immensely difficult ones. Yet, over the three months that have ensued after our closing session during which the papers in this volume were being

prepared for publication, the threats have grown so rapidly that it is quite tempting to employ that much overused word, "exponential," in describing their evolution.

RUSSIA POST-CRIMEA: IS THIS THE END OF THE RULE-BASED SECURITY SYSTEM?

Upsetting the Vision of Europe as "Whole, Free, and at Peace"

For the millions of TV viewers watching the flamboyant closing ceremonies of the Sochi Olympics, any thought that Russia would be annexing Crimea barely a month later in March 2014—followed by advances into Eastern Ukraine—would have seemed inconceivable. And this crisis is all the more serious because, as Georgian Defense Minister Irakli Alasania says, it is by no means Russia's first aggression in the region: "What we are witnessing in Ukraine is a direct continuation of what was happening in Georgia in 2008." And according to Romania's former Defense Minister, Ioan Mircea Pascu,"Russia is openly challenging the international legal order…such a challenge should not remain unanswered."

"Russia is challenging the international legal order…it should not remain unanswered."

In fact, the crisis created by Russia's unexpected military interventions is so extremely grave that it dramatically alters the fundamental nature of the relations between NATO and most western countries with Russia. In fact, it threatens to pull the relationship back in the direction of the Cold War (or at least towards a "Cool War").

According to Ambassador Terry Stamatopoulos, NATO's Assistant Secretary General for Political Affairs and Security Policy, the Crimean annexation and support for rebels in Eastern Ukraine is not "merely" a grave political-military crisis—which would be unfortunate enough. In fact, the consequences for our relationships with Russia are absolutely fundamental and transformational: Russian actions are effectively "undermining the entire rule-based security system—from the Helsinki Final Act to the conventional and nuclear arms control regimes." A senior NATO military official, Germany's four-star General Hans Lothar Domröse who serves as the Allied Joint Force Commander Brunssum, says that Russia's aggression has completely "upset the vision of Europe as whole, free, and at peace." And as one workshop speaker thoughtfully asks, "Is a *rule of power* now emerging—if not a *rule of violence*—that is beginning to overshadow the *rule of law*?"

Russian actions are effectively "undermining the entire rule-based security system—from the Helsinki Final Act to the conventional and nuclear arms control regimes."

The Crisis in Ukraine: Seen through Russian Eyes

Given the vital historic importance of the relationship with Russia, how can such a rupture be allowed to happen? Is there a lack of understanding or have there been major misjudgments on both sides? According to Ukraine's Ambassador to NATO, Ihor Dolhov, a key factor is that Russia sees Ukraine as "within its areas of geopolitical interest and…part of Russia's national territory." Supporting this interpretation, the former French Defense Minister, Senator Alain Richard, says, "Ukrainians are not perceived as a separate nationality by the rest of Russia." In other words, Russia may consider that the annexation of Crimea is nothing more than taking back its own territory. Ambassador Dolhov also speculates that Ukraine's newly reaffirmed desire to get closer to the EU threatens Russia's "imperial ambitions to restore the USSR" of which Ukraine would be an essential element. He adds that it may be the objection to Ukraine's "goal of integration into the EU" that "has led to an unexpected explosion of aggression."

In fact, these views are close to being a mirror image of those expressed by Russian sEU Ambassador Vladimir Chizhov, who refers to these same issues from his country's perspective. He points out that Russia has "…witnessed an open-ended expansion toward Russian borders" since the 1991 Rome Summit which clearly goes against Russia's strategic national interests. And he also describes

Ukraine as "a young state with enormous hardships [that] was driven to a binary choice between Russia and the EU." In other words, were Ukraine to join the EU, it would be blocked from joining the Eurasian Customs Union that President Putin has founded with Belarus, Kazakhstan, and Armenia. Thus, in purely economic terms, it is not so difficult to understand Russia's fierce opposition to Ukraine's EU membership since it would imply the rejection of Putin's Customs Union. Moreover, as Senator Richard emphasizes: "Ukraine's possible entry into the EU was also a signal of the future failure of an essential Russian ambition."

"Ukraine's possible EU entry signals the future failure of an essential Russian ambition."

Recent Developments: Collapsing Oil and the Holland-Merkel Visit to Moscow

As NATO's Dr. Jamie Shea mentioned, "energy security…has an almost constant capacity to surprise us, and to overturn our most firmly entrenched assumptions. Over the last few months, there have been startling changes that have gone far beyond those anticipated at the time of our workshop: The Russian economy is reeling not only from economic sanctions, as hoped, but also from an unexpectedly sharp drop in crude oil prices that, at least temporarily, have fallen below $50 per barrel. The collapse in the crude oil price is partly attributed to the strategic objectives of Saudi Arabia i.e. slowing the rapid growth of shale oil production. Yet, the Saudis may also want to punish Russia for its support of the Syrian government, and that may be a factor as well. Whatever the causes, the oil price collapse and its extraordinary implications for the global economy has been just as unexpected as Russia's aggression in Ukraine—if not more so.

"The key issue of corruption in Ukraine or Russia was directly mentioned only once."

The effects of collapsing oil prices were not discussed at the workshop for the understandably good reason that they were absolutely unanticipated at the time. Yet, other well-known issues that are key to understanding the Ukraine/Russia (and other) crises were discussed little or not at all—perhaps because they were simply too inconvenient or too embarrassing. For example, both Russia and Ukraine are widely viewed as being massively corrupt, with parts of Ukraine possibly worse than Russia. Yet, the key issue of corruption was directly mentioned only once in these *Proceedings*—by Ukraine's Ambassador Dolhov who described the anti-corruption efforts that are a key part of his government's strategy for 2020.

According to the ancient principle of "know your enemy," which goes all the way back to Sun Tzu's two thousand year-old book, "The Art of War," understanding the situation from a Russian perspective, while openly discussing all of the key issues including sensitive ones, may be an essential step in any effort to resolve the Ukraine/Russia conflict. And it might help us to return to the more cooperative NATO-Russia relationship of recent years. Certainly, the 6 February visit by President Hollande and Chancellor Merkel with President Putin in Moscow would seem to be a useful step in the right direction. In his opening keynote address, General Patrick de Rousiers cited Mrs. Federica Mogherini, the High Representative of the European Union for Foreign Affairs and Security Policy: "It is not by military means that we will solve the crisis in Ukraine."

"It is not by military means that we will solve the crisis in Ukraine." - Mrs. Federica Mogherini

CYBER SECURITY POST-SNOWDEN: IS INTERNATIONAL COOPERATION IMPOSSIBLE?

The Rapid Spread of Large-Scale Cyber Attacks

The U.S. State Department's cyber coordinator, Chris Painter, opened his workshop address by citing remarks made by President Barack Obama, soon after taking office, that lay out the challenge for cyber security in order to protect the tremendous advances and opportunities that the Internet makes possible:

"It is the great irony of our Information Age that the very technologies that empower us to create and to build also empower those who would disrupt and destroy."

In fact, the empowering role of the Internet in the lives of billions of people is not only growing but the growth is accelerating, especially with the arrival of the Internet of Things—which Tim Bloechl describes as, "a world where virtually anything we do…is somehow connected to the Internet." Yet, because of the Internet of Things, hackers will soon have a far greater attack surface, i.e. more devices to attack. Already, the frequency and scope of cyber attacks have reached the point where, as Tenable's Gavin Millard points out, "Breaches of large organisations happen weekly—TJ Maxx, Home Depot, Target, Zappos, Neiman Marcus and JP Morgan." In 2013, Lockheed Martin's Haden Land says "there were eight 'mega breaches'—each leaking more than 10 million identities."

"The Anthem Blue Cross hack lost personal records for 80 million people—including our own!"

And this means that, unless security improves very quickly, events such as the recent Sony hack—recently followed by an Anthem Blue Cross hack that lost personal records for 80 million people (including our own personal data)—will be even more common. Major General John Allan Davis, who heads cyber policy for the U.S. Department of Defense, warns, "…our exploding reliance on information technology stands in stark contrast to the inadequacy of the security of that environment."

How Governments and Industry Are Responding

Since the cyber threat is both global and growing, dealing with it effectively will require cooperation and information sharing between international agencies, governments, industry (not just large corporations or critical infrastructure ones), and especially the public. As NATO Assistant Secretary General Sorin Ducaru says, "cyber defense is, by definition, a team sport." In order to address these complex issues, the workshop brought together more than two dozen major experts[1] representing organizations ranging from NATO and the EU, the French and U.S. governments, to think tanks and cyber security companies. Their presentations appear in the chapters that follow. Since important ideas are presented in virtually every paper, a complete summary of their presentations would be far too lengthy. Nonetheless, a few of the key issues follow:

"Cyber defense is, by definition, a team sport."

- *Countries are reluctant to share information.* Countries stand to benefit from cooperation against the growing cyber threats and, as Major General David Senty points out, the ones "who are generationally behind will benefit most from the sharing of threat information." Despite the strong need for cooperation in the "team sport" of cyber security—and the many successes that have been achieved, broad international cooperation in cyber security is not easy to obtain. For example, some large European countries (like the U.K., France, or Germany) may be reluctant to

[1] Among the major cyber experts addressing the workshop were:
From the North Atlantic Treaty Organization: Czech Ambassador Jiří Šedivý (former Assistant Secretary General); Ambassador Sorin Ducaru, Assistant Secretary General;
From the European Union: Ms. Marietje Schaake, MEP, European Parliament; Ms. Heli Tiirmaa-Klaar, Head of EU Cyber Policy Coordination;
From the French government: Senator Jean-Marie Bockel (former Secretary of State for Defense); Mr. Henri Serres, Ministry of the Economy and Finance; Ing. Général Robert Ranquet, Deputy Director of IHEDN; Dr. Frédérick Douzet, IHEDN (Castex Chair of Cyber Security); Ms. Isabelle Valentini, Head of Cyber Policy, Joint Defense Staff;
From the U.S. government: Major General John Allan Davis (Deputy Assistant Secretary of Defense for Cyber Policy); Mr. Chris Painter, Coordinator for Cyber Issues, State Department; and Ms. Michele Markoff, Deputy Coordinator for Cyber Issues; Major General David Senty, MITRE (former Chief of Staff, Cyber Command);
From industry and academia: Mr. Haden Land, Lockheed Martin IS&GS; Mr. James R. Wylly, Microsoft; Mr. David Grout and Mr. Maurice Cashman, McAfee; Mr. Gavin Millard, Tenable; Mr. Timothy D. Bloechl, Quantum Research International; Dr. Itamara Lochard, MIIS at Monterey; Mr. Jim Cowie, Dyn; Mr. Marco Braccioli, Area SpA; and Mr. Anton Shingarev, Kaspersky Lab.

share confidential cyber information with many of their smaller European allies, especially ones whose limited capabilities do not permit them to offer much in return.

"Countries may be willing to share threat Intelligence with only a small number of very close allies."

Another factor is that effective cyber defense often involves sharing Intelligence, which can often be sensitive, on technical matters ranging from the appearance of new forms of malware to vulnerabilities in systems. For this reason, some large countries may be willing to share with only a small number of very close allies. In fact, according to the "five eyes" principle, the U.S., U.K., Australia, New Zealand, and (somewhat unexpectedly) Israel reportedly share Intelligence among themselves—and this principle presumably applies to sharing cyber-related Intelligence, at least to some degree.

- *Cooperation between government, industry, and the general public is difficult, too*. Even when government agencies are able to cooperate, they may have difficulties in dealing with large companies (including critical infrastructure) and even more problems in dealing with smaller companies or the public.
- *Computer software needs to have security "built-in."* Microsoft has developed a "Trustworthy Computing Initiative." As Jamie Wylly explains, "instead of securing products after we have written them, security and privacy now go into every line of code, beginning with the first line that gets written on every product." According to Anton Shingarev, Kaspersky Labs believes that existing operating systems are not completely secure, so their approach is to build a "fully trustworthy operating system for critical infrastructure." There is a strong tension, however, between developing exciting products and making them secure. In fact, McAfee's Maurice Cashman says (at least for the case of "big data) "security of the platforms is rarely if ever the top priority."
- *Zero-day threats are openly marketed.* Ms. Marietje Schaake at the EU Parliament is one of the experts who are deeply concerned by markets in "zero-day threats." These are vulnerabilities that have been known to the industry for "zero days," which means that patches or other defenses are not yet available. She believes that "markets in zero-day threats need to be regulated, but it is difficult when both governments and companies are buyers in this market"—together with various non-state actors and criminals, as well. Moreover, when governments and militaries buy zero-day threats, it may be in order to spy on or even prepare attacks against other countries. If so, they would definitely want to keep the zero-days for themselves and would be most unlikely to share them with others. The market in zero-days is just one illustration of why international cooperation and sharing of threat information among countries is so difficult.
- *Attribution of cyber attacks can be difficult—or even impossible.* As the Sony hack demonstrates, attribution is not easy. The U.S. government blames North Korea, but the available evidence would be unconvincing without Intelligence that the U.S. says points to Pyongyang hackers. At the French Joint Defense Staff, Head of Cyber Policy Isabelle Valentini says that without "Intelligence, politics, strategy, economics, and the geopolitical context," direct evidence that can be discovered on the hacked network may not be sufficient.

Attribution of cyber attacks often depends on "Intelligence, politics, strategy, economics, and the geopolitical context."

- *Active Cyber Defense has a Potential for Conflict Escalation.* Dr. Frédérick Douzet, who holds the Castex Chair at IHEDN, warns that the "concept of active cyber defense raises serious questions and has a potential for conflict escalation." As the concept of "active defense" migrates toward industry, it leads to the temptation to "hack back," i.e. tracing back and even attacking the attacker. As Dr. Douzet points out, "hacking back" raises legal issues—to say the least. While "many deny that active cyber defense means to hack back," she believes that "a lot of companies have been crossing the line."

- *Sharing of threat and assessement information needs to be automated.* Because of the scale of cyber threats and their speed of arrival, McAfee's Maurice Cashman advocates standards like MITRE's STIX and CVE to facilitate automation in assessing and sharing information. David Grout, also at McAfee, says it is urgent for government agencies to support standards for sharing malware. Among the standards he cites are IOC (Indicator of Compromise) and STIX™ (MITRE's Structured Threat Intelligence eXchange) or CybOX™ (the Cyber Observable eXpression). In order to have stronger cyber capabilities across NATO, Major General David Senty also calls for common standards or formats for rapid threat information sharing."
- *Anti-virus protection may be the best that many people can get, but it is simply not effective*. As General David Senty mentions, anti-virus protection blocks only a portion of the viruses. Moreover, "it is reactive, not proactive, and has [other] limitations." Worse yet, many individuals and even small companies do not even have the limited protection that anti-virus software provides.
- *Apathy may be the greatest cyber threat of all.* While the APT (Advanced Persistant Threat) and other threats are widely feared, the greatest danger may simply be "apathy." As Gavin Millard points out, "Most organizations fail to cover the basic security controls suggested [for example] by the SANS Institute."
- *Organizations need to take basic steps to protect themselves from attack.* Governments and companies can be seduced far too easily by extensive technologies while forgetting to take basic steps. Major General John Allan Davis suggests that "80% of the problem could be addressed with some very basic standards and discipline." This would make it easier for organizations to focus on the remaining 20% of the risks. Gavin Millard gives some specific suggestions: "(a) Discover all the systems within the network (b) Discover all the software running on those systems (c) Identify weaknesses in the configuration of those systems (d) Identify vulnerabilities, and (e) Have good malware defences."

"80% of the problem could be addressed with basic standards and discipline."

- Lockheed Martin's Haden Land offers a broader and more complete list: (a) Prioritize your information assets based on security risks (b) Provide differentiated protection based on importance of assets, (c) Develop deep integration of security for the interdependence driven by technology convergence (d) Develop active defenses to uncover attacks proactively (e) Establish the needed pipeline for the cyber security workforce (f) Integrate cyber-resilience into enterprise-wide risk management and governance processes (g) Influence policy to better enable the hyper-connected world.
- *Critical infrastructure is vulnerable, especially in case of cyber war.* Not only is critical infrastructure vulnerable, it is likely to be a prime target in case of a full-fledged war. As Anton Shingarev points out, nation states could probably take advantage of cyber criminal groups for such attacks.
- *Peer-to-Peer risks may be overlooked by security teams.* Tiversa, a workshop sponsor, has identified peer-to-peer networks as a source of significant data leakage from government and corporate networks. When information is shared on a peer-to-peer network, there is often an unrecognized risk that critical information could be shared accidentally at the same time.

"Critical infrastructure is likely to be a target in case of cyber war."

- *Can NATO invoke Article 5 in response to a cyber attack?* At NATO, an early concern was whether or not a cyber attack on a member country could ever be so serious that it would lead to invoking Article 5—the section of the NATO Charter that permits all NATO countries to come to the assistance of a country, or countries, that have been attacked. While there was initially tremendous resistance, Czech Ambassador Jiří Šedivý says that the answer is now, "yes." Ambassador Ducaru points out, however, that the concept of linking a cyber attack and Article 5 "has been deliberately given some flexibility."

- *What can the U.N., EU, and other international organizations do?* As Chris Painter mentioned, Senator Jean-Marie Bockel and many others have called for "some kind of U.N. code of conduct or binding document" to establish what can legally be done in cyber space. However, State's Chris Painter, NATO's Sorin Ducaru, and the EU's Heli Tiirmaa-Klaar are in agreement that "…international law is applicable in cyber space." Their consensus is important: It means that cyber threats can be addressed far more easily, with existing judicial machinery and without requiring additional international treaties to be signed. Both the EU and OSCE are working on broad guidelines for cyber policies to be adopted by their members. At the EU, Heli Tiirmaa-Klaar says they are asking countries to establish national CERTS (Computer Emergency Response Teams, among other recommendations. And OSCE recommendations are being prepared for release very soon.

LOOKING TO THE FUTURE: THE NEED TO DEAL WITH RELIGIOUS EXTREMISM AND EXTREME ECONOMIC INEQUALITY

At this year's workshop, we focused on several issues that are key to global security: The Russia/ Ukraine conflict, the accelerating threats to global cyber security, and—to a lesser degree—the security implications of energy as well as the Syria/ISIS crisis.

All these factors are closely linked in multiple ways: Russia's intervention in Ukraine was facilitated by revenues from its vast energy resources together with the high price of oil (about $110 per barrel); its support for the Syrian regime worsened the Syria/ISIS crisis. Yet, one of Saudi Arabia's motivations in allowing oil prices to drop below $50 a barrel may have been to hurt both Russia and ISIS by sharply cutting their oil revenues. We can also speculate that Russian aggression in Ukraine is, to some degree, an expression of frustration with Western opposition to its support of the Syrian regime.

While President Hollande, Chancellor Merkel, and other powerful actors are mobilizing international efforts to address the terrible crisis in Ukraine, the underlying causes are hardly addressed at all, or even mentioned—simply because the actors are so powerful. Across the globe, Saudi Arabia and Qatar finance extremely conservative forms of Islam (On September 11, fifteen of the nineteen hijackers were Saudi and many of the Taliban were formed in madrassas that they financed). Yet, over the few last decades, we have experienced a vast redistribution of wealth to the so-called 1% in the West, to the oligarchs in Ukraine (and especially Russia), and of course to the elite of the oil-rich states of the Gulf. The inevitable consequence of this combination of extreme religious view and extreme income is perhaps best explained by Jean-Pierre Maulny, Deputy Director of France's prestigious IRIS institute:

"Saudi Arabia and Qatar finance extremely conservative forms of Islam in Europe."

> In France, there are about two thousand migrants in Calais with no legal status, no place to sleep, no food, and at great risk of serious incidents between migrants themselves as well as between migrants and the local population. Around nine hundred French citizens, sometimes very young, have left France to go to Syria to fight alongside Daech. They have not been recruited in the mosques by imams, but on the Internet through social networks. They live in suburbs, where the education they receive will be unable to bring them their desired social status. Often these people have no hope of ever acquiring a decent social status in their own society. Their only hope is to go to a website that glorifies the djihad: A new hope for them!

The implications of Professor Maulny's analysis are inescapable: There can never be any hope of peace without our respecting the humanity of our citizens, so that everyone—not just the 1%, not merely the oligarchs, nor the princes of the gulf states—has a real opportunity for justice, equality, and hope!

Acknowledgements

Anne Baylon, M.A.,
Editor

One of the pleasures in preparing these *Proceedings* of the 31st International Workshop on Global Security is to express our thanks for the wonderful support of the many individuals and organizations who made the workshop possible—especially the participants, speakers, various staff members, and sponsoring organizations. While we have tried to thank as many as possible (some more than once), it is truly impossible to recognize everyone whose efforts were vital in ways ranging from logistic support to assistance with the publication of the papers in this volume.

Workshop Patron and Speakers

Workshop Patron. For the second year, French Defense Minister Jean-Yves Le Drian offered his Patronage to the International Workshop on Global Security. It is truly an honor, which we appreciate immensely. We are also grateful for the high patronage in recent years of French Defense Ministers: Ms. Michèle Alliot-Marie, Mr. Hervé Morin, Mr. Gérard Longuet, and, for a short period, Mr. Alain Juppé.

Keynote Speakers. The workshop's opening keynote address was presented by General Patrick de Rousiers, a four-star General of the French Air Force and, currently, the Chairman of the European Union Military Committee and Military Advisor to the High Representative of the European Union for Foreign Affairs. Other keynote speakers were Ambassador Thrasyvoulos "Terry" Stamatopoulos, NATO Assistant Secretary General for Political Affairs and Security Policy; Ms. Marietje Schaake, MEP, Member of the European Parliament (The Netherlands); Senator Jean-Marie Bockel, member of the French Senate and former Minister; Senator Alain Richard, member of the French Senate (Val d'Oise) and one of most highly-regarded former Ministers of Defense; as well as Mr. Chris Painter, Coordinator for Cyber Issues, U.S. Department of State.

Session chairs and major speakers. Sir Kevin Tebbit KCB CMG, a former U.K. Permanent Secretary of State for Defense, led the understandably intense workshop debate on the extraordinary crisis in Crimea/Ukraine between Russia's Ambassador to the EU Vladimir Chizhov, Ukraine's Ambassador to NATO Ihor Dolhov, Georgia's Defense Minister Irakli Alasania, and EU Parliamentarian Ioan Mircea Pascu, former Minister of Defense of Romania. General Hans-Lothar Domröse, Allied Joint Force Commander Brunssum; Poland's Ambassador to the EU Boguslaw Winid; and Lieutenant General Patrick Auroy, NATO Assistant Secretary General for Defense Investment addressed the military and defense investment implications of this same theme, while Dr. Jamie Shea, NATO Deputy Assistant Secretary General for Emerging Security Challenges discussed the closely related issues of energy policy.

The challenges surrounding ISIS, Iraq, and Afghanistan, which are equally threatening to global peace and security, were each discussed very effectively by four very senior political and military experts: Ambassador Haydar Berk (Senior Advisor at the Turkish Ministry of Foreign Affairs), Ambassador Omar Samad (Advisor to Chief Executive Abdullah Abdullah and Former Ambassador of Afghanistan to France), Ambassador Fareed Yasseen, Iraq's Ambassador to France, and Senior Colonel Zonglin BAI (China Institute of International Studies).

In the three months that have passed since our 31st workshop, the dangers of cyber security have repeatedly drawn international attention with the Sony hack that was at the center of a major confrontation with North Korea and Anthem Blue Cross hack, where 80 million personal records were lost. Governments and international organizations are struggling to deal with these issues. The

views and approaches of NATO, the E.U., and the French and U.S. governments were discussed by Czech Ambassador to NATO Jiří Šedivý; Ambassador Sorin Ducaru, NATO's Assistant Secretary General for Emerging Security Challenges; Ms. Heli Tiirmaa-Klaar, Head of Cyber Policy Coordination, Conflict Prevention and Security Policy Directorate at the European External Action Service; Ms. Michele Markoff, Deputy Coordinator for Cyber Issues, U.S. Department of State, Mr. Henri Serres, High Council for Economy, Industry, Energy and Technology, French Ministry of the Economy and Finance and Member of the Board of Directors, Orange Group; Ing. Général Robert Ranquet, Deputy Director, Institute for Higher Defense Studies (IHEDN); Ms. Isabelle Valentini, Deputy to the General Officer Cyber Defence, Head of Cyber Policy, French Joint Defence Staff**;** Major General John Allan Davis, Deputy Assistant Secretary for Cyber Policy, U.S. Department of Defense, and Major General David Senty, former Chief of Staff, U.S. Cyber Command and Director, Cyber Operations, The MITRE Corporation.

Since industry "owns" most of the Internet assets, cooperation with industry is essential for any efforts to address the growing cyber security challenges. Key industry and academic speakers were Mr. James R. Wylly, General Manager, Worldwide Public Safety and National Security, Microsoft Corporation; Mr. Gavin Millard, Technical Director, EMEA, Tenable Network Security; LTC (USA, Ret) Timothy D. Bloechl, Director, Cyber Security, Quantum Research International; Dr. Itamara Lochard, Middlebury Institute of International Studies at Monterey (MIIS); Mr. Haden Land, Vice President, Research and Technology, Lockheed Martin IS&GS; Mr. David Grout, Director of Pre-Sales Southern Europe, McAfee, Part of Intel Security; Dr. Frédérick Douzet, Castex Chair of Cyber Strategy, Institute for Higher Defense Studies (IHEDN) and Professor, University of Paris 8; Mr. Jim Cowie, Chief Scientist, Dyn; Mr. Marco Braccioli, Senior Vice President, Area SpA; Mr. Maurice Cashman, Director, Enterprise Architects EMEA, McAfee - part of Intel Security**;** Mr. Anton Shingarev, Head of the CEO Office and Director of Global Government Relations, Kaspersky Lab.

The workshop's final panel was led by Dr. Gerlinde Niehus, Head of NATO's Engagements Section/Public Diplomacy Division. She helped us look to the future together with Portugal's Ambassador João Mira Gomes; NATO Deputy Assistant Secretary for Defense Investment Mr. E. J. Herold; IRIS Deputy Director Jean-Pierre Maulny; and Ms. Roya Mohadjer, STEM/STEAM Strategy Lead at Lockheed Martin Information Systems & Global Solutions.

Principal Sponsors

French Ministry of Defense. Lieutenant General Bernard de Courrèges d'Ustou gave opening remarks in his role as Director of the Institute for Higher Defense Studies (IHEDN), our partner again this year in presenting the 31st International Workshop. IHEDN's Deputy Director, Ingénieur Général Robert Ranquet, was especially helpful and we thank him warmly, as well as Dr. Frédérick Douzet, the Castex Chair, and Mr. Thorniké Gordadze, advisor for educational programs. Mr. Gordadze is a former Deputy Foreign Minister of Georgia and State Minister for Euro-Atlantic Integration.

Since the workshop sessions were presented in the beautiful and historic "Grand Salon" of the Invalides—the "Council Chamber" of King Louis XIV who commissioned the Invalides, we are grateful to the Defense Ministry for making this wonderful venue available and we especially appreciate the support of the Military Governor of the Invalides, Lieutenant General Hervé Charpentier, who kindly made his "salons du gouverneur militaire" available as well. Major Daniel Raty coordinated much of the logistics.

Vice Admiral Arnaud Coustilliere, Head of Cyber Policy for the French Joint Defence Staff, was very effectively represented by Ms. Isabelle Valentini, his Deputy for Cyber Policy, who was most helpful in the planning of workshop cyber security sessions.

French Senate and other French officials. From the French Senate, Senator Alain Richard, former Minister of Defense as well as Senator Jean-Marie Bockel, former Secretary of State for Defense, gave important workshop presentations. Additional French officials included Admiral Jean Betermier, President of Forum du Futur; Ms. Hélène de Rochefort, Secretary General of Forum du Future; Mr. Henri Serres, High Council for Economy, Industry, Energy and Technology, French Ministry of the Economy and Finance; and Ms. Pascale Trimbach, a French diplomat, who now has security-related responsibilities at the Foreign Ministry.

North Atlantic Treaty Organization. While NATO Deputy Secretary General Alexander Vershbow was unable to give the opening keynote as planned, we are delighted that he was represented by Ambassador Thrasyvoulos "Terry" Stamatopoulos, Assistant Secretary General for Political Affairs and Security Policy.

Assistant Secretary General Sorin Ducaru and his Deputy, Dr. Jamie Shea, helped make Emerging Security Challenges one on the main workshop themes, while Lieutenant General Patrick Auroy, Assistant Secretary General for Defense Investment—represented by his Deputy Mr. E.J. Herold—helped emphasize the need for greater defense investments. We were pleased to welcome back Deputy Secretary General for Operations Rick Froh, who contributed much to some of our earliest workshops. NATO diplomats comprised the Czech Republic's Ambassador Jirí Šedivý, Ukraine's Ambassador Ihor Dolhov, and Azerbaijan's Ambassador Khazar Ibrahim.

General Hans-Lothar Domröse, Allied Joint Force Commander Brunssum and one of the very few four-star generals of the German Armed Forces gave his military perspective on the developing crisis in Ukraine.

At the NATO Public Affairs Division, we would like to thank Ms. Angélique Burnet-Thomsen and Ms. Marie-Line Boricaud for their valuable support for this workshop through a NATO grant. As mentioned above, Dr. Gerlinde Niehus, Head of the Engagements Section, led the closing workshop panel, while Mr. Franky Saegerman, Head Social Media Team and Ms. Karli Johnston, consultant to NATO, were extremely helpful in planning the workshop's first-ever efforts with the social media.

United States Department of Defense. We would like to acknowledge the continued support—for the last three decades—of the Office of Net Assessment and its Director, Mr. Andrew Marshall, as well as Ms. Rebecca Bash, who participated in the workshop as Net Assessment's representative. Mr. Marshall, who has retired this year after leading Net Assessment for four decades, has been a strong voice in U.S. defense policy issues at the highest levels. Major General John Allan Davis, Deputy Assistant Secretary for Cyber Policy, gave a strategic overview of the factors driving cyber threats and responses. At the National Defense University (NDU), Dr. Lin Wells has supported the workshop from his time as Acting Assistant Secretary of Defense and we are grateful for Lin's participation this year in his new role as an NU Distinguished Senior Research Fellow.

Major Sponsors

Lockheed Martin. From Lockheed Martin, Mr. Haden Land, Vice President, Research and Technology, IS&GS, was our senior industry sponsor. Ms. Roya Mohadjer, STEM/STEAM Strategy Lead, highlighted the importance of STEM/STEAM education and training, not only because of the need for these technical skills, but because they can even offer a viable future for groups that might otherwise be drawn to religious extremism.

Microsoft. At Microsoft, we appreciated the address by Mr. James R. Wylly, General Manager, Worldwide Public Safety and National Security, on cyber in the context of Mobile and the Cloud. We are also most grateful for the interest and active involvement of Mr. D. A. Harris, Managing Director, Worldwide Defense; Lt. Col. Robert Kosla (Ret.), Director, Central and Eastern Europe, National Security/Defense, and Mr. Bernard Marty, Director for Public Safety and National Security.

McAfee –Part of Intel. Addressing the workshop on behalf of McAfee were Mr. David Grout, Director of Pre-Sales Southern Europe and Mr. Maurice Cashman, Director, Enterprise Architects EMEA; Mr. Jean-Francois Sebastian, Director, Public Sector, was extremely helpful with suggestions for speakers and themes as was Ms. Patricia Murphy, Vice President Sales - Southern Europe. We would also like to thank Thierry Bedos, Regional Director and, above all, Mr. Thomas Gann who was the "architect" of McAfee's workshop participation. He helped us plan the overall workshop agenda as well as the McAfee presentations.

Fortinet. From Fortinet, we appreciated the very active participation of Mr. Patrick Grillo, Senior Director, Solutions Marketing and Mr. Christophe Auberger, Director Systems Engineering, as well as the strong support of Ms. Dalia Pereira, Marketing Manager.

Tenable Network Security. At Tenable, we would also like to thank Mr. Gavin Millard, Technical Director, EMEA; Mr. Stéphane Aouichia, Regional Sales Manager, Southwest Europe; as well as EMEA Marketing Managers Ms. Mehreen Moore and Ms. Jess Patey.

MITRE. The MITRE Corporation has sponsored the workshop for three decades. For their support, we gratefully acknowledge the contributions of Mr. Raymond Haller, Senior Vice President and General Manager, Center for National Security; Mr. Gary Gagnon, Senior Vice President and Corporate Director of Cyber Security; as well as Major General David Senty, Director, Cyber Operations; and Mr. Kevin Scheid, Special Advisor to the President and CEO. For all of our recent workshops, Ms. Fran Harris has been extremely helpful in helping prepare MITRE's participation.

Tiversa. Tiversa sponsored the workshop for the second time this year, with the participation of Mr. Robert Boback, CEO; Mr. Tim Hall, Chief Technical Officer; and Dr. Jack Wheeler, Geopolitical Strategist. We welcomed the chance to discuss their interesting findings concerning peer-to-peer risks.

Area S.p.A. Thanks to Mr. Andrea Formenti, CEO, and Mr. Marco Braccioli, Senior Vice President, Area S.p.A. was an important sponsor for the third time. Mr. Braccioli gave an important address concerning the deep web.

Dyn. We appreciate the continued sponsorship of Dyn as well as the participation and workshop presentation of Mr. Jim Cowie, Chief Scientist, and the opportunity to better understand what they have learned from "mapping the Internet."

Associate Sponsors

- *Kaspersky Lab.* We thank Mr. Anton Shingarev, Head of the CEO Office and Director of Global Government Relations, Kaspersky Lab and Mr. Evgeny Grigorenko, Senior Public Affairs Manager, CEO Office, for joing the workshop. And we appreciate the support of Mr. Eugene Kaspersky, who made Kasperky Lab's sponsorship possible.

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

- *URS Federal Services.* Mr. David Swindle, Executive Vice President, was an important sponsor again this year, and Sir Kevin Tebbit, KCM, CMG, former Permanent Secretary of Defense of the United Kingdom, participated as his representative.

- *Quantum Research International.* We appreciate the support of Mr. Frank Pitts, CEO, and the many contributions of LTC (USA, Ret) Timothy D. Bloechl, Director, Cyber Security, who generously shared his broad ties across the international cyber security community and greatly contributed to the

workshop's success, as he has done for many years, beginning with his contributions while at the U.S. Department of Defense.

- *Middlebury Institute of International Studies at Monterey (MIIS).* Dr. Linton Wells II, and Dr. Itamara Lochard were important contributors to the workshop discussions. Lin's summary of the cyber discussions is reported in these Proceedings, and he played a key role in facilitating participation by U.S. government officials.

Other Key Contributions

Key supporters. We especially appreciated the encouragement and support of Ambassador Dr. Assad Omer, Afghanistan's Ambassador to France; Prof. Dr. Holger Mey, Head of Advanced Concepts, Cassidian; and Senior Colonel BAI Zonglin, Senior Advisor, at the China Institute for International Strategic Studies (CIISS) within the Chinese Foreign Ministry. Italy's Major General Centore of the Centro Militare di Studi Strategici (CeMiSS) joined us for the third year. From Finland, Mr. Vesa Virtanen's contributions were greatly appreciated as well. From Germany, Ambassador Christoph Eichhorn, Deputy Federal Government Commissioner of Germany for Disarmament and Arms Control, was a most welcome representative.

Special thanks. We would like to give special thanks to Mr. Tim Bloechl and Dr. Linton Wells II who were extremely helpful in many ways. Finally, we would like to acknowledge the efforts of Ing. General Robert Ranquet, since he has played a unique role in each of our Paris Workshops. From the Belgian Armed Forces, Vice Admiral Marc Ectors and Admiral (retired) Willy Herteleer, former Chief of Defense Staff of the Belgian Armed Forces, were extremely generous with their advice and played important roles in the development of the workshop agenda.

Workshop Staff. Again this year, our principal staff members were Jean Lee, a graphic designer and professional photographer; Dr. Ania Garlitski, a board-certified cardiologist, who was until recently Assistant Professor of Medicine at Tufts University: and Caroline Baylon, a graduate of Stanford and Oxford universities who is now the Research Associate in Science, Technology and Cyber Security at the Royal Institute of International Affairs in London. All three have frequently supported the workshop since their graduation from Stanford University. Joining us for the first time this year were César Castelain, who has just been admitted by competitive examination to the French Foreign Ministry, and Pablo Kerblat, a recent Master's Degree graduate of St Antony's College, University of Oxford.

Menlo Park, California and Paris, France | February, 2015
Anne D. Baylon

PART ONE:
NEW CHALLENGES TO GLOBAL SECURITY

Keynote Address: Consequences of Global Challenges for the Armed Forces in the European Union

General Patrick de Rousiers
Chairman of the European Union Military Committee;
Military Advisor to the High Representative of the European Union for Foreign Affairs

Ministers, Ambassadors, Admirals and Generals,
Dear friends,

It is an honor and a pleasure to be with you and I thank Professor Weissinger-Baylon for inviting me to your workshop.

The complexity and scale of the crises facing us since the summer remind us of how much dialogue—the exchange and sharing of our respective points of view—is necessary in order to attempt to find together solutions based on cooperation and confidence.

"It is not by military means that we will solve the crisis in Ukraine"—Federica Mogherini

But at the risk of astonishing, and perhaps disappointing you, my remarks will not address the events in Ukraine and Crimea, or the relations with Russia which you have chosen to address during the firstz part of your seminar. Such subjects are extremely political and, at the moment, are occupying all the attention of our leaders. On the occasion of her appearance before the European Parliament, Mrs. Federica Mogherini, the new High Representative of the European Union for Foreign Affairs and Security Policy, has in fact emphasized that, "It is not by military means that we will solve the crisis in Ukraine."

Instead, and more broadly, I prefer to call attention to the consequences of the new challenges that the European armed forces are confronting on the Eastern and Southern borders as well as in the Middle East and explain the way in which these situations are perceived and interpreted in Brussels and, above all, by the 28 chiefs of defense staff of which I am the spokesman.

If you will allow me, I will develop my presentation around three convictions: Solidarity, Partnerships, Prevention.

First Conviction: We Must Reinforce our Solidarity

Today, conflicts are multiplying both near and beyond our border; the threats are there; and they are very real. I will not list them, but one has the feeling of an acceleration, of an increase in volume, and of a growing diversity of the challenges.

But there is another threat, just as crucial. It is the structural disarmament of Europe and the critical absence of capacity that is confronting all of us. At a time when budgets are especially tight, the objective of allocating 2% of the GNP of each member state to defense, including 20% for investments, is actually extremely difficult to obtain—it is even an illusion. In addition to these financial limitations, there is the burden of engagements by several European countries in theaters of operation during the last few years, which have sometimes hindered the development of certain operational capabilities. If our world were at peace, this would not matter.

"There is another threat: Europe's structural disarmament."

We Must Plan beyond Our National Requirements

The enormous instability that has emerged at the frontiers of the European continent, and even much beyond, obliges us to plan beyond our national requirements. These new fields of battle, which are the bases for transnational terrorist threats or cyber attacks, have no "front" or "rear." There is, from the onset, a "rear front" that can be struck at its very heart and whose protection we must imperatively guarantee. Recent events in the U.S. and Canada remind us of this reality.

Today, certain member states fear the return of asymmetric conflicts and the dispute of borders that they have paid dearly to establish. Consequently, they focus their modernization efforts on their land capabilities, their strengthened capacity to act, or even reinforced cooperation with reserve forces, because it is territorial defense that dominates.

"Countries that deal with endless flows of immigrants would prefer to give priority to the surveillance of coastal waters."

Others, who must deal with endless flows of immigrants, would prefer to give priority to the surveillance of coastal waters as well as the reinforcement of their naval forces, without forgetting the stabilization of transit countries or aid to the countries of origin.

Finally, for the majority of member states, the recognition of the significance of information warfare, both defensive and offensive, as well as the development of Intelligence capabilities based on imagery and drones also represent essential interests. All these specific and indispensable capabilities must not distract us from global requirements that we must address together.

And because the second part of your seminar is devoted to cyber threats, I would like to emphasize the magnitude of the consequences that they might bring to the very heart of our economies and our structures, especially our national critical infrastructures. They could be so grave that the collective defense clause that requires member states to act together when one of them is the victim of a terrorist attack or a catastrophe of either natural or human origin, would have to be applicable. Yes, more than ever, the collective defense clause is an absolute imperative!

"It is not a matter of spending 'more' but of spending 'better'—and with solidarity."

Spending with Solidarity. From now on, it is not a matter of spending "more" but of spending "better." This means, in a certain sense, "spending with solidarity." This is the focus of the framework for defense planning cooperation, which is being developed by the European External Action Service (EEAS) in close cooperation with the European Defense Agency and which, I am convinced, will be a huge step forward in the development of our planning processes.

In fact, it is a matter of calling attention to the overall longevity of our equipment and capabilities. It is equally a matter of making sure that sovereignty is exercised where it is required, but only where it is necessary. Finally, it is a matter of prioritizing convergence and cooperation as soon as needs are identified.

Second Conviction: We Must Increase our Partnerships

Today, no member state can assume by itself the responsibility for military operations; strategic isolation is over. It is therefore indispensable to reinforce our partnerships and cooperation in defense matters. This is true for everyone: It is especially true for Europeans.

Partnership and Cooperation with Non-Member Countries. The European Union already has strategic partnerships with a number of countries. Currently, more than 450 soldiers belonging to 9 non-member countries participate in operations and military missions conducted in the framework of the Common Security and Defense Policy (PSDC).

I am thinking in particular of Georgia, which assures the protection of the Bangui airport in the Central African Republic for the operation EUFOR RCA, as well as Turkey, whose soldiers are participating actively in operation EUFOR ALTHEA in Bosnia and Herzegovina, and also Serbia, which made a vital contribution in medical assistance during the EUTM SOMALIA mission to Mogadiscio in Somalia and which—for operation ATALANTE—currently protects a ship chartered for the United Nations food program. Working together under the European flag, alongside soldiers of the 28 member states, they make an essential contribution to the maintenance of peace and to international security.

Other partner countries also bring a significant contribution to our military operations. This is the case for Canada in Mali, the United States in Somalia, Ukraine, which provided a ship last year for operation EUNAVFOR ATALANTA to fight against piracy, as well as China, which regularly offers its support by escorting ships for the World food program.

"China offers its support by escorting ships for the World food program."

This is also the case for Japan. On 16 October, the destroyer TAKANAMI of the Japanese Self-Defense Forces and the Italian frigate ANDREA DORIA which participates in operation ATALANTE have, in fact, participated in a joint counter-piracy exercise in the Golf of Aden.

Close Relations with the Main International Organizations. Likewise, this cooperation permits the maintenance of close relations with the principal international organizations, and evidently with the United Nations. This is why Ambassador Ladsous, Head of the Department of Peacekeeping Operations (DPKO), regularly participates in meetings of the Ministries of Defense of the European Union and meetings of the Chiefs of Defense Staff which I preside.

Likewise, there are solid contacts with the African Union, and also with the OSCE and other regional actors, such as the Sahel College of Security or the West African Police Information System (WAPIS).

But today, we also need to progress further and the strengthening of these partnerships is a priority focus of efforts for the European Union. The recent crises, especially the one in Ukraine, reinforce the logic of partnership between the European Union and the Atlantic Alliance: Sharing a common understanding of the situation and coordinating our actions are indispensable objectives of our work. This is why the NATO's North Atlantic Council (NAC) and the EU's Political and Security Committee (PSC) have met together very regularly in recent months and will continue to do so in the coming weeks.

"We must also guarantee a fair distribution of roles between members and non-members."

The numerous countries that support our missions and operations are also very eager to contribute further. We must therefore integrate our partners more broadly in our strategic discussions, in our training activities, and in our "lessons learned." But at the same time, we must also guarantee a fair distribution of roles between members and non-members. Evidently, the sharing of "savoir-faire," of procedures, or of means of organizations requires large and solid efforts, including in the very concrete area of language comprehension, but our capability to respond globally to global conflicts depends on this principle of "acting together."

It is not a question of building a "European army" but, once more, of building more solidarity everywhere it is needed. We can no longer operate in isolation with our own national limitations. It is no longer an option. This was what Kofi Annan pointed out at the U.N. General Assembly on the day after 11 September when he said, "The only route that offers any hope of a better future for all of humanity is that of cooperation and partnership."[2]

[2] Kofi Annan – Speech to the General Assembly of the United Nations, 24 September 2001

Third Conviction: We Must Reinforce our Means of Crisis Prevention

Today, the European Union is asked more and more to intervene in numerous theaters, in extremely varied security situations. The fight against the spread of Ebola is a perfect example, among many others. But the global management of crises by mobilizing political, diplomatic, economic, legal, police, and military means requires advance planning and sharing of information.

"The EU has a network of 140 delegations across the world for analysis and information sharing."

Successful Crisis Management depends on Advance Planning. In Brussels, this work is perpetually "under construction." It is characterized by a permanent dialogue between the political authorities and the various actors who are involved. In particular, the EU has a network of nearly 140 delegations across the world, which are sources of privileged analysis and information sharing. It also has an Intelligence Analysis Center (EU INTCEN) which, on a permanent basis, provides information on the security and political situation of countries where EU delegations or missions are present. It relies, moreover, on the military intelligence capabilities of the member states, which provide information to the military headquarters of the EU in Brussels. The group responsible for the policy of security and conflict prevention, as well as the EU satellite center based at Torrejón in Spain, both participate in situation evaluations by providing analyses, respectively, on political situations and satellite imagery. But that is not enough!

Transparency and Sharing of Information. The recent lessons of operations in the Balkans, in Afghanistan, and in Africa demonstrate, in fact, the imperative need for reliable, real-time Intelligence for the planning and conduct of operations. The same applies when a crisis appears (Crimea, ISIS,…) and it is necessary to rapidly inform the political authorities in Brussels. Early warning and situation evaluation are areas where we must make progress. It is a matter of planning further "upstream," being more reactive, more coherent, but also providing a more consistent support to deployed missions in difficult situations. We also need to reinforce transparency in order to permit, when it seems relevant, a greater convergence of analyses and thus facilitate the rapid engagement of civil means, even military ones.

"There is an imperative need for reliable, real-time Intelligence for the planning and conduct of operations."

A Clear Definition of Priorities. Today, no one can predict what the next crisis will be. With this in mind, it is necessary to have clearly defined priorities in order to be an actor with the ability to influence events on the international scene. The European Union cannot intervene on every front. It must therefore give direction, coherence, and strategic depth to its actions. This is why it seems necessary to redefine priorities based on a shared analysis of the risks and threats. During her hearing before the European Parliament, Mrs. Mogherini has notably expressed her intention to work on a revision of the European Security Strategy of 2003 in order to establish a list of threats, even if at this stage, no format has yet been agreed upon. I will quote her, "It is necessary to emphasize a common vision, build a common front, and do more prevention than reaction."

"The European Union cannot intervene on every front."

Distinguished Guests, Dear friends,

To wrap up my intervention, my aim was to highlight the challenges faced by the 28 chiefs of defence of the European Union, through three convictions:

- We need to enhance our mutual support: The question is not just how much we spend, but how we can spend better together. It is not just burdens we share, but opportunities as well. A policy framework is being elaborated by the EEAS and the European Defence Agency that should help us enhance systematic and long-term defence cooperation.

- We need to increase our partnerships: The European Union is firmly committed to working in close cooperation with partners and other countries who are decisively contributing to our military missions and operations. But we need to boost our interaction with them and with other international organizations such as the U.N., NATO, the African Union…
- We need to strengthen our conflict prevention and crisis management: In particular, we need to increase transparency and information sharing in order to facilitate convergence of political will among member states. And because of the new security challenges we are facing, we need to focus on priorities. Mrs. Mogherini has stated very clearly that one of her first task will be to have a big public debate on this topic in order to start building *"a common vision and priorities for the European Union foreign and security policy."*

"A new set of powers is rising, bringing their own worldviews to global affairs."

Today we are entering a world where a new set of powers is rising, bringing their own worldviews to global affairs. The challenges and choices before us will demand leadership that reaches into the future without stumbling over the present. In these circumstances, interconnected political, diplomatic, economic and military tools become more and more relevant. We have to use them in a combined manner, with strong will. We are different actors, we may have divergent worldviews, but we must work together to advance our shared interest in security and stability.

Now looking back in history and as a French fighter pilot, I would like to refer to the Normandie-Niemen squadron which is dear to my heart. During World War II, this prestigious unit provided mutual support to forces deployed on the Eastern Front at the suggestion of General de Gaulle. Later on, France and many European countries continued to collaborate with Russia in many different areas, space being one example among many others and a very successful one.

Yet the 2014 crisis in Ukraine was a game changer with sanctions agreed unanimously by European leaders and announcements that "Russia might not be a partner…at the moment."

My hope is that peaceful relations—or should I say, trust and confidence—will soon be restored. Merci pour votre attention!

General Patrick de Rousiers, Chairman of the European Union Military Committee; Military Advisor to the High Representative of the European Union for Foreign Affairs

Consequences of Global Challenges for the Armed Forces in the European Union

General Patrick de Rousiers
Chairman of the European Union Military Committee;
Military Advisor to the High Representative of the European Union for Foreign Affairs

Messieurs les Ministres,
Messieurs les Ambassadeurs,
Messieurs les Officiers Généraux,

Chers amis,

C'est un honneur et un plaisir d'intervenir devant vous et je remercie le Professeur Weissinger-Baylon de m'avoir invité à participer à votre séminaire.

La complexité et l'ampleur des crises auxquels nous sommes confrontés depuis cet été nous rappellent combien le dialogue, l'échange et le partage de nos points de vue respectifs sont nécessaires pour tenter, ensemble, d'y apporter des réponses fondées sur la coopération et la confiance.

Mais au risque de vous étonner, et même de vous décevoir, mon propos ne portera pas sur les événements d'Ukraine et de Crimée, ou sur les relations avec la Russie auxquels vous avez choisi de consacrer la première partie de votre rencontre.

Ces sujets sont éminemment politiques et mobilisent actuellement toute l'attention de nos dirigeants. Au cours de son audition au Parlement européen Madame Federica Mogherini, la très prochaine Haute Représentante de l'Union Européenne pour les Affaires étrangères et la politique de sécurité, l'a d'ailleurs récemment souligné : *"ce n'est pas par des moyens militaires que nous allons résoudre la crise en Ukraine*".

En revanche, et plus largement, je souhaite plutôt évoquer les conséquences des nouveaux défis auxquels les forces armées européennes sont confrontées aux frontières est et sud ainsi qu'au Moyen Orient, vous faire part de la façon dont les choses sont perçues et ressenties à Bruxelles, mais aussi et surtout par les 28 chefs d'état-major d'armées dont je suis le porte-parole.

Si vous me le permettez, j'articulerai mon propos autour de trois convictions : Solidarité, Partenariats, Prévention.

Première conviction : nous devons renforcer notre solidarité

Aujourd'hui, les conflits se multiplient au-delà ou à proximité de nos frontières et les menaces sont là, bien réelles. Je ne les énumère pas … mais on a le sentiment d'une accélération, d'un accroissement du volume et d'une diversité croissante des problématiques.

Mais il est une autre menace, tout aussi cruciale.

Il s'agit du désarmement structurel de l'Europe et du manque crucial de capacités auxquels nous sommes tous confrontés.

A l'heure où les budgets sont particulièrement tendus, l'objectif qui vise à consacrer 2% du PIB de chaque Etat Membre à la défense, dont 20% aux investissements, est en effet extrêmement difficile à atteindre … voire illusoire.

A ces contraintes financières s'ajoute le poids des engagements conduits par plusieurs pays européens sur les théâtres d'opérations au cours des dernières années qui a parfois entraîné l'arrêt du développement de certaines capacités opérationnelles.

Si notre monde était pacifique, cela pourrait ne pas être un enjeu.

- Mais la forte instabilité qui s'est installée aux frontières du continent européen, et bien plus largement encore, nous invite à planifier au-delà de nos seuls besoins nationaux.

  Car sur les nouveaux champs de bataille où se déploient la menace terroriste transnationale ou les cyber-attaques, il n'y a plus ni "avant" ni "arrière". Il y a d'emblée un "front arrière" qui peut être frappé en plein coeur et dont nous devons impérativement assurer la protection. Les évènements récents survenus aux USA ou au Canada sont là pour nous le rappeler.

  Aujourd'hui certains Etats Membres craignent le retour de conflits asymétriques et la remise en cause de frontières chèrement acquises. En conséquence, ils portent leurs efforts sur la modernisation de leurs capacités terrestres, le renforcement des moyens d'action qu'elles peuvent apporter ou bien encore une coopération renforcée avec les forces de réserve car c'est la défense du territoire qui domine.

  D'autres, qui se trouvent confrontés aux flux incessants d'immigrés, souhaitent accorder la priorité à la surveillance des approches maritimes ainsi qu'au renforcement de leurs forces navales sans oublier la stabilisation des pays de transit et l'aide aux pays d'origine.

  Pour la plupart des états membres enfin, la prise en compte de la lutte informatique, défensive et offensive, mais aussi le développement des capacités de renseignement à base d'imagerie et de drones représentent également un enjeu essentiel.

  Autant de capacités spécifiques indispensables qui ne doivent pourtant pas nous détourner des besoins globaux auxquels nous devons faire face ensemble.

  Et puisque la deuxième partie de votre rencontre est consacrée aux cyber-menaces, je voudrais insister sur l'ampleur des conséquences que celles-ci pourraient entraîner au coeur de nos économies et de nos structures, notamment vis-à-vis de nos infrastructures nationales critiques. Celles-ci pourraient être telles que l'usage de la clause de solidarité, qui prévoit l'obligation pour les États membres d'agir conjointement lorsque l'un d'entre eux est victime d'une attaque terroriste ou d'une catastrophe d'origine naturelle ou humaine, doit pouvoir être appliquée.

  Oui, bien plus qu'auparavant, la solidarité est un impératif absolu !

- Dès lors, il ne s'agit donc pas de dépenser "plus" mais de dépenser "mieux". C'est-à-dire en quelque sorte "dépenser solidaire".

  C'est tout l'objet du document cadre consacré à la coopération en matière de planification de défense qui est en cours d'élaboration par le Service Européen d'Action Extérieure, en coopération étroite avec l'Agence Européenne de Défense, et qui, j'en suis convaincu, marquera une rupture dans l'élaboration de nos processus de planification.

  Il s'agit en effet de porter notre attention sur la durée de vie globale de nos équipements et de nos capacités.

  Il s'agit également de faire en sorte que la souveraineté s'exerce là où elle est requise….mais

seulement là où c'est nécessaire.

Enfin, il s'agit de privilégier la convergence et la coopération dès l'expression des besoins.

Deuxième conviction, nous devons accroître nos partenariats

Aujourd'hui, plus aucun Etat Membre n'est en mesure d'assumer seul la responsabilité d'opérations militaires : l'isolationnisme stratégique est révolu.

Il est donc indispensable de renforcer les partenariats et les coopérations en matière de défense.

C'est vrai pour tous. C'est particulièrement vrai pour les Européens.

- L'Union Européenne entretient déjà des partenariats stratégiques avec un certain nombre de pays.

  Actuellement, près de 450 militaires appartenant à 9 "Etats tiers" participent aux opérations et missions militaires conduites dans le cadre de la PSDC.

  Je pense en particulier à la Géorgie qui assure la protection de l'aéroport de Bangui en République Centrafricaine au sein de l'opération EUFOR RCA, mais aussi à la Turquie dont les militaires participent activement à l'opération EUFOR ALTHEA en Bosnie Herzégovine ou encore à la Serbie qui a apporté une contribution essentielle dans le domaine du soutien médical lors du déplacement de la mission EUTM SOMALIA vers Mogadiscio en Somalie et qui – dans le cadre de l'opération ATALANTE – protège actuellement un navire affrété par le programme alimentaire mondial de l'ONU.

  Engagés ensemble sous le drapeau européen, aux côtés des militaires des 28 Etats membres, ils apportent une contribution essentielle au maintien de la paix et de la sécurité internationale.

  D'autres pays partenaires apportent également une contribution significative à nos opérations militaires. C'est le cas du Canada au Mali, des Etats-Unis en Somalie, de l'Ukraine dont un bâtiment a participé l'an dernier à l'opération EUNAVFOR ATALANTA de lutte contre la piraterie, mais aussi de la Chine qui apporte régulièrement son soutien en escortant les bâtiments du programme alimentaire mondial.

  C'est aussi le cas du Japon. Le 16 octobre dernier, le destroyer TAKANAMI appartenant aux forces d'autodéfense japonaises et la frégate italienne ANDREA DORIA qui participe à l'opération ATALANTE ont en effet participé à un exercice conjoint de lutte contre la piraterie dans le Golfe d'Aden.

- Parallèlement, cette coopération se traduit par l'entretien de relations étroites avec les grandes organisations internationales.

  Avec l'ONU, bien évidemment, et c'est la raison pour laquelle l'Ambassadeur Ladsous (DPKO) participe régulièrement aux réunions des Ministres de la Défense de l'Union Européenne ou aux réunions des Chefs d'état-major d'armées que je préside.

  Parallèlement des contacts étroits sont bien sûr établis avec l'Union Africaine, mais aussi avec l'OSCE et différents acteurs régionaux, tels que le Collège de sécurité au Sahel ou bien le système d'information de la Police d'Afrique de l'Ouest.

- Mais aujourd'hui, il nous faut encore progresser et le renforcement de ces partenariats est un axe de travail prioritaire pour l'Union Européenne.

  Les crises récentes, notamment celle en Ukraine, renforcent la logique de partenariat entre l'Union Européenne et l'Alliance Atlantique : partager une compréhension commune de la situation et coordonner nos actions sont des axes d'effort indispensables. C'est ainsi que NAC et PSC se sont réunis très régulièrement au cours de ces derniers mois et vont continuer dans les semaines à venir.

  Les nombreux pays qui apportent leur soutien à nos missions et opérations sont d'ailleurs très désireux d'y contribuer davantage.

  Nous devons donc intégrer plus largement nos partenaires dans nos réflexions stratégiques et dans nos actions de formation ainsi que dans le retour d'expérience.

  Mais parallèlement, nous devons aussi garantir une juste répartition des rôles entre Etats Membres et non-membres.

  Certes la mise en commun de savoir-faire, de procédures, de modes d'organisation, nécessite d'importants et durables efforts, y compris dans le domaine très concret de la compréhension linguistique, mais de cet "agir ensemble" dépend notre capacité à apporter des réponses globales à des conflits globaux.

  Il ne s'agit pas d'établir une "armée européenne", mais encore une fois de bâtir plus de solidarité partout où cela est nécessaire.

  Car nous ne pouvons plus continuer à gérer isolément nos propres contraintes nationales. Ce n'est plus une option !

  C'était déjà ce que rappelait Kofi Annan à l'assemblée général de l'ONU au lendemain du 11 septembre 2001 lorsqu'il déclarait : *"La seule voie qui offre quelque espoir d'un avenir meilleur pour toute l'humanité est celle de la coopération et du partenariat."*[3]

Troisième conviction, nous devons renforcer notre dispositif de prévention des crises

Aujourd'hui, l'Union Européenne est de plus en plus sollicitée pour intervenir sur de nombreux théâtres, dans des contextes sécuritaires extrêmement variés. La lutte contre la propagation du virus Ebola en constitue d'ailleurs une parfaite illustration, parmi bien d'autres.

Mais la gestion globale des crises par la mobilisation de moyens politiques, diplomatiques, économiques, juridiques, policiers et militaires nécessite anticipation et partage de l'information.

A Bruxelles ce travail est perpétuellement à construire.

- Il se caractérise par le dialogue permanent qui s'instaure entre les autorités politiques et les différents acteurs concernés.

  L'UE dispose en particulier d'un réseau de près de 140 délégations réparties à travers le monde qui sont des capteurs privilégiés d'analyse et de partage de l'information.

[3] Kofi Annan - *Discours à l'Assemblée générale de l'ONU* - 24 Septembre 2001

Elle possède également un Centre d'analyse du renseignement (EU INTCEN) qui, en permanence, fournit des informations sur la situation sécuritaire et politique des pays où les délégations ou missions de l'UE sont présentes.

Elle s'appuie enfin sur les structures de renseignement militaires des Etats membres qui alimentent l'état-major militaire de l'UE à Bruxelles.

La cellule chargée de la Politique de sécurité et de prévention des conflits, ainsi que le centre satellitaire de l'Union Européenne, basé à Torrejón en Espagne, participent également à l'évaluation de la situation en fournissant respectivement des appréciations de situation politique et de l'imagerie satellitaire.

Mais cela n'est pas suffisant !

- Les enseignements récents des opérations dans les Balkans, en Afghanistan et en Afrique confirment en effet l'impérieuse nécessité de disposer d'un renseignement fiable, en temps réel, pour la planification et la conduite des opérations. Il en va de même lorsqu'une crise survient (Crimée, ISIS…) et qu'il faut informer rapidement les autorités politiques à Bruxelles.

  L'alerte précoce et l'évaluation de situation sont des domaines dans lesquels nous devons progresser.

  Il s'agit en particulier de planifier plus en amont, d'être plus réactifs, plus cohérents, mais aussi d'apporter un soutien plus consistant aux missions déployées sur des terrains difficiles.

  Il nous faut également renforcer la transparence pour permettre, là où cela est jugé pertinent, une plus grande convergence des analyses et favoriser ainsi l'engagement rapide des moyens civils… voire militaires.

- Aujourd'hui nul ne peut prédire quelle sera la prochaine crise.

  Cependant, pour s'imposer comme un acteur capable de peser sur la scène internationale, il faut des priorités bien définies.

  L'Union Européenne ne peut intervenir sur tous les fronts. Il faut donc pouvoir donner du sens, de la cohérence et de la profondeur stratégique à son action.

  C'est la raison pour laquelle il apparaît nécessaire de redéfinir des priorités à partir d'une analyse partagée des risques et des menaces. Au cours de son audition au Parlement Européen, Madame Mogherini a notamment exprimé son intention de travailler sur une révision de la Stratégie européenne de sécurité élaborée en 2003 afin de dresser un état des lieux des menaces, même si à ce stade cependant, aucun format n'est encore arrêté à ce jour.

  Je la cite : "Il faut mettre l'accent sur une vision commune. Bâtir un front commun et faire plus de prévention que de réaction

Distinguished Guests, Dear friends,

To wrap up my intervention, my aim was to highlight the challenges faced by the 28 chiefs of defence of the European Union, through three convictions:

1. We need to enhance our mutual support:

The question is not just how much we spend, but how we better spend together. It's not just burdens we share, but opportunities, as well.
A policy framework is being elaborated by the EEAS and the European Defence Agency that should help us enhance systematic and long-term defence cooperation.

2. We need to increase our partnerships:

The European Union is firmly committed to working in close cooperation with partners and other countries who are decisively contributing to our military missions and operations.

But we need to boost our interaction with them and with other international organizations such as UN, NATO, the African Union…

3. We need to strengthen our conflict prevention and crisis management:

In particular, we need to increase transparency and information sharing in order to facilitate convergence of political will amongst Member States.
And because of the new security challenges we are facing, we need to focus on priorities.

During her hearing at the European Parliament, Mrs Mogherini stated very clearly that one of her first tasks will be to have a big public debate on this topic in order to start building *"a common vision and priorities for the European Union foreign and security policy".*

Today we are entering a world where a new set of powers is rising, bringing their own worldviews to global affairs.

The challenges and choices before us will demand leadership that reaches into the future without stumbling over the present.

In these circumstances, interconnected political, diplomatic, economic and military tools become more and more relevant. We have to use them in a combined manner, with strong will.

We are different actors, we may have divergent worldviews but we must work together to advance our shared interest in security and stability.

Now looking back in history and as a French fighter pilot, I would like to refer to the Normandie-Niemen squadron which is dear to my heart.

During World War II, this prestigious unit provided mutual support to forces deployed on the Eastern Front at the suggestion of General de Gaulle.

Later on, France and many European countries continued to collaborate with Russia in many different areas: space being one example amongst many others and a very successful one.

Yet the 2014 crisis in Ukraine was a game changer with sanctions agreed unanimously by European leaders and announcements that "Russia might not be a partner …. at the moment."

My hope is that peaceful relations—or should I say, trust and confidence—will soon be restored.
Merci pour votre attention!

The Wales Summit—The Way Forward

Ambassador Thrasyvoulos "Terry" Stamatopoulos
NATO Assistant Secretary General for Political Affairs and Security Policy

Keynote Speaker Ambassador Thrasyvoulos "Terry" Stamatopoulos, NATO Assistant Secretary General.

It is an honour to speak to you today in this beautiful venue, which once served as the Council Chamber for King Louis XIV. So we are not the first ones to be discussing matters of peace and security within these walls.

Let me highlight three principal facts to set the scene for our discussion today.

- First, Russia's aggressive actions against Ukraine constitute a direct challenge to our system of cooperative security; a system that has helped to keep the peace on our continent for two decades. Through its actions, Russia has put into question not only the independence, territorial integrity and sovereignty of Ukraine and other East European countries, but it is also undermining the entire rules-based security system—from the Helsinki Final Act to the conventional and nuclear arms control regimes. This is a deliberate challenge, which requires a clear and concerted response.

"Russia's aggressive actions against Ukraine constitute a direct challenge to our system of cooperative security."

- Second, our security is challenged not only in the East, but also to our South. In the Sahel and in Libya, religious extremists, terrorists, and weak state structures endanger stability and hinder economic progress. Off the coast of Somalia, we have been successful in combating piracy, but the international community faces a long and complex battle with Al-Shabab militants on land. And in parts of Syria and Iraq, we have seen the rise of Daesh, the so-called Islamic State, an "enterprise" run by terrorists, attracting terrorists, and likely exporting terrorists back to our countries. The instability in our Southern neighbourhood directly affects our security at home.
- Third, the West's military and economic might is still unmatched anywhere on the globe. NATO's forces are beyond challenge. And the transatlantic bond that unites us is strong. But some trends are worrisome. For many years now, NATO countries, especially European Allies, have cut defence expenditure by as much as 20% as they have grappled with the economic crisis. At the same time, countries such as

"Countries such as Russia have increased defense investments by as much as 50%."

Russia have increased their investments in weaponry and military training by as much as 50%. And among our North American Allies, there is an understandable reluctance to continue to fill gaps in European capabilities indefinitely.

These are the facts.

Now, how do we deal with them? This is what NATO leaders discussed in Wales a little more than seven weeks ago. And this is where I come to the less gloomy part of my intervention. Because I believe that the Wales Summit actually charted a clear course to overcome today's difficult security challenges.

First, we will strengthen our collective defence. In the East, we already have more planes in the air, more troops on the ground, and more ships in the water. And at the Wales Summit, we approved a Readiness Action Plan to ensure that the Alliance will be able to act with the necessary speed and the required forces to meet any military threat to an Ally—from *any* direction, East or South.

But we also know that improving our collective defence is not the only answer to the challenges that we face. The Alliance's Strategic Concept sets out three core tasks for NATO: collective defence, cooperative security, and crisis management. All three tasks remain valid. And this is why we decided at the Wales Summit to also reinforce our partnerships, including with other international organizations, in particular the EU and the U.N.

We will step up our support to Ukraine and to other Eastern European partners, to help them implement their own foreign policy choices and their domestic reform programmes. And we have launched a "Partnership Interoperability Initiative", to provide partners with a platform to continue to improve their capabilities alongside NATO Allies, even after the ISAF operation in Afghanistan comes to an end. This work allows us to continue to quickly integrate partners in our crisis management efforts, should the need arise.

"We will step up our support to Ukraine and to other Eastern European partners."

But partnership is not only about working together in operations; it is also a political undertaking. And this is why we are also strengthening links with those partners who satisfy the criteria set and are looking for opportunities to consult more closely with the Alliance. At the Wales Summit, we met with Australia, Finland, Georgia, Jordan, and Sweden to discuss current security challenges. And we are now developing this dialogue into a sustained programme of enhanced opportunities.

We are also improving our ability to help countries in our Eastern and our Southern neighbourhood to build their own security forces, should they turn to us for assistance. The rationale is clear: if we can help them enhance their ability to take care of local security, we can project stability without necessarily projecting large numbers of our own troops. At the Wales Summit, we decided to extend such assistance to Georgia, Jordan, and Moldova. And we also decided that we would consider defence capacity building assistance for Iraq, should the new inclusive government request it.

"We are deploying Resolute Support to train, advise and assist Afghan Security forces."

NATO will also continue to play a strong role in crisis management. We are investing, based on the Wales decision, in new military capability, like Intelligence, Surveillance and Reconnaissance (ISR). We are stepping up our exercise program. We have deployed Patriots in Turkey to protect against possible missile strikes. We are deploying a new operation, Resolute Support, to train, advise and assist the Afghan Security forces. And we still have operations in the Balkans and off the coast of Somalia.

So the Wales Summit has set out a clear way forward to address the current security challenges. But this way forward comes with a price tag. And this brings me to my final point: Investment in defence.

Security does not come for free. But beyond this room and beyond Ministries of Defence and expert circles, this message does not always resonate well. Defence expenditure competes against a whole host of other important priorities, such as health, education, and social welfare. And governments throughout the Euro-Atlantic area are facing tough choices in all areas of spending.

"The cost of guarding against security challenges is rising. But the economic cost of insecurity would be much higher."

This is an unenviable dilemma for our political leaders to face, but this dilemma must not lead us to false choices. The cost of guarding against security challenges is rising. But the economic cost of insecurity would be much higher. And this is why our NATO leaders agreed to a Defence Investment Pledge at the Wales Summit: To ensure that our investment matches the threats and challenges that we face.

NATO Allies will work to achieve, within a decade, the agreed Alliance benchmarks for defence spending and the proportion of defence expenditure dedicated to major equipment, and research and development. Some Allied countries meet these benchmarks already. Others are very close to meeting them. But some Allies still have a long way to go. For them, it will not be an easy journey, but it is one that is absolutely necessary if we want to maintain robust capabilities across all three of the Alliance's core tasks, and ensure an equitable sharing of responsibilities among Allies, both within Europe and across the Atlantic.

We face security challenges of a magnitude and complexity that we have not seen in two decades. But these challenges are not insurmountable. If we strengthen our collective defence; improve our partnerships; contribute effectively to crisis management; and underpin these measures with the necessary investment in our defence, we can consolidate security for the entire Euro-Atlantic area. The Alliance's Wales Summit has put us on the right path towards that goal. We must now work to deliver on all the decisions taken.

Lieutenant General Bernard de Courrèges d'Ustou, Director of IHEDN; Mr. Ioan Mircea Pascu, MEP, and former Minister of Defense of Romania: Ambassador of the Russian Federation to the EU Vladimir Chizhov; Dr. Roger Weissinger-Baylon, Workshop Chairman and Co-Founder; Sir Kevin Tebbit, former Permanent Under Secretary of State, U.K. Ministry of Defense; and Georgian Defense Minister Irakli Alasania (left to right). Panel discussion: The Crisis in Crimea and Eastern Ukraine—What it all means for the relationship with Russia.

The Crisis in Crimea and Eastern Ukraine: What It All Means for the Relationship with Russia—Introductory Remarks

Sir Kevin Tebbit KCB CMG
Former Permanent Secretary of State, United Kingdom Ministry of Defense

We are fortunate to have a distinguished panel of speakers present with us this morning. I would like to introduce Ambassador Vladimir Chizhov, Permanent Representative of the Russian Federation to the EU; His Excellency Irakli Alasania, Minister of Defence of Georgia; and Mr Ioan Mircea Pascu, Member of the European Parliament and former Minister of defence of Romania.

In view of the sensitivities of this vital subject, and a crisis in which 3,700 lives have already been lost, I suggest that in order to generate a productive discussion it might be helpful to focus the session around three inter-related themes.

- First, what is the nature of the crisis? Is it a largely unintended consequence arising from the instabilities inherent within Ukraine itself, drawing other parties in beyond where they intended to go? Or, is it a deeper manifestation of a deliberate strategic shift, upsetting the Post- Cold War international order, put in place after the events of 1989, 1991, the Budapest Memorandum, the NATO/ Russia Act of 1997, etc—with all the implications this would have for international law, European security, national sovereignty and renewed competitive tension between Russia and NATO/EU?

"What is now needed to put an end to the violence, and repair the damage caused?

- Secondly, looked at as an exercise in crisis management, how well have the various participants fared in seeking to limit the damage caused—that is to say, Russia, EU/NAT0; and the Ukrainian authorities themselves?
- Thirdly, what is now needed to achieve a solution that puts an end to the violence, repairs the damage caused, both within Ukraine and to the international order, while protecting the interests of the various protagonists?

The Development of the Ukraine-Crimea Crisis and How Such Crises Might Be Prevented in the Future

Ambassador Vladimir Chizhov
Permanent Representative of the Russian Federation to the European Union

I would like to thank you for this very timely opportunity to address an issue that is keeping a lot of people busy across the Euro-Atlantic space. Apart from the rather crude attempts to portray Russia as a natural-born aggressor in this neighborhood, I find it deeply symbolic that the introductory thesis for this panel refers to the nascent ring of insecurity around Europe. It thus seems like the entire European continent was somehow confined to the privileged holders of EU membership cards. I am sure that my Turkish colleague will agree that this is not the case. All our countries from the Atlantic to the Urals, from the North Cape of Norway to Anatolia have a stake and a say in matters related to European security, so the sooner this widespread conceptual flaw is recognized and remedied, the easier it will be for all of us to find solutions to the Ukraine conundrum. More importantly, it may actually help us come closer to something resembling the much talked about Common European Home.

The Post-Cold War Euro-Atlantic Security Architecture

"We have witnessed an open-ended expansion toward Russian borders."

I am stressing this point because, in the Russian worldview, the situation in and around Ukraine is not just a regional crisis *per se.* Rather, what we are facing is an acute symptom of the underlying malaise of the post-Cold War Euro-Atlantic security architecture. Ever since the 1991 Rome NATO Summit, we have witnessed an open-ended expansion toward Russian borders. You may be aware of the recent statement by the U.S. Secretary of Defense about NATO facing Russia at its threshold. The problem is not the highly competent Russian army that he referred to but that the threshold has been moving eastwards.

May I also remind you that back in May 2013, and I am quoting the Lithuanian Foreign Minister, Linas Linkevicius, who made it absolutely clear that the Vilnius Summit of the Eastern Partnership would be about "winning Ukraine in the geo-political battle of Europe." Well, as a former high official of the Young Communist League of the Lithuanian Soviet Socialist Republic, he must be aware of the terminology he was using. Quite simply put, a young state with enormous hardships and a delicate social, linguistic, and ethnic fabric was driven to a binary choice between Russia and the EU. My last quotation would be from this morning's coverage by western (including French) TV channels concerning yesterday's Parliamentary elections in Ukraine. The implications of the election were made as simple as possible: 70% of the votes were won by pro-western parties as if the election was a choice between pro-western and pro-eastern or pro-EU and pro-Russia. Again, this notion of a binary choice was put before the public opinion.

"A young state with enormous hardships was driven to a binary choice between Russia and the EU."

To set the record straight, let me enumerate the efforts made by the West in order to help Ukraine make the "right" choice. It overtly supported an anti-constitutional coup d'état against a democratically elected President of Ukraine. Whether you like it or not, by all international rules and laws, it was a coup d'état. Then, it threw its backing behind a self-proclaimed government of "winners" which appeared on the scene in Kiev, instead of the government of national unity that was promised to the European Union and included as a provision in a document co-signed by the new Ukrainian authorities, the now former Ukrainian President, and three EU Foreign Ministers.

As to this government of winners, the first thing they did was to deny political, cultural, and linguistic rights to a considerable part of the Ukrainian society. Ok, you will say that the law on the role of the Russian language was in the end not implemented. But it was enough to scare millions of people across Ukraine, where people naturally saw this new government as not representing them and not representing their interests. And then, more disturbingly, the West idly watched as Ukrainian forces—both the army and the so-called volunteer battalions (including people adorned with swastikas)—employed a military campaign against the eastern regions of the country. Needless to say, the much-relished European principles such as respect for the rights of national minorities and peaceful settlement of conflicts were trampled under foot in the process.

"The law on the role of the Russian language was enough to scare millions of people."

As for Russia, my country has accommodated more than half a million Ukrainian refugees displaced by the hostilities. Half-year down the road, the result could not be clearer: It is a full-blown civil conflict in a deeply torn country faced by a dire economic situation, with the prospect of a very cold winter. When I refer to refugees, let's look logically at the situation. Is it usual or is it the norm when refugees flee a conflict zone and go into the territory of the so-called aggressor—to settle there, to get residence permits, and in some cases to apply for citizenship?

The Economic Sanctions and their Effects

My intervention would be incomplete without mentioning the issue of the so-called sanctions. These were adopted by the EU unilaterally in breach of the norms of international law since only the U.N. Security Council has the right to impose sanctions. And of course the sanctions were imposed under intense U.S. pressure, as Vice President Joe Biden recently admitted. In our view, these measures have done nothing to de-escalate the conflict and they could not do anything to de-escalate it—or alleviate the plight of civilians caught up in the fighting. In fact, they did backfire on Western economies, and much more on the European economies than on the U.S. economy. That is a fact. The reason lies in the statistics. The volume of trade between Russia and the European Union is about 12 times the volume of Russian trade with the United States. The EU Commission itself estimates that the economic restrictions will cost the EU around 40 billion euros this year and another 50 billion euros next year, if the sanctions are not abrogated. Now it is up to those countries that have started down the erroneous path of sanctions to ponder on how to backtrack to *status quo ante*.

"Has there been any ceasefire after any conflict across the globe that was watertight?"

Against this background, I feel that I need to show some encouraging signs. Above all, there is the ceasefire on the ground agreed to in the course of the Minsk negotiation process. This was in line with the joint initiative of Presidents Putin and Poroshenko that established a much-needed window of opportunity for a political process to commence in earnest. You will say "ok, but the ceasefire is patchy and there are violations" and I will agree to that. And I will admit that there are violations on both sides. But tell me, has there been any ceasefire after any conflict across the globe that was watertight? There are always violations. What matters is for this process to endure those violations and proceed toward a common goal, which is a political settlement of the crisis.

Achieving an Inclusive Dialogue between All Political Forces in Ukraine

We believe that this valuable chance should be seized. The overall objective should be to obtain a lasting comprehensive and peaceful solution in Ukraine through an inclusive dialogue between all credible political forces in the country representing its regions and populations.

The EU has done the right thing by proposing to suspend the implementation of the trade sanctions of the EU-Ukraine association agreement until the end of 2015. Ironically, in so doing, Brussels

followed in the footsteps of President Yanukovych who had been forcibly removed for having done the exact same thing. He requested a postponement in the signing of the association agreement, and he was overthrown for that. Well, nobody has overthrown the European Commission—it is leaving in an orderly fashion on the 31st of October!

So, we look forward to further tri-lateral Russia-EU-Ukraine discussions on this matter. In our view, they should focus on the likely negative effects of a free-trade agreement between the EU and Ukraine, including the possible disruption of trade routes and distortions in the conditions for economic operators within the CIS free-trade area. Most importantly, before there is a return to the "business as usual" mode, there needs to be a reassessment of Russia-EU relations in the area of our common neighborhood. This crisis has amply demonstrated that flawed methods produce flawed results.

"This crisis has amply demonstrated that flawed methods produce flawed results."

A unilateral attempt by the West to execute what some people would say was a hostile takeover of a country the size and complexity of Ukraine has been a blunder of immense proportions. It is encouraging that the incoming EU High Representative for Foreign and Security Policy, Ms. Federica Mogherini, admitted in the EU Parliament that the conclusion of the EU-Ukraine Association Agreement should have been preceded by more deliberations. She also referred to a need for greater coordination between the European and the Eurasian projects of integration. This is exactly what we were urging long before the fateful Vilnius Summit of last year.

Georgian Defense Minister Irakli Alasania and Russian Ambassador to the European Union Vladimir Chizhov (left to right).

Hopefully, the ongoing crisis in Ukraine, tragic though it may be, will yet deliver a moment of truth in revitalizing the concept of a Europe whole and free—and free from dividing lines.

Ukraine's Evolving Relations with Russia and the West: Genesis, Implications, Challenges

Ambassador Ihor Dolhov
Ambassador of Ukraine to NATO

The events that happened in Kyiv from October 2013 to February 2104 have, in fact, become "the Revolution of Dignity," and resulted in Ukraine's return to the principles of democratic development. This fact was welcomed by the democratic community, with the exception of one country—our neighbor, a country that acts as a state-guarantor of Ukraine's territorial integrity in accordance with the Budapest Memorandum.

At the same time, a week after the bloodshed on Independence Square in Kyiv, unprecedented events took place—the Russian Federation annexed a part of Ukrainian territory, the Autonomous Republic of Crimea, directly assisted separatists' armed revolt in the Donetsk and Lugansk regions, and conducted a military invasion into Eastern Ukraine. The Russian Federation's actions have been condemned by the international community, including by the U.N. General Assembly's Resolution. The Russian Federation has in fact initiated a global confrontation with the West, at the core of which are the fundamentally different values and interests of both sides. This global confrontation has led to a change in global security.

"A week after the bloodshed on Independence Square in Kyiv Russian annexed Crimea."

Russian Annexation of Crimea and the Russian Armed Forces' Invasion of Eastern Ukraine—The first "Triumph of Violence" since the End of Cold War

What do we have now in Ukraine? Is Ukraine involved in the escalation of global tension?

First. Ukraine has had a renewal of leadership and is now able to implement democratic changes. The results of the Presidential elections in May bear witness to the Ukrainian people's aspiration to conduct radical changes in the political and economic life of the country. The elections of the Supreme Council (Parliament) of Ukraine were an important step in renewing the legislative branch. A qualitative composition of the Ukrainian parliament has to become a mechanism for creating a synergy of efforts in implementing domestic changes. The change of power authorities has to contribute to the implementation of the wide-scale reforms recently announced by the President of Ukraine and called "Strategy-2020." The first step in this direction was the signing of the comprehensive document that defines the social and economic development of Ukraine for the decades ahead—the EU-Ukraine Association Agreement.

Second. Ukraine has found itself face-to-face with a country that rejects the rules of international law by violating provisions of the Treaty on Friendship, Cooperation and Partnership between Ukraine and the Russian Federation, the Budapest Memorandum on Security Assurances, the Helsinki Final Act, and the basic provisions of the Charter of the United Nations.

The principles employed by the Russian leadership are:

Russia's leadership is playing "a game without rules."

- a game without rules;
- the use of power methods to achieve their own political gains;
- international legal nihilism.

Third. The international community's reaction. Ukraine's return to its previously declared goal of integration into the EU has led to an unexpected explosion of aggression from the Russian Federation. Unprecedented activities of the Kremlin in Ukraine have not gone unnoticed by Western countries and leading international institutions. Reacting to the changes in the security environment

in the region, the international community followed the rules of international law that prohibit unilateral interference in internal affairs by conquering the territory of a sovereign state and changing its borders. The introduction of economic sanctions against selected state and private Russian companies and persons is a civilized, and I would stress, quite moderate reaction of the West towards the uncivilized actions of the political leadership of the country which claims to be a world leader.

"Ukraine's goal of integration into the EU has led to an unexpected explosion of aggression."

Fourth. Russian aggression in Ukraine in 2014—a reaction to the "the Revolution of Dignity" or implementation of imperial ambitions to restore the USSR? Since its independence, Ukraine's relations with Russia have almost never been easy. Guided by imperial ambitions as well as a selective historical and cultural retrospective, Russia considered and still considers Ukraine to be within its area of geopolitical interest and claims it as a part of Russia's national territory. To give just a few examples: Acute confrontation in the Crimea in the mid-90s, the conflict over Tuzla Island in the Kerch Strait in 2003, gas and trade wars that have become an integral part of our "friendly" relations in recent years, and repeated attempts to draw our state into the Customs Union.

Russian annexation of the Crimean Peninsula with disregard for all international norms and its own obligations towards Ukraine, support of separatists, direct military intervention in the East and "slacking" of the situation in the South of Ukraine are the events of recent months. Our northern neighbor has chosen the course of general and profound destabilization of the situation in Ukraine, including through the use of economic war. All this comes amid a strong anti-Ukrainian propaganda campaign at the state level, aimed at a target audience both in Russia and abroad.

"Russia is reinforcing its "gas pressure," setting unjustified rates."

Recent events in Eastern Ukraine have shown deliberate destruction of the region's infrastructure by terrorists. There is a so-called "nationalization" of Ukrainian public and private companies' property by the illegitimate Crimean leadership. Russia is reinforcing its "gas pressure," setting unjustified rates and completely stopping the gas supply in June of this year. They have forbidden the import into Russia of a wide range of Ukrainian products.

The steps above by Ukraine's former "strategic partner" are aimed at one thing—to force our country to change its foreign policy vector back towards Russia.

Fifth. What has the Russian Federation achieved? Pursuing its own purposes in Ukraine, Russia is trying to show, especially to the West, and then to Ukraine, that it is not going to give up its interests, which consist in maintaining influence in our country. Estimating the depth and the extent of this influence in the Crimea and Eastern Ukraine, one may ascertain Russia's true intentions.

Today Russia's political leadership has cynically positioned itself as a "peacemaker," whom enemy forces try to discredit and win over the "dark side."

On the one hand, Russia expresses interest in a stable, strategic relationship with the United States and the European Union. It hopes that artificial external obstacles will not prevent such a mutually beneficial partnership, and emphasizes its commitment to constructive dialogue to form an "actually indivisible security and equal cooperation" with European countries against the backdrop of the current crisis. On the other hand, Russia insists on Ukraine maintaining a neutral status, and considers the removal of "Ukrainian sanctions" put forward by the West as a frivolous, illogical approach. It argues that it will not allow a new arms race, while announcing it will take into account new threats while performing the military planning.

I would like to remind you that the "artificial external obstacles," which Russia is referring to, are actually thousands of lost lives, separated families, intentional destruction of the entire infrastructure of the Crimea and the Ukrainian Donbass, and stolen Ukrainian public and private

"Russia has created a crisis that requires a joint effort to find new forms and ways of relations."

property. And this is what Russia calls a system of "really equal and indivisible security cooperation?"

Let's recall the recent statements by the Russian President concerning the revolution in Ukraine, the creation of the new state, and therefore, Russia's release of any commitments to guarantee its security under the Budapest Memorandum. I would like to ask the audience how you would behave in this situation, while reflecting on the demand for neutral status?

All this proves one thing: Russia has created a crisis that requires a joint effort to find new forms and ways of relations with it.

Peace Comes after War, the Need for a New Strategy for Relations between Ukraine, the West, and Russia.

Peace always comes after war, and de-escalation comes after conflict, so today both in Ukraine and in the West there is a need to establish a *new strategy for relations with Russia.* In my view, the need to define such a strategy is due to the following factors:

- *First,* to guarantee Ukraine's sovereignty and territorial integrity, and to protect it against any form of aggression;
- *Second,* to further deepen the strategic partnership in the framework of Ukraine-EU-U.S.-NATO;
- *Third,* to provide economic and energy security assurance.

Apart from purely security processes, an important factor, affecting the formation of such a strategy in the coming years, will be economic relations within the West-Ukraine-Russia triangle. According to the Russian leadership's perspective, changes in Ukraine's approach to the European Community constitutes a challenge for Russia.

In my opinion, the strategy of relationships with Russia needs to be developed on the basis of the *fundamental values* that unite the European Community. However, taking into account the difference in positions on the Ukrainian-Russian conflict, the strategy's implementation is not straightforward among the EU member states. There are certain factors that have significant impact on formatting an EU position. They are: First, economic and energy dependence of some EU member states on Russia; second, business interests; and third, the degree of influence of Russian public opinion. Nevertheless, European leaders have repeatedly stated that even economic losses due to sanctions imposed by, and against Russia, cannot justify violations of the fundamental values that are vital to the West. Ukraine appreciates such a position by leading European actors and looks forward to strict adherence to this position if Russia continues the current situation.

Therefore, a significant task for the West today is to consolidate its own position with the aim of addressing its geopolitical dilemma regarding the development of its relations with Russia. On the one hand, this could be the way of appeasement, concessions and agreements with the aggressor, for which the Munich Agreement of 1938 could serve as the example. On the other hand—it could be the way of consistency, integration of efforts, and continuation of sanctions.

In this context, we welcome the position of the President of Poland, Bronislaw Komorowski, which was highlighted during a meeting with the newly appointed NATO Secretary General. It was stated that the number one task for the European Community today is to support Ukraine.

The current Ukraine-Russia relations could be described as a deep transformation in all areas and, in particular, in the economic dimension. The reasons for this are the continuing aggression and cognitive dissonance between political elites and social circles of the countries. This dissonance has only been amplified in recent years. Different judgments of Ukrainian events expressed in Kiev and Moscow and lack of compromise have had a negative impact on the results of recent meetings

between the two countries' political leadership and have left little room for productive dialogue. From the other side, what we are witnessing in Russia is: A transition to an authoritarian society with signs of totalitarianism, trampling of human rights and freedoms of citizens, militarization of the country, and an aggressive foreign policy. None of these contribute to the establishment of an adequate political dialogue.

"…what we are witnessing in Russia is a transition to an authoritarian society with signs of totalitarianism."

The position of the Russian leadership is based on the recent dominant conception of the "Russian World," the thought that the West by its actions is testing Russian strength, and the belief that, for Russia, Ukraine today is a kind of "vital foothold" to defend itself against the "alien West." At the same time that the presidents of Ukraine and Russia were meeting in Minsk, Russian regular troops were openly invading Eastern Ukraine. The blocking of separatists by Ukrainian forces in late August did not meet Russian interests and therefore Russia decided to radically change the balance of power in the region.

"For Russia, Ukraine is a kind of "vital foothold" to defend itself against the "alien West."

Today Ukraine and Russia have a high degree of economic ties. Will such ties support the normalization of relations between countries, or vice versa, will they increase the need for their gradual minimization? The trade wars that we have witnessed in recent years have only intensified since the beginning of the conflict. All of this does not add optimism for the future.

Perspectives on the development of Ukraine-Russia relations to a certain extent reflect the well-known and distorted thesis written by the classic Marxist Vladimir Ulyanov-Lenin that Russia's *economy is the concentrated expression of its politics*, not vice versa. In particular, political interests are determining Russian economic policy towards Ukraine. It is very difficult to build pragmatic economic relations with Russia given the condition that everything is subordinated to its politics and to the authoritarian will of the charmed circle of current Russian leaders. Therefore, it is easy to conclude that in the near future our relations will develop in an unpredictable way.

"Everything is subordinated to the authoritarian will of the charmed circle of current Russian leaders."

Under such conditions, the strategy of relations between the West and Russia, and the strategy for resolving the crisis, must be based on respect for Ukraine's right to define its own foreign and domestic policy, including its right to adhere to EU integration and to the development of its relations with NATO.

Implementation of the Ukrainian President's Peace Plan to resolve the crisis in Eastern Ukraine, complemented by the signing of the Minsk Protocol on the 5th of September by representatives of Ukraine, Russia, and the OSCE, will be the first step towards developing such a strategy.

On the other hand, the strategy of Ukraine-Russia relations has to be closely related to the implementation of the internal reforms in Ukraine proposed by the President of Ukraine in his "Strategy-2020." These reforms which cover (i) the fight against corruption, (ii) the system of courts, law enforcement, national security and defense, (iii) decentralization of power and state governance reform, (iv) deregulation and development of private enterprises, and (v) health care. The main goal of these reforms is to meet vital social requirements, and to create the institutional background to implement other reforms for which we have the EU-Ukraine Association Agreement as the basis document.

Ukraine, Georgia and Moldova Integration into the European Union:
The Development of the Eurasian Market.

The similarity of the euro-integration processes currently taking place in Ukraine, Georgia and Moldova, their purposeful desire to deepen their relationships with the EU, and also the actions of

Russia in the post-Soviet space all show the need to strengthen measures within the framework of the EU Eastern Partnership Programme and to develop new and more effective mechanisms that will enhance cooperation with these countries that are of key importance to the EU.

The implementation of the wide-scale reform package proposed by the President of Ukraine in the Ukrainian context and similar processes that have already started or are currently ongoing in Moldova and Georgia will soon become the EU's indicator that these countries are ready to integrate.

Today, these three countries in my opinion fulfill all the necessary conditions, which they never had before, to move further in the direction of euro-integration:

"For the future, the dominance of the economic component of European security is obvious."

- *First*—their readiness to perform radical reforms;
- *Second*—the popular demand and widespread support for their implementation.
- *Third*—the dominance of the economic component in the European security landscape is becoming obvious for the future. For the vast majority of the EU countries, and for Ukraine, Georgia and Moldova as well, diversification of resources and energy independence are of the highest priority. The "Russian factor" will play a key role in this regard.

It is not that difficult to recall that, for the Russian Federation, the sole prospect or notion of NATO membership for the former Soviet countries has become unacceptable. In Russia's opinion, such actions could severely undermine its security. The question of European integration had never caused a negative reaction from Russia before.

"For Russia, the prospect of NATO membership for former Soviet countries has become unacceptable."

Today, the situation has dramatically changed. NATO is deeply concerned about its own security, and Russia finds itself in the position of being a potential adversary of NATO. We are witnessing the unprecedented pressure of Russia on Ukraine to prevent the creation of a Free Trade Area with the EU. Lately, Russia has presented its own set of potentially unacceptable conditions for it, and threatened Ukraine with the prospect of a full-scale trade war.

Ambassador Ihor Dolhov (second from left), Ambassador of Ukraine to NATO, addressing workshop participants.

Such actions have caused outrage in the EU and Ukraine. At the same time, the parties have demonstrated initiative by expressing their willingness to find connecting dots with the radical opposition of Russia. As a result, a series of agreements have been reached to postpone the introduction of the free trade area until January 1, 2016. In addition, the EU has highlighted that the delay in introducing the FTA is an integral part of the peaceful resolution of the situation in Ukraine.

Having acknowledged *the Russian threat and its scale,* the EU on the one hand has to act respectfully in a well-coordinated and determined

way by proposing new tools and opportunities to the countries for their subsequent integration into the EU, and on the other hand, it must show Russia the immutability of the EU approach to conclude the association agreements.

And we can see the first results: The relevant concept has been approved and an EU advisory mission has been started to assist Ukraine with reform of the civil security sector; and several agreements have been reached on establishing broad EU support for the reconstruction of the Donbass and implementation of other structural reforms in Ukraine.

"An EU advisory mission has started to assist Ukraine with reform of the civil security and other sectors."

In order to summarize, it is worth highlighting that implementing the provisions of the association agreements for Ukraine, Georgia and Moldova is the cornerstone for qualitative changes in all spheres of these countries' lives. Keeping in mind their geostrategic location, it will also facilitate the development of the Eurasian market.

In relation to my country, the fight for Ukraine and its freedom of choice is actually the fight for security in Europe as a whole.

Securing Europe from Military Adventures

His Excellency Irakli Alasania
Minister of Defense of Georgia

At last year's workshop, I remember that we had a very detailed and intellectual discussion about what was ahead for the Russia-Georgia relationship. I was arguing that the new approach of Georgia towards Russia was a policy of pragmatism and normalization of the relationship. Although this policy is still in place, it has changed dramatically in the wake of the Russian aggression against Ukraine.

I want to congratulate my friend, Ukrainian Ambassador to NATO Ihor Dolhov, now that pro-Western forces have acquired a solid upper hand in the elections. This is very promising and reassuring for Georgia and shows that Ukraine will not derail its course.

The Conflict in Ukraine

"Events in Ukraine are a direct continuation of what was happening in Georgia in 2008."

Having said that, I would like to answer the question about the nature of the conflict in Ukraine. Of course, it is not due to Ukraine and to the problems inside Ukraine. What we are witnessing in Ukraine is a direct continuation of what was happening in Georgia in 2008. The war against Georgia, which brought the annexation and occupation of Georgia's Abkhazia and South Ossetia, was left unchecked and unanswered by the international community. Today, it is the price that we are paying in Ukraine. This aggressive hybrid warfare that Russia is waging in Ukraine was tested for about 18 years in Georgia after Georgia regained its independence in 1991. And we saw in Crimea an unprecedented violation of the liberal and open rule-based international law. The agreement that was forged in Budapest by the U.K., the United States, and Russia in order to protect the sovereignty of Ukraine has become tissue paper, nothing more, and this is why we are all concerned and asking ourselves "What is next? How are we going to resolve this problem?"

"A smart combination of economic sanctions and military deterrence is the only way we should proceed."

How Should We Resolve the Problem with Russia?

First and foremost, I think that we all agree that NATO is on the right course when it is putting together and reinforcing its military presence in Eastern Ukraine. A smart combination of economic sanctions and military deterrence is the only way we should proceed to make sure that Russia's aggressive military incursions will be kept in check.

Second, it is very important to have open channels of communication with Russia and in Ukraine. The agreement between the Ukrainian leadership, Russia, and European leaders must be kept in place.

A third and very important element I would like to emphasize concerns the willingness of the Western powers to demonstrate that they will act politically, economically and, if it is needed, militarily to deter further Russian military interventionism in Europe.

Georgia's Pragmatic Approach as a NATO Partner

Georgia itself is very pragmatic in its approach to Russia and, at the same time, it is very steadfast in its goal to move closer to the European and Euro-Atlantic security. As a non-NATO country, we are the largest contributor of security in Afghanistan; we are also the largest contributor in EU-led operations in the Central African Republic. Basically, we are acting like NATO and EU members, and when the historical opportunity will open up to join the two alliances, we will be fully ready to do so. Through pre-deployment training to Afghanistan, we have trained more than 12,000 of our troops according to the high standards of the NATO and U.S. militaries. Georgia has been named as the most interoperable partner at the NATO Summit and will be able to contribute substantially to the NATO-Georgia package.

Of course we were disappointed by the decision at the time of the Summit that again Georgia was not granted the Membership Action Plan, but this was not the enlargement summit. So we are very grateful and happy the way our relationship is going with NATO and we are adding substance to the NATO-Georgia package. We will be opening a joint NATO-Georgia training evaluation center in Georgia. New infrastructure will be built in Georgia to facilitate the routine and regular training and exercises of NATO and partner countries on Georgian soil. And, most importantly for us, Georgia is finally getting rid of this detestable ex-Soviet track by promoting itself in the region as the promoter of a democratic transition. Georgia is the first country in the region that underwent, through elections, a democratic and peaceful transition of power. This is why we feel strongly about the future of Georgia within the European and Euro-Atlantic community.

"Georgia is the first country in the region that underwent through elections a democratic and peaceful transition of power."

Russia's Actions in Ukraine Are a Threat to All of Us

We think that it is very important to bear in mind that what Russia is doing today is a threat to all of us. It is not for neighbors only. Ukraine, Georgia, Moldova, have already openly declared that they want to be part of the liberal democracies of the world. This is the choice of the Georgian, Ukrainian, Moldovan and other peoples and it must be respected. At the same time, we are working hard to protect the security of the Euro-Atlantic community by promoting our defense and security capabilities.

What is next and how should we respond?

- *Political pressures.* The response should be political: The alliance is getting stronger and revitalizing its purpose, which is very reassuring for Eastern European countries and partners. The European Union is getting a stronger security identity as well: General de Rousiers spoke about the interoperability of EU and NATO forces and how they can complement each other to secure all of us and our region.
- *Economic sanctions.* The response should also be economic: Sanctions are crucial and maintaining this pressure will be very important to get across the message to Russia that the West means business.
- *Deterrence.* Finally, the third response is the military deterrent. Of course I am not talking about waging a war, but making sure that the adversary understands that there is a sufficient amount of military presence on the ground in Eastern Europe and partner countries. If Russia continues its aggression, these forces will be prepared to react.

The Changing Strategic Landscape in the Black Sea, including the More General Significance of the Ukraine Crisis

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

The Altered Strategic Landscape in the Black Sea and its Consequences

The illegal annexation of Crimea and the subsequent destabilization of Eastern Ukraine by Russia have significantly altered the strategic landscape in the Black Sea and the adjacent area. Russia has the entire Peninsula, not only the Sevastopol naval base, at its disposal. This has important strategic implications: Russia has come some hundreds of kilometers closer to NATO. For all practical purposes, Russia has become Romania's direct neighbor; It can base in Crimea long-range weapon systems threatening strikes in Central Europe (during WWII, Soviet bombers bombed Romania from Crimean bases); Crimea provides a launching pad towards Transnistria and the mouths of the Danube; and Crimea consolidates Russia's posture both offensively (naval power projection to the Eastern Mediterranean, the Middle East and the Gulf) and defensively (against any potentially threatening naval air force in the Black Sea).

"Russia now has the entire Peninsula, not only the Sevastopol naval base.

Russia illegally annexed the Crimean waters, too, sealing the Azov Sea, which was transformed practically into a Russian lake, thus securing the water access to the canal systems that provide access to Moscow proper.

- It thus obtained access to the substantial oil and gas reserves of the continental shelf of Ukraine.
- It can interfere with the oil and gas explorations of the other countries in the region, whose security has thus decreased.
- It can shorten the envisioned route for the South Stream, cutting out Turkey (and the lucrative contracts for the Turkish firms associated with the old route).
- It can control the current oil and gas routes coming from the Caucasus and beyond and going towards the Western consumers.

The balance of naval forces between Turkey—the largest NATO power in the basin—and Russia has shifted in favor of the latter.

- While Turkey, for internal political reasons, has put its naval modernization program in the Black Sea (MILGEM) on hold, Russia is moving fast ahead, announcing plans for an addition to its Black Sea Fleet of six modern diesel submarines and six frigates of the Admiral Grigorovich class by 2016. Russia will add at least one Mistral assault ship, most probably the Sevastopol, to the Black Sea Fleet and probably other similar ships. Later, production would be transferred completely to Russia.

"Russia will add at least one Mistral assault ship to the Black Sea Fleet."

- Consequently, according to the evaluation of specialists, Turkey might trail Russia in naval terms for the next 4-8 years, not 1 year as officially announced. This places Turkey in a lesser position than it was at the time of the Georgian War in 2008.
- Still, by exercising control, through Turkey, of the Black Sea Straits (which have always attracted Russian attempts either to seize them or, at least, set a foot there), combined with naval and air general superiority, NATO continues to hold the upper hand militarily in the Black Sea.

However, it seems a reasonable bet that, in the near future, access to economic gain of both oil and gas exploration and transportation in the Black Sea will be mediated by the expected naval arms race in the region, which could not be alleviated by the existing cooperative formulas like the BLACKSEAFOR or BLUE HARMONY.

Russia's Open Challenge to the International Legal Order

By its actions, Russia is openly challenging the international legal order and the established rules of behavior between states. The problem is that such a challenge should not remain unanswered and was answered by sanctions on the part of the U.S. and the EU and by the "strategic reassurance" NATO provided to its eastern member. If, in the 1990s, these countries considered that obtaining NATO membership—implicitly access to Article 5 of the Washington Treaty—was sufficient to deter a resurgent Russia, now, after Georgia and, much more important, Ukraine, these countries need strong material guarantees that Article 5 will be effectively implemented in case of a Russian attack. The simple truth is that Russia had suffered a massive hemorrhage of trust in the eyes of most eastern members of NATO, irrespective of how unimportant they might be to Russia, in terms of their even cumulated power.

"Russia is openly challenging the international legal order… such a challenge should not remain unanswered…"

But the problem is that Article 5 is intended to defend against military aggression in its classical sense, ignoring, for instance, subversion and hybrid war, both of which were employed by Russia in the current crisis over Ukraine. (It appears that Russia is pursuing a strategic goal through tactical moves, in order to prevent a strategic response).

In two contributions to the Atlantic Council written with Edgar Buckley, we argued that Article 5 should stay as it is, given that its application is anyway contingent on the case at hand, but I am glad that NATO has recently included cyber security within its collective defense missions. Nonetheless, further efforts are needed to respond properly to subversion and hybrid war, which, as Russia has demonstrated, have to be seriously considered.

Naturally, Russia is an indispensable major actor of the international system and will remain so for the foreseeable future. Consequently, in the medium to long run, cooperation rather than conflict should govern relations with it. Still, in the short term, two requirements have to be met: First, any resumption of cooperation should be backed up by a strong strategic reassurance that needs to be offered to NATO's eastern members and, second, as Georgia has demonstrated, any so-called solution without returning to *status quo ante* might not be a solution, but rather an invitation to see more of the same conduct in the future.

Mr. Ioan Mircea Pascu (second from left), Member of the European Parliament; Former Minister of Defense of Romania.

Recent Developments in the NATO Alliance including the Crisis in Ukraine

General Hans-Lothar Domröse
Allied Joint Force Commander Brunssum

When the NATO Summit, held in early September in Wales, was originally scheduled, the focus of the Alliance was on the transition in Afghanistan—both politically with a new government in Kabul and with an imminent fundamental change in NATO's military presence in that country. Notwithstanding that the last 65 years have demonstrated that NATO is the most successful alliance in history, many within and outside the Alliance looked at the downscaling in Afghanistan and asked the question "What role is there for NATO in the coming decades?" The answer came sooner than we had hoped. I think you will agree that recent events have proven the *raison d'être* of NATO beyond any doubt. The collective strength of 28 Allies today is more relevant than it was even two decades ago.

Russia's aggression has "upset the vision of Europe as whole, free, and at peace."

Russia's aggressive actions in and around Ukraine have gravely upset the vision of Europe as whole, free, and at peace. And there is growing instability on NATO's southern borders across the Middle East and North Africa. The new and violent expressions of Islamic radicalism underline the need for unified and adequate responses.

With these disturbances in mind, the leaders of NATO member states came together in Wales and strongly re-affirmed the Trans-Atlantic bond between Europe and North America that is at the heart of the Alliance.

The Wales Summit—NATO's Core Tasks

The core tasks of NATO were paramount at the Summit: Collective Defence, Crisis Management, and Cooperative Security.

- *Collective Defence.* The commitment vested in Article 5 of the Washington Treaty by all members determines the Collective Defence; and this commitment today is again not only most relevant, it is also most reassuring. We are capable of and determined to respond to threats against Allied nations.
- *Crisis Management.* Over the last two decades, NATO has shown that it is prepared to be called upon by the international community for stabilization and peace building—be it in the Balkans or in the most challenging environment of Afghanistan. For instance, by building Afghan National Security Forces (ANSF), the groundwork is laid to give the Afghans the opportunity to shape their own future.
- *Cooperative Security.* In the last few weeks, for the first time in Afghan history, there has been a peaceful transition of political power, and the Afghans are now securing their own country. While NATO has completed its counter-insurgency mission, we will remain committed to Afghanistan through prolonged training, advice, and assistance to the ANSF. And NATO will continue to maintain its strategic partnership with Afghanistan.

NATO's Response to the New Requirements

This positive track stands in stark contrast to Russia's pattern of intimidation of its neighbors, violation of international law by the annexation of Crimea and undermining the unity of Ukraine. Russia's behavior has reinforced Alliance cohesion. Today, all 28 members are united in condemning Russia's actions, while increasing our military power by coordination and exercises. All Allied

"Russia's behavior in Ukraine has reinforced Alliance cohesion."

members have immediately intensified military training, reaping also the benefit of the deepened interoperability practiced in Afghanistan. We have seen increased support to Air Policing Missions in the Eastern Allies' airspace as well as more land forces conducting readiness exercises across Europe. NATO's maritime presence in the Baltic Sea and the Black Sea is manifest; they keep an eye on our vital economic lines of communication.

Realizing the change in NATO requirements, Allied leaders in Wales agreed to stem the decline of defense spending in order to assure the Alliance is fit for purpose. The leaders agreed to a Readiness Action Plan (RAP) that provides NATO with the framework for a stronger, better prepared, and faster military response. The RAP is underpinned by an already existing robust network of support by all Allies to the NATO structures. For instance, already a year ago, we moved forces and NATO headquarters into four NATO nations in order to conduct Exercise Steadfast Jazz in the Baltics. Next year, over 25,000 personnel from 29 nations will conduct Exercise Trident Juncture in Portugal, Spain, and Italy and surrounding waters. My own headquarters in Brunssum has built the necessary networks with NATO Allies and Partners in the North and North East. Better connectivity, tested coordination mechanisms and strong personal relationships with military leaders in the region allow for better execution of our defence plans when the time comes.

The creation of a Family of Northern HQs was already well advanced before the Ukraine crisis induced Mr. Putin's aggressive behavior, and will be intensified further. Since the beginning of the Russian aggression against Ukraine, we have sent integration teams to five Allied countries on the Eastern NATO border and enhanced multiple national exercises by incorporating them into NATO. It is good to realize that NATO is already operating at a very high level of integration, responsiveness, interoperability, and capacity.

But these developments during the spring and over the summer were only the initial stages of the Alliance demonstrating its collective will. We now consider this to be the new baseline of the Allied posture with the ability to expand activity when necessary.

During the Wales Summit, the RAP was approved as the document shaping our future as an Alliance. Leaders agreed to increase the readiness and responsiveness of the NATO Response Force or NRF. The NRF has served as the NATO on-call action group for over a decade, but the new security environment has called for an even more flexible, adaptable, and faster mechanism. Allied nations agreed to create and support a Very High Readiness Joint Task Force. The new force will stand ready to move quickly, that is in less than seven days. The Task Force will be there rapidly to protect any Allied member in a time of crisis.

Russia's hybrid warfare model "no longer relies on overt military power, but employs diverse and covert ways to achieve strategic and political aims."

We have soberly assessed that the Russian model no longer relies solely on overt military power and formations, but employs diverse and covert ways to achieve strategic and political aims. To respond to this hybrid warfare model, NATO is adapting the NRF to provide the Alliance with a set of tools that can be used throughout our territory beyond just countering an overt military threat.

From a purely military perspective, readiness is borne from regular and multilateral military exchanges and exercises. In order to demonstrate this commitment, NATO is embarking upon a very robust training calendar across the Alliance. The aim is not just to transform national training events into multilateral and interoperability exercises, but also to execute more NATO joint exercises across Alliance territory.

In these exercises you will see a closer integration between NATO military headquarters and Allied operational and tactical formations. In my own headquarters, we have a close relationship with the

Multi-national Corps HQ North East in Poland as well as with the Danish Division. Through sustained exchanges as well as integration with these units, I have directed my headquarters to increase our overall interoperability and strategic awareness in the Baltic Sea region.

We, the military, cannot do any of this without the political direction and support of our leaders. While being a four-star general and Commander of a Joint NATO Headquarters, I am still a soldier who follows my orders once they are issued.

The Alliance's Role—Securing Peace, its Territory, and its Sovereignty

In Wales, the Alliance military structure received a broad mission to provide a more ready and responsive force. This political support has set the conditions for the NATO forces to respond to global threats, whether on our own territory or beyond, as directed by the North Atlantic Council. We have demonstrated our commitment as a defensive Alliance to maintain the peace and secure the territory and sovereignty of the Alliance. At the same time NATO remains a transparent and open Alliance whose members are willing to partner with other like-minded nations. In Brunssum, for instance, we have a particularly strong relationship with Sweden and Finland. NATO maintains dialogue with our North African neighbors and partners in the Middle East. NATO is an international organisation intent on fostering peace and stability. Meanwhile our forces have the capability to respond to our political authorities' direction.

But most importantly, we are a cohesive Alliance of 28 nations with extremely intelligent, dedicated and capable soldiers, sailors, airmen and marines.

Mr. E.J. Herold, NATO Deputy Assistant Secretary General; General Hans-Lothar Domröse, Allied Joint Force Commander Brunssum; Dr. Roger Weissinger-Baylon; Ambassador Ihor Dolhov, Ukraine's Ambassadorto NATO; Ambassador Haydar Berk, Turkish Foreign Ministry; and Ambassador Boguslaw Winid, Permanent Representative of Poland to the United Nations (left to right).

The Crisis in Crimea and Eastern Ukraine: A Polish Perspective

Ambassador Boguslaw Winid
Permanent Representative of the Republic of Poland to the United Nations

The Legal Aspects of the Crimean Crisis

In my presentation I will focus on three main topics: The legal aspects of the Crimean crisis; Eastern Ukraine and the way forward; and Poland's support of Ukraine. The recent developments in Crimea opened several fundamental questions that have to be answered by the international community. By acting against Ukraine, the Russian Federation has breached a number of norms of international law, including principles that constitute the bedrock of the international legal order. While, in our opinion, there is no doubt about the illegality of Russia actions, it is important to explain why we consider Russia's arguments as legally unjustified, and to reflect on how the international community should react to these violations. The Legal Advisory Committee of Poland's Foreign Ministry raised seven issues that could well serve as guidance in this regard.

"Russian actions are an example of illegal acquisition of the territory of another state by threat or use of force."

1. The incorporation of the Crimean Peninsula, which forms part of Ukraine's territory, into the Russian Federation qualifies as annexation. In light of international law, Russian acts constitute an example of illegal acquisition of the territory of another state by threat or use of force. By annexing Crimea, the Russian Federation has violated the principle of non-intervention into the domestic affairs of another state, the prohibition against the threat or use of force, and the prohibition against violating the territorial integrity of another state. These principles are enshrined in the U.N. Charter and form part of customary law.

2. Actions by the Russian Federation directed at Ukraine are an act of aggression. Actions taken by Russia at the end of February and in the first half of March 2014, i.e., the use of armed forces deployed in the territory of Ukraine, qualify as acts of direct aggression against Ukraine, pursuant to the U.N. General Assembly Resolution no. 3314 of 1974 which now is regarded as customary law. According to Article 3 of the Annex to the resolution, we qualify as acts of aggression: "the blockade of the ports or coasts of a state by the armed forces of another state" and "the use of armed forces of one state which are within the territory of another State with the agreement of the receiving State, in contravention of the conditions provided for in the agreement or any extension of their presence in such territory beyond the termination of the agreement." It is also undisputable that Russian activities violated the 1997 Ukrainian-Russian agreement on the status and stationing conditions of the Black Sea Fleet.

Russia is also responsible "for the act of indirect aggression by sending armed bands, groups, irregulars or mercenaries against Ukraine"

Russia also bears responsibility for the so-called act of indirect aggression by sending off armed bands, groups, irregulars or mercenaries, who carried out acts of armed force against Ukraine. The armed activities by armed irregulars called "Crimea's self-defense units" or the so-called "green men" can be attributed to the Russian Federation in line with the principles of attribution of responsibility to a state for actions carried out by non-state actors, as defined in the articles on "Responsibility of States for Internationally Wrongful Acts." Adopted in 2001 by the U.N. International Law Commission, these articles are generally recognized as reflecting applicable customary law. The responsibility of the Russian Federation for the activity of irregulars is now undisputed in light of the public statement made by the President of the Russian Federation, Vladimir Putin, on March 17, 2014 when he admitted that these groups were formed out of the soldiers of the Russian Federation's armed forces.

3. Protection of the rights of citizens does not provide a legal justification for the acts directed by the Russian Federation at Ukraine. The Russian Federation's justification of its use of armed force for the protection of the Russian-speaking population outside its borders, including the Russian minority in Ukraine, finds no legal ground in modern international law.

4. "Intervention by invitation" provides no legal grounds to operations by the Russian Federation against Ukraine. The so-called "intervention by invitation" may be regarded as the legal use of armed force, provided that armed force is used with the consent of the authorities of the state on whose territory another state is engaged in military operations. Invocation by the intervening state of local, autonomous, or other lower-level government authorities is inadmissible. In light of this, the appeal on March 1, 2014 by the prime minister of the Autonomous Republic of Crimea to the authorities of the Russian Federation to "ensure peace and public order in Crimea" remains ineffective under international law.

Former President Viktor Yanukovych had no power "to issue a legally effective invitation to the Russian authorities to use armed force."

The construction of "intervention by invitation" is also inapplicable with regard to the alleged appeal by Ukraine's former president, Viktor Yanukovych, as he was not empowered to issue a legally effective invitation to the authorities of the Russian Federation to use armed force. In March 2014 he no longer exercised effective power in Ukraine and remained in Russia, outside Ukraine's borders.

5. *The right to self-determination and secession are not legal ground for separating Crimea from Ukraine.* Russian officials are trying to justify the illegal annexation of Crimea to the Russian Federation as a secession done pursuant to the right of nations to self-determination. However, there is no act of international law that provides grounds for a unilateral secession as an element of the principle of self-determination of nations. Secession by a national community inhabiting a multinational state is, as a rule, legally admissible only with the consent of the authorities of the state.

According to U.N. General Assembly Resolution 68/262, the March referendum in Crimea was invalid.

Russia was directly engaged militarily in Ukraine's disintegration as well as in the referendum on the status of Crimea. An unequivocal legal assessment of this referendum was provided by U.N. General Assembly Resolution 68/262 of March 27, 2014 which states that the referendum conducted on March 16, 2014 in the Autonomous Republic of Crimea and in the city of Sevastopol has no validity and therefore cannot constitute ground for changing their status.

6. *Crimea—under international law—remains an occupied territory by the Russian Federation.* Two factors constitute wartime occupation: 1) effective military and administrative control over the territory of another state; 2) lack of consent of the territorial authority to the presence of armed forces in its territory.

As any wartime occupation, the occupation of Crimea is a transitory condition, which in itself does not change the legal title to the occupied territory. International law prohibits the occupant to change the legal status of the occupied territory. The operations by the Russian Federation in Crimea, the final stage of which became the annexation of the Peninsula, unequivocally represent a serious breach of established norms of international law.

7. *In the face of Crimea's annexation, members of the international community have a duty not to recognize this annexation.* The Russian Federation's operations directed at Ukraine in Crimea are a breach of peremptory norms of international law (*iuris congentis*). Due to the special legal status of the principles that have been violated, the Russian Federation has breached its commitments under the law to the entire international community. Consequently, this community has an international legal obligation, both positive and negative, vis-à-vis these breaches.

The fundamental negative obligation is the prohibition to recognize illegal factual situations that occurred as a breach of peremptory norms. The customary nature of this obligation was reaffirmed and specified more precisely in the Articles on the Responsibility of States for Internationally Wrongful Acts of 2001. The duty not to recognize the annexation of Crimea is also reaffirmed by the U.N. General Assembly resolution of March 27, 2014.

With respect to positive obligations, the above mentioned articles provide that States shall cooperate to bring to an end through lawful means any serious breach by a state of an obligation arising under a peremptory norm of general international law. Apart from the collective condemnation of these violations in international organizations, one of the measures would be to support Ukraine's legal steps in international organizations and bodies responsible for the settlement of international disputes. These actions could ultimately lead to a cessation of the unlawful situation and, consequently, to regaining effective control by Ukraine over its territory of Crimea.

Eastern Ukraine and the Way Forward

Poland supports the peace talks on resolving the Donbass crisis. In our view, the current crisis can be overcome only by political, not military efforts. We hope that the ceasefire protocol signed in Minsk on September 5, 2014 will bring a lasting solution.

Poland appreciates the will and actions taken by the Ukrainian side that led to the implementation of the Minsk agreements. In addition to the decision on the ceasefire, the Supreme Council of Ukraine adopted a new law on special temporary rules of local self-government in parts of Donbass. Ukraine also plans to conduct an early election of local authorities in the region this December, which fulfills one of the main objectives of the Russian side. Poland emphasizes that, by implementing the above steps, the Ukrainian authorities are fulfilling the provisions of the Minsk agreements, while complying with the principle of territorial integrity and sovereignty of Ukraine's power over this part of its territory.

However, in my view the Minsk agreements are rather imperfect and, despite their partial implementation, the situation in Donbass remains tense. There is a problem of differing interpretation of the agreements by its parties and, most of all, of different approach to the main issue—the future of the Donbass region. Separatists do not fully agree to the ceasefire provisions and also disavow other arrangements, including a key one—conducting local elections and the emergence of new local authorities. There is also an urgent need for real de-escalation steps on the Russian side. Russian soldiers are still in the area of Mariupol and new "volunteers" are still coming. A part of the Ukrainian border remains beyond the control of the government in Kiev. Until now, an effective buffer zone has not been established. In this context, sanctions should remain in force until the full implementation of the provisions of the Minsk agreement, securing the border with operational readiness.

"Sanctions should remain until the full implementation of the provisions of the Minsk agreement."

Poland's Minister of Foreign Affairs, Grzegorz Schetyna, stresses that all peace initiatives should be based on the dominant role of Ukraine as the "owner" and the host of the peace process. The starting point on resolving the crisis should remain the respect for international law, territorial integrity and the right of Ukraine to its sovereign choices.

Poland's Support of Ukraine

Ukraine is one of the priority areas of Polish development assistance. Since 2004, as part of bilateral aid, a substantial amount of the '*Polish Aid*' funds is being spent annually on projects aimed at the Ukrainian society—a total of approximately $30 million over the last decade. In 2014, due to the

situation in Ukraine, the Ministry of Foreign Affairs has increased the '*Polish Aid'* budget and planned to spend approximately $6.5 million on civilian assistance to Ukraine.

A particular area of Polish development aid is dedicated to supporting the regional development and capacity building of the public administration. Projects are implemented mainly through non-governmental organizations, local government units and universities, and are related to improving municipal services. The Chancellery of Poland's Prime Minister organizes traineeships for the representatives of the Secretariat of Ukraine's Cabinet of Ministers.

Aid activities are also directed at supporting entrepreneurship, including small and medium-size enterprises, and creating new jobs. The support refers to various levels, starting from business education at schools, through creating academic business incubators, to offering direct support for companies.

Since 2010, the MFA has been financing activities in support of the Ukrainian fire services, which includes seminars for high-ranking fire services officers and representatives of government administration, and specialist trainings for workers and students of Ukrainian fire academies covering topics of emergency medical care, firefighting, rescues and evacuation. Poland also gives equipment to the fire services of Ukraine.

Through the '*Polish Solidarity Fund'*, the MFA finances activities in the field of democratization, including activities boosting public access to independent information, support for civil society organizations and actions. Since 2011, Ukrainian officials have the opportunity to participate in the Eastern Partnership Academy of Public Administration, which is run by the MFA in cooperation with the National School of Public Administration.

I truly believe that Ukraine has a chance of becoming a strong modern state and joining the family of European countries which share common values.

Ambassador Haydar Berk, Turkish Foreign Ministry; Ambassador Boguslaw Winid, Permanent Representative of Poland to the United Nations; and Ambassador Jiří Šedivý, Permanent Representative of the Czech Republic to NATO (left to right).

Dealing with the EmergIng Crises: Crimea/Ukraine and ISIS

Ambassador Haydar Berk
Senior Advisor, Turkish Ministry of Foreign Affairs; Former Permanent Representative of Turkey on the North Atlantic Council

The Situation in Ukraine: Turkey's View

Since previous speakers extensively spoke on the situation in Ukraine, upon the recommendation of the Chairman, the focus of my presentation will be on the situation in Syria and Iraq, in particular on the ISIS threat.

But, before that, I would like to say a few words on our position regarding Ukraine. Turkey will continue to support the efforts aiming at the resolution of the crisis within the framework of the sovereignty, territorial integrity of Ukraine and international law. Turkey strongly supported the Peace Plan of President Poroshenko. We also welcomed the ceasefire agreement reached at the meeting of the Trilateral Contact Group. Turkey does not recognize the illegal annexation of the Autonomous Republic of Crimea. We are concerned about the well-being of Crimean Tatar people and condemn actions intimidating the Tatar people.

We have conveyed our views to the Russian Federation at the highest levels. In that context, we also believe that it is important to keep lines of communication open with the Russian Federation.

"We have conveyed our views to the Russian Federation at the highest levels."

ISIS is a Threat to Regional and Global Stability

ISIS is a serious threat to the security and stability in the Middle East and beyond. Turkey, being the only NATO country that shares a border with ISIS controlled areas, considers ISIS as a direct threat to its national security. Turkey has designated ISIS as a terrorist organization since 2005 under its previous names and revised it by its new name, the Islamic State of Iraq and the Levant, on 10 October 2013. Turkey is taking the necessary steps in the struggle to eliminate ISIS in coordination and collaboration with its friends and allies as well as with the rest of the international community.

Turkey is "the only NATO country that shares a border with ISIS controlled areas."

On 2 October, 2014, pursuant to Turkey's threat perception and also the recent U.N. Security Council resolutions, the Turkish Parliament has authorized the Turkish Government to use Turkish armed forces in Syria and Iraq to counter threats from terrorist organizations to its security. It also allows allied military forces to use Turkish territory, where necessary. This provides the legal ground on which we will be able to build Turkey's strategy within the larger allied efforts aimed at destroying ISIS. However, Turkey's involvement in efforts to counter the ISIS threat actually precedes this decision. Turkey has actively participated in all meetings where international efforts against ISIS were devised and discussed.

Air attacks by the coalition forces against ISIS have been critically important in checking ISIS's advance. However, they should constitute one component of a comprehensive and integrated strategy. Otherwise, we are running the risk of wasting valuable time and resources. Past experience shows that this will be no short or easy endeavor.

The Root Causes of Extremism in the Region within Syria and Iraq

The real focus should be to tackle the root causes in the fight against extremism. As confirmed by the NATO Wales Summit Declaration, Syria and Iraq have been a single theater of operations.

Syria. In Syria, the regime has been and continues to be the patron of the extremism. The policies the regime has consistently pursued based on sectarianism and ethnic divisions keep triggering further instabilities and threats in the wider region. As long as Assad and his clan remain in Damascus, stability cannot be achieved in either Syria or the region. No Fly Zones and Safe Areas in Syria must be the central point of a comprehensive and integrated strategy to combat ISIS. Without NFZs/Safe Areas, it will not be possible to protect the opposition from air operations carried out by the regime and prevent large-scale refugee movements. Intensifying the support to the opposition in Syria should also be bolstered. The opposition is fighting not only the regime, but also ISIS. It is working hard to build peace and democracy in Syria.

"No Fly Zones and Safe Areas in Syria must be the central point of a strategy to combat ISIS."

A genuine political transformation on the basis of the Geneva Declaration and the legitimate expectations of the Syrian people should be the main objective. The coalition that has been put together to counter ISIS should also be utilized in putting pressure on the regime for a political solution. Efforts to revitalize the political process in Syria by the U.N. Secretary General's Special Envoy, Staffan De Mistura, are noteworthy.

The Situation in Iraq: A Need for Reforms

Iraq. In Iraq, the former government's sectarian choice of action has provided a fertile social ground for ISIS to exploit. In order to overcome the ISIS threat and recapture parts of Iraq under its control, Iraqi security forces need to go through serious reform, which would also require a major mentality reform in the government. Iraqi security forces should be organized and run as an inclusive, professional and capable national force, which has the trust and respect of all segments of Iraqi society. This cannot happen overnight. And this cannot happen unless a major shift of mentality in the policies of the Iraqi Government takes place.

"The establishment of a new government in Iraq is a chance that should not be missed."

The establishment of a new government in Iraq is a good chance that should not be missed. The New Prime Minister, Haider al-Abadi, should embark upon a new policy of inclusiveness to embrace all parts of the society. And unless the Iraqi security forces are organized as a national force that has the respect and trust of the Iraqi nation as a whole, it will not be able to liberate the parts of its country under ISIS control.

The Kurds. It is not only the Sunnis in Iraq, who were frustrated with the policies of the previous government. The Kurds have lost their confidence in the central government. Within that context, we welcomed the appointments to the Defense and Interior Ministries in the Iraqi Government on 18 October 2014. We also welcomed the fact that the Kurdish Ministers were sworn in and assumed their duties. The appointments of Defense and Interior Ministers that bear direct responsibility in the fight against the current threat of terrorism and security are important steps in the right direction in terms of restructuring the Iraqi security forces.

"The Kurds have lost their confidence in the central government."

The PKK. One potential, but critical, mistake in the struggle against ISIS would be to misperceive other terrorist groups active in the region, such as the PKK, which present itself as useful fighting forces against ISIS. This should not be a way for any terrorist organization to legitimize itself. It is also very important to make sure that military assistance provided to forces in the region does not end up in the hands of terrorist organizations.

Humanitarian Efforts. Turkey also conducts a large humanitarian effort for the Internally Displaced People (IDPs) who had to flee the ISIS atrocities. Those who have chosen to come to Turkey from Syria and Iraq as a result of ISIS attacks have exceeded 300,000. The Turkish aid agency AFAD has been constructing three camps in Iraq to host 35,000 IDPs. Turkish aid workers and trucks carrying humanitarian assistance have been in Iraq since the first week of June. All this effort is an additional undertaking to assist more than 1.5 million refugees who have fled to Turkey from Syria. This is simply dealing with the end results of the ISIS threat. The best solution to end this humanitarian crisis is to end the ISIS threat in the region. Our common enemy is terror—under any name and in any form.

Foreign Terrorist Fighters

The recent advances of ISIS clearly demonstrated the need for the "foreign fighter phenomenon" to be handled in a wider security perspective. In other words, the developments in Syria and Iraq, as well as the spillover effects in the greater Middle East, should be treated with a view toward reaching an enhanced integrated approach.

The scale of the threat is so unprecedented that it also requires unprecedented insight and international cooperation. We welcome the United Nations Security Council's resolutions 2170 (dated 15 August 2014) and 2178 (24 September 2014) to that end. Turkey co-sponsored the UNSC Resolution 2178, which underlines the importance of international cooperation to counter the foreign-trained fighter (FTF) threat. The threat from FTFs to Turkey begins from the moment they leave their countries and doubles with their attempts to return. The attack to our security personnel on 20 March 2014 by three ISIS affiliates, who tried to transit from Turkish territory, confirmed the validity of our concerns.

"There should be a priority for stopping foreign fighters travelling to conflict zones."

At their country of departure, there should be a priority for spotting and stopping foreign fighters travelling to conflict zones, including Syria. If that fails, then our priority is to stop them at the first port of entry. For that, we need timely, concrete and full information sharing from source countries. Our relevant authorities are taking all necessary measures to prevent third country citizens from travelling to Syria to join radical groups.

Lastly, enhancing efforts to counter ISIS's terrorism financing by destroying and interrupting activities at their sources, mainly in Syria and Iraq, is of high importance.

Recent Developments in Afghanistan and the Region

Ambassador Omar Samad
Advisor to the Chief Executive Officer of Afghanistan: Former Ambassador of Afghanistan to France

The First Democratic Transition in Afghanistan's History

I would like to express my deep appreciation for the invitation to speak to you this evening in the historic setting offered by the Invalides in Paris about developments in Afghanistan and its region.

As you are all aware, the country recently completed a very complex and challenging political transition highlighted by two rounds of elections, an audit and, finally, a political agreement to set up a Government of national unity that is led by the two top contenders, Dr. Ashraf Ghani and Dr. Abdullah—now respectively President and Chief Executive.

We have experienced "the first-ever peaceful and democratic transfer of power from one leader to another in Afghanistan's history."

Although final poll results were inconclusive—due to allegations of fraud, there is agreement that both men garnered an overwhelming majority of support among more than 7 million voters—men and women who defied Taliban intimidations and voted in April and again in June. This transition represents the first-ever peaceful and democratic transfer of power from one leader to another in Afghanistan's history. It also paves the way for a reform-minded government that seeks to address Afghanistan's security and economic problems at a time when the U.S. and NATO are ending the decade-long combat mission to secure Afghanistan by Dec. 31, while reducing aid and funding as well.

The Security, Economic and Political Challenges—Including Dealing with the Taliban

Security and defense responsibilities are now in the hands of Afghan forces. Over the next few years, the U.S. and NATO bilateral security agreements to help Afghan forces with training, advising, assisting and equipping will be crucial. The agreements also allow NATO and other contributing nations to send more than 12,000 trainers and advisors as well as special counter-terrorism forces as part of a new mission until 2017.

On the economic front, the country has undergone a recession over the past two years as part of the difficult transition that saw a reduction in funds and investment.

The other critical item on the new government's agenda is to come up with a strategy to deal with the armed Taliban factions that seek to destabilize the political order, threaten security and disrupt the development process. What makes the Taliban lethal and dangerous is their ability to make use of external sanctuaries and depend on cross-border networks of extremists and criminal elements that benefit from continued conflict in Afghanistan. It is imperative that Afghans be able to defend their country effectively while pursuing a real and tangible plan for political talks that would lead to a settlement with those Afghan militants who are ready and willing to make peace and return to their country. To achieve such an outcome will primarily require a thorough re-examination of strategic priorities and security policies on the part of the Pakistani regime, and need the encouragement and support of other international stakeholders, including the U.S., China, the EU, Saudi Arabia, Iran, Turkey and Russia.

"What makes the Taliban dangerous is their ability to make use of cross-border networks of extremists."

Afghanistan's Future Prospects

Overall, Afghanistan in 2014 is a changed country. While we face daily threats, we are also cognizant of the tremendous contributions that friendly countries have made since September 11, 2001 to help our people take charge of their destiny and allow for progress in all spheres. The Afghan population, including women and children, has far better prospects now than they did 13 years ago. Our majority youth population has benefited from education and better health opportunities, whereas our private sector has become an engine for growth. Moreover, despite the fragility of the situation, it also offers hope and a window of opportunity for durable peace and progress. It will be crucial for the new government to take measures that have the backing of the Afghan people, while the international community remains engaged and supportive as part of a new paradigm to assure that their sacrifices are not in vain and their efforts succeed.

The Afghan population, including women and children, has better prospects than 13 years ago.

Ambassador Omar Samad, Advisor to the Chief Executive Officer of Afghanistan and Former Ambassador of Afghanistan to France, speaking to participants during an evening dinner reception in the salons of the Military Governor of Paris.

Afghanistan: Lessons of the Past Decade and Perspectives for the Future

Senior Colonel Zonglin Bai
Senior Research Fellow, China Institute of International Studies

ACHIEVEMENTS AND LESSONS OF THE PAST DECADE

Since the topic for this session is "Lessons of the Past Decade and Perspectives for the Future," we can begin by discussing past achievements. As we know, after the "9/11" attack, the U.S. has led a global war against terrorism, and the war started right from Afghanistan. Over the past decade, with the common efforts of the international community, Afghanistan has made great achievements: Six million refugees have returned home; there are seven million children receiving education, out of which 38% are female. After being ravaged by wars for decades, most people in Afghanistan now enjoy a relatively peaceful life. The Afghan economy has grown by over 9% each year for 10 consecutive years. Afghanistan security troops total up to 350,000 and have participated in a large part of the military operations by coalition forces. They have taken over the security responsibility of almost 70% of the administrative region and 75% of the total population. Therefore, the international community should be aware of the achievements in Afghanistan and feel encouraged while seeing its future challenges.

"Afghanistan has made great achievements and six million refugees have returned home."

At the same time, some difficult lessons must be acknowledged (due to limited time, I will not go into details):

- Radical Taliban armed forces have not yet been eliminated and could possibly stage a comeback;
- Ethnic reconciliation is not realized;
- An independent economy is not established.

PERSPECTIVES FOR THE FUTURE

On 30 September 2014, the U.S. and Afghanistan signed a bilateral Security Agreement, paving the way for the U.S. and NATO to withdraw all combat troops by the end of 2014. And the trend of development for Afghanistan after 2014 has become a focus of the international community.

Favorable Factors for Afghan Peace and Stability

First, the international community unanimously believes that maintaining security and stability conforms to the interests of the Afghan people and regional countries and is conducive to world peace and development. Secondly, Afghan people who have long been tormented by wars have not had peace for long. And if properly directed, their aspiration for peace would be translated into concrete efforts, which should not be underestimated. Thirdly, taking the Istanbul Process as a platform, regional countries are willing to make more efforts for the peace and stability of Afghanistan. The next foreign

"The next foreign ministers' meeting of the Istanbul Process will be held in China."

ministers' meeting of the Istanbul Process will be held in China. This is the first time for China to organize a special meeting on the Afghanistan issue. Foreign ministers from over 40 countries will attend the meeting to discuss the peace and reconstruction of Afghanistan. This meeting should be a good sign that China and relevant regional countries are willing to play a bigger role on the Afghanistan issue.

Unfavourable Factors for Peace and Stability in Afghanistan

Despite this potential for progress, there are at least three unfavourable factors to deal with:

- Transitions will be difficult in several areas: After 2014, Afghanistan will face transitions in the political, security and economic aspects. Each transition should be handled carefully and, if not properly dealt with, ethnic reconciliation would be hopeless; there are still risks of a worsening security situation; the problem of assistance-dependent economy is still not resolved; a drug economy runs rampant.
- The four core parties concerned with Afghanistan's security, including the U.S., the Taliban, the Afghan government and Pakistan, have not established an effective dialogue platform;
- The relations among the U.S., NATO and regional countries require further coordination.

Since the U.S. and NATO will station troops in Afghanistan for a long time, regional countries should maintain a strategic dialogue with the U.S., Europe, and NATO to enhance their mutual understanding and avoid strategic competition. At the same time, regional countries should establish a set of dialogue mechanisms on security guarantees, which consider and safeguard the security concerns of regional countries (especially countries such as Pakistan) and different political sections within Afghanistan.

"There are major differences within the Taliban on whether to conduct peace talks."

Therefore, I take a prudently optimistic attitude towards Afghanistan's future peace, stability and reconstruction. However, the political reconciliation would have to do with the interests of different parties, and there are still many factors of uncertainty for the future reconciliation process. (First, there are major differences within the Taliban on whether to conduct peace talks; secondly, the "Northern Alliance" with most of the ruling resources fears that the Taliban would damage its own status and rights after entering the government, so they are opposed to peace talks; third, the extent to which the U.S. and the Kabul government would be willing to meet the conditions of the Taliban is also uncertain. So it is difficult for the Afghan peace process to make substantial progress in the short term.)

CHINA'S POSITION AND ATTITUDE TOWARDS THE FUTURE SITUATION IN AFGHANISTAN

China is the biggest neighboring country of Afghanistan and Afghan peace and stability is closely related to the security of western China. Our country supports a political reconciliation process owned and led by the Afghan people and is willing to play a more active role for the future prosperity and development of Afghanistan. China hopes to see an Afghanistan which is united, stable, developing and friendly. We are ready to work with the international community to actively support Afghanistan's political reconciliation and peaceful reconstruction as well as more Afghan participation in regional cooperation.

"China needs to strengthen cooperation with Afghanistan."

China needs to strengthen cooperation with Afghanistan in cracking down on drug trafficking and transnational crimes. China provides political and economic assistance to Afghanistan. There is no reason or possibility for the Chinese military to enter Afghanistan and fill the position previously occupied by NATO. China will provide security support to Afghanistan within the framework of international cooperation.

Energy Policy

Dr. Jamie Shea
Deputy Assistant Secretary General, Emerging Security Challenges, NATO

Dr. Jamie Shea (at right), NATO Deputy Assistant Secretary General for Emerging Security Challenges with Dr. Jack Wheeler, Tiversa Geopolitical Strategist (at left).

Energy Security's Capacity to Surprise

The first point to make about energy security is that it has an almost constant capacity to surprise us, and to overturn our most firmly entrenched assumptions. A few years ago, the debate revolved around the West's dependency on imported oil, particularly from unstable regions such as the Persian Gulf, or suppliers like Russia that could be tempted to use oil and gas as a political weapon. There were also fears regarding "peak oil" or tight oil" which referred to dwindling reserves of fossil fuel and the growing difficulty of extracting those reserves from inhospitable areas such as the ocean seabed or the Arctic ice cap.

Oil's Rapid Evolution from Scarcity to Surplus

"We now have, if not an oil glut, at least an oil surplus."

Today, by contrast, we are in a very different situation. In just a few months, the price of Brent crude has gone from 110 to 86 dollars per barrel. The U.S. is producing an extra 3.9 million barrels per day relative to 2008, which means that it has increased its production by 78%. Libya has managed to quadruple production despite political turmoil and having two oil ministers in two different governments. Iraq is now producing 3 million barrels per day, also notwithstanding political turmoil; and Saudi Arabia (the world's largest producer) has still not agreed to reduce production levels within OPEC, despite pressures from others to move in this direction. So we now have, if not an oil glut, at least an oil surplus. This situation could be potentially disastrous for Russia, which is the world's second largest oil producer and which relies on a Brent crude price of around 115-117 dollars per barrel to maintain its public spending levels. Economists calculate that for every 10% reduction in the oil price, 2% is wiped off the Russian GDP. Russia can survive this situation for the immediate future, given its large national welfare and sovereign funds (around 450 billion dollars) but if the price of oil goes down even further and stays there, Russia will be in serious difficulty given that it is dependent on oil and gas for over 50% of its national earnings. The Russian economy minister has recently warned that Russia's ten year military modernization programme which was to increase defence spending by 34% and re-equip 70% of its forces by 2020 may well have to be scaled back.

"For every 10% reduction in the oil price, 2% is wiped off Russian GDP."

Other long-term trends should also make it easier for Europe to access alternative oil and gas supplies relative to the current high level provided by Russia. Qatar, Norway and Algeria have increased their supplies to Europe and the market looks promising in terms of Europe's greater capacity to receive and process liquefied natural gas from these countries. Recently, Lithuania acquired the "Independence" floating liquefied natural gas (LNG) terminal, which was co-financed by a Norwegian company. New fields have been discovered in the Caspian Sea region and, although the earlier vision of the Nabucco pipeline has not been realized, there is nonetheless a southern corridor route for Europe to access gas from the Caspian region without transiting through Russia by using the trans-Anatolian and trans-Adriatic pipelines. The U.S. is also debating whether to open up more exports of its domestic LNG, which would also help Europe to diversify its sources of supply, and even if much of this will go to Asia because the price there for LNG is higher. At least, in the meantime, the U.S. does not need to import LNG from other countries, which means that surplus LNG is available to be re-shipped towards Europe. If a political solution can be found to the Iranian nuclear weapons issue, and if Iraq can be stabilized, there is the prospect of millions of barrels of oil or cubic metres of gas coming on to the market in the years ahead. Moreover, Israel has discovered two large gas fields (Tamar and Leviathan) in the Eastern Mediterranean and is seeking to develop these in conjunction with Cyprus and the U.S. prospection company Noble. Tamar contains around 8.9 trillion cubic feet and Leviathan 19 trillion cubic feet. Some of this gas of course will be used by Israel and also to assist neighbours such as Jordan and Egypt, but a great deal will no doubt also find its way to the EU.

As is so often the case with energy security, there are political uncertainties. In this case, there is the dispute between Turkey and Cyprus over the delimitation of the gas fields in the Eastern Mediterranean and possible disruptions to excavation and exploitation. This being said, the pessimistic visions of a few years ago, regarding the scarcity of fossil fuels and growing competition for these scarce supplies, no longer appear relevant.

Europe Faces Daunting Energy Security Challenges despite the "Oil Glut"

However, in the short term, Europe will still have to face some daunting energy security challenges.

"Seven EU states totally depend on Gazprom via the pipeline systems in Ukraine."

The first is that the presence of Russian gas and oil in Europe's energy mix is still very high and indeed has even gone slightly upwards over the last four years. The EU obtains 25% of its gas from Russia and some countries, such as Finland, Czech Republic, Bulgaria or the Baltic States, import more than 50% of their gas from Russia. Indeed, seven EU states totally depend on Gazprom via the pipeline systems in the Ukraine—which has been the biggest geopolitical issue in EU energy security for the last decade. Clearly, an EU energy supply mix which would all together exclude Russian gas and oil is not achievable in the short-term. LNG is currently underexploited (the EU is using only 16% of its overall capacity at the present time) and supplies from other sources such as Algeria, Nigeria, Mozambique or Qatar would need to be developed further. In the short-term, the EU could withstand a sudden complete cut-off of Russian gas for some time because it is able to store up to 86 billion cubic meters of gas in its storage tanks. A recent EU Commission stress test of member states' stored capacity and emergency contingency plans confirmed this relatively healthy situation. 86 billion cubic metres in storage represent half of the 163 billion cubic metres that the EU imports from Russia every year. So it would provide a considerable cushion in a crisis situation.

Europe Needs to Diversify its Energy Mix

For the long term however, it is not enough for Europe to simply diversify its gas supply routes. Avoiding Ukraine by building the Nord Stream pipeline to Germany or the South Stream pipeline into the Western Balkans and into Hungary and Austria will still make Europe dependent on Gazprom,

which is the unique supplier for these pipelines at the present time. Therefore, Europe needs diversification of its energy mix and not just its energy transportation networks. Here the debate revolves around four alternatives to conventional gas and oil.

- *The first is renewables, essentially wind and solar but including second-generation biofuels as well.* These are currently 15% of Germany's energy mix and the EU has just come out with a climate change policy to increase this to 27% for all EU countries by 2030. The problem with renewables however, is that they are not always available (for instance solar and wind) and as these are produced in only certain regions of the EU (wind in the north and solar in the south) a grid has to be constructed to distribute them to other parts of Europe. Also, whereas oil and gas can be stored for long periods, there is as of yet no equivalent system for storing renewable energy, which needs to be consumed quite soon after its production.

- *The second issue concerns shale gas.* Europe has potentially large quantities, especially in France and Poland but environmentalists' opposition to fracking means that, so far, almost none of this has been exploited. Three companies that were prospecting in Poland have now stopped their activities and exploration in Lancashire in the U.K. was stopped after a minor earth tremor. Although Europe has an estimated 26 years of gas supplies potentially available from shale, it does not look like following the United States at the present time into widespread exploration and production. Two EU states (France and Bulgaria) have outright bans on fracking, and Germany, Denmark, Ireland and the Netherlands have informal restrictions.

- *The third is nuclear.* Germany has decided to abandon nuclear power generation, which means that nuclear plants will be decommissioned in some cases 20 years before the end of their natural lifespan. Other countries, such as Belgium, the U.K. and Finland, are grappling with the issue of how to move to the next generation of nuclear power plants with all the associated costs, subsidies and environmental impact studies. Nuclear power is around 15% of the EU energy mix. If it goes down significantly, nuclear energy will need to be replaced by polluting fossil fuels or by renewables. For instance, Germany has started to use more coal since deciding to quit nuclear power and Germany's industrial energy costs are now three times higher than in the United States, which could persuade some German corporations to relocate outside Europe.

- *Finally, there is coal.* Europe still has abundant reserves of both brown and black coal and coal is available also cheaply from elsewhere; for instance from the United States in the wake of the shale gas and unconventional oil discoveries. Poland currently generates 90% of its electricity from coal and still employs 100,000 miners, which is one reason why it has sometimes been critical of ambitious EU CO2 reduction targets. Of course, if the EU were able to develop affordable and effective carbon capture and storage technologies, coal might become more publicly acceptable and useable.

What Europe Needs to Do

So, in a nutshell, if Europe wishes to diversify its energy supplies, it will need to have a serious debate about the way ahead with renewables, shale, nuclear and coal—none of which have a clear or secure future on the European energy policy scene at the present time.

In the meantime, there are many things that the EU can do and is doing, to increase the continent's energy resilience. I have mentioned already storage. An EU directive requires member states to hold oil supplies up to 90 days of imports or 61 days of consumption. Gas is being stored offshore, such as near Groningen. The EU has also introduced inter-connectors, so that countries can more easily supply others in the event of a blackout or crisis situation. It has pushed member states like Slovakia and Hungary to facilitate the reverse transit of Russian gas from West to East to help Ukraine during a period when Russia has stopped supplying Ukraine because of payment and other disputes. The EU

in its third energy package has also been stringent in applying competition rules to ensure that suppliers of gas do not also gain monopoly ownership of distribution networks. These measures have been used against Gazprom. In the future, the EU could also revise its directive on renewable energy in order to liberalize markets in the same way that it has tried to liberalize the EU internal gas market. The former Polish Prime Minister, Donald Tusk, proposed the bulk purchase by EU countries of Russian gas in order to negotiate better prices (Lithuania for instance pays one-third more for Russian gas than Germany). Even if this idea is not retained, the EU can certainly make more of the fact that Russia is as dependent if not more, on its European markets as the EU is dependent upon Russia for its supplies. 55% of Russia's gas goes to the EU and 75% of its gas reserves are in Western Siberia where the pipelines run west towards Europe and not east towards China. Despite much Russian hype about a pivot to Asia and the recent Russian-Chinese gas deal, four times more Russian gas will go to Europe in the next decade than will go to China.

"Former Polish Prime Minister Donald Tusk proposed the bulk purchase by EU countries of Russian gas to get better prices."

A Word about Ukraine

A deal between Russia and Ukraine brokered by the EU Commission will hopefully avert another gas crisis this winter and allow Russian supplies to Ukraine to be resumed. But the EU must use this opportunity to encourage Ukraine to fundamentally reform its energy sector. Ukraine spends 7% of its GDP on energy subsidies and its use of energy per unit of production is one of the highest in the world. Ukraine also has far less storage of gas than the EU and now faces the prospect of losing control of potentially rich gas fields off the coast of Crimea. So the EU will need to encourage Kyiv to move towards a more realistic pricing of energy and towards considerable energy savings. The fact that two thirds of Ukraine's coal comes from the Donetsk region, which is where the Russian-speaking separatists are active, makes this effort all the more urgent. Therefore, EU money should not be used in the long run only to subsidise Ukraine's wasteful use of Russian gas but also to initiate the economic and technical reforms that will make Ukraine's energy market less corrupt, more transparent and more efficient.

"Ukraine must reform its energy sector to move towards more realistic pricing and energy savings."

Economic and Political Aspects of the Ukraine and Russia Crises

Senator Alain Richard
French Senate (Val d'Oise); Former Minister of Defense of France

I would like to offer some reflections about the historic roots, both recent and less recent, of the situation concerning Russia and its neighbor, Ukraine. Today's Russia is the legacy of the Soviet Union. And this still influences its ways of thinking and making decisions. The Soviet Union was created after the Soviet revolution—which was based on a mobilization of the proletariat, which was very small compared to the bulk of Russian society of the time. But the Soviet revolution was also an alliance of nationalities. The Russian empire had conquered and subdued a number of smaller nations, and managed the relationship with all these nations in a basically authoritarian way. One of the strategic talents of the Soviets, and especially Stalin himself, was in organizing an alliance based on a concrete policy of nationalities.

"Today's Russia is the legacy of the Soviet Union."

The basic agreement in the years 1917-1920 was that the various nationalities had a right to independence, but they were offered a federal system that would protect their national rights, their right to secede, and of course their national culture. They agreed to be governed by the party, which was the unifying factor, and which of course overwhelmed all the rest.

The subsequent Soviet constitutions were very precise on the protection of different nationalities. There was an interesting detail, however. The design of the areas and borders of nationalities was managed by the central power and by Stalin himself for decades. So in1991, with the explosion of the Soviet Union, the basic components of the future nations were the republics created by the Soviet system in the 1920s. Ukraine is one of these republics, but the borders of this new Ukraine are fairly artificial. And Ukrainians are not perceived as a natural and real nationality by the rest of Russia. We all remember that the base of the Russian empire was Kiev, not Moscow. The Czars moved to Moscow in the 16th century. So, for many people in today's Russia, Ukraine is as much a historic part of Russia as it is an independent nation.

"Ukrainians are not perceived as a real nationality by the rest of Russia."

This ambiguity is one of the fundamental aspects of the present Russian policy for Ukraine. Ukraine itself—as seen by the world—is, in theory, a legally independent state. Yet, in many aspects it is under post-Soviet tutorship, under a certain control by Russia. The first element of this relationship was of course the dismantlement of the previous Soviet military system that was present in Ukraine. In 1991 or 1992, Ukraine was a nuclear power. This power had to be suppressed as such, and Ukraine had to consent to that.

"Ukraine is of interest to Russia, because it opens up the south of its territory to the Black Sea."

But other factors make this new nation state fairly fragile. I do not want to go on too far concerning the history, but the western borders of the Russian Empire had moved very frequently due to conquests and wars with the central European powers and with the Ottoman Empire during the 18th and 19th centuries. Thus, the territories covered by today's Ukraine possess very different histories, and the national unity of this country had to be constructed, because there was no common history—Ukraine had never constituted a nation state before recent times. In fact, for Russia, during the last two decades, Ukraine has been a very special area of interest, because it opens up the south of its territory to the Black Sea. Of course, Russia has its own access to the Black Sea, but it is fairly limited. And it is in a region that has been in economic crisis for quite a while.

And for Russians, the period of the Yeltsin era is now considered by 95% of the people as a period of decay, and a curse for the nation. It is one of the worst memories for Russians over the whole history of their country.

As soon as the Putin system replaced Yeltsin's, the challenge of recovering influence if not control over a large part of the previous empire and of the Soviet Union itself became a basic national challenge, a national goal. That is why Russia has always expressed its hostility toward the extension of NATO and the EU. (The hostility is in that order: NATO is a military body and so more provocative, and it is resented more since it is seen as more hostile to Russia than the EU, whose influence is largely in the economic field.)

"The Ukraine-Russia relationship was good as long as Ukraine showed no sign of joining NATO or the EU."

Russia has always considered the extension of NATO close to its present borders and the inclusion within NATO of its former partners of the empire as a very strong hostile signal. That explains why, in its relationship with Ukraine, Russia was basically cooperative during the last two decades. Russia always tried to control the central international choices of Ukraine, but the relationship was good as long as Ukraine showed no sign of wanting to join NATO or the EU.

To sum up, Ukraine is the center of what I could call the Russian neighborhood policy. In the EU, we officially have a neighborhood policy. Russia has one, too, even though it does not have the same inspiration, and it is less cooperative. And, until recently, Russia considered that Ukraine was making its international decisions in a satisfactory way (or at least satisfactory for Russia).

The economy was also an issue for a couple of reasons—for example, because of what Jamie Shea has said about energy in his presentation. Geographically, Ukraine provides a passage to export energy towards many countries.

Nonetheless, if Russia wants to have a serious and structured area of influence, it must be based on an economic zone. And Russia has been trying very painfully to build such a zone with few successes—trying consistently to build a proper economic zone that it would lead. If possible, it would like to have a zone that would be of more or less the same status as the European Union. At the very least, it would need to be equivalent to other economic cooperation and free trade areas. And for this, of course, Ukraine is a basic component—especially if you look at what the balance can be with Russia itself, plus Belarus (10 million inhabitants and a level of economic development which is not

very viable), plus Kazakhstan, which is of course a serious economic power, but only as an energy center.

If you bring Ukraine into this unity, however, you have expanded it by one third. So the idea that Ukraine might even gradually and cautiously grow closer to the EU, become a partner that could one day be part of the European Union—or at least be strongly linked to it—was also a signal of the future failure of an essential Russian ambition at the economic and political level. So the present challenge for Russia is also revealing how Russia is preparing and designing its decisions and strategy.

"Ukraine's possible entry into the EU was a signal of the future failure of an essential Russian ambition."

The Russian regime, as it now exists, has gained authority and successes which basically result from the achievement of renewed and reconstituted prosperity after the Yeltsin era.

For most Russians, President Putin represents a recovered sense of dignity and basic economic and social stability. For those who experienced the level of salaries in Russia in the 1990s, the chaos, the unpredictability, or even social status, it was shocking. Thus, you can see that the simple fact that Putin has been able to recreate a basically stable environment for day-to-day life for citizens and their families is a serious success. And there has been progress in law and order—even if it is a special kind of law and fairly brutal, because the Yeltsin era was also considered to be a period when everyone was stealing. It was a time when even the authoritative order created by the Soviet Union was challenged and refused by many people and especially by the oligarchs.

"For Russians, President Putin represents a recovered sense of dignity and basic economic and social stability."

So the credibility of this regime is now based on prosperity and—as Jamie Shea said—exclusively on exporting energy. Russia is less and less competitive in all other areas, even including the remainder of the "jewels" of the former Soviet technology, like space for instance. Russia used to be much more competitive and much more reliable when I was in office 15 years ago than it is today. So they are losing ground, except with money provided by gas and oil.

And I would also mention national assertiveness. There is a reconstitution of national pride and the feeling that they are recovering at least part of the authority of one of the great powers—as we have seen in the few areas in which Russia is a cooperative partner, like dealing with Iran on nuclear issues, for example. Everything that entitles Russia to think of itself as one of the great powers, with a status at the same level as that of the United States, is of course essential to them.

"Russia can be a cooperative partner, for example, in dealing with Iran on nuclear issues."

There has been a slow evolution in Ukraine, moving toward the EU and potentially toward NATO—since the discussion about joining NATO has now taken roots in Ukraine society. So the risk of Ukraine becoming more durably separated from Russia is resented as a danger for this regime.

In Ukraine, the sense of national unity was very fragile for historic reasons, but also fragile because of the dreadful balance sheet of various Ukrainian governments over the last two decades. As a result, Ukrainians are now paying for the bad government that has been quasi-permanent in their country for this short period of independence.

Apart from the Russian-speaking citizens of Ukraine, those of Russian culture, who legitimately and naturally are hesitant about their relationship with the two nations, there are also people who consider themselves to be Ukrainian but see that salaries and pensions in Russia are getting paid, whereas, in Ukraine, you never know if they will be paid. So the moment when the shock appeared between Russia and Ukraine, based also on serious civil confrontations, the outcome was truly serious.

What are the challenges for the Alliance and for Europe? I will be very simple and simplistic. First, we must defend international law in Ukraine—and even if it is Russia that is really challenging (or trodding on) international law. Russia must be sanctioned; it must be opposed on this.

"We must defend international law in Ukraine—Russia must be sanctioned."

We have to defend it, even if the present situation there is not very encouraging. We have to support the fact that Ukraine is an independent country, which is entitled to make its own choices and to make its own decisions over its economic relationship and its alliances. And we have to show Russia the relative disadvantage of being constantly negative and constantly hostile compared to the advantage of being cooperative.

Today, they are hostile on most issues, but they are cooperative on some. So, we have to develop a strategy—and it needs to be a common one—showing that, IF they choose hostility and non-reliability, there will be heavy costs for them. They need to see that their evolution in the longer term will be really threatened if they do not behave as a normal partner. And, on the other hand, they need to see that, if they come to terms with international law and accept the independence of their neighbors, of course, they can have a significant international influence, be a true partner, and be respected as such.

"Russia needs to see that it can have a significant international influence, be a true partner, and be respected as such."

Defence Investment: Reversing the Trend

Lieutenant General Patrick Auroy
Assistant Secretary General for Defense Investments, NATO

Presented by Mr. E.J. Herold

Introduction

The North Atlantic Alliance is faced with new challenges in both its Eastern and Southern neighborhoods: The Ukraine crisis and aggression by Russia on one flank, and the growing challenge of terrorism on the other flank. These challenges are complex and wide-ranging. They are game changers, just like cyber security, the other main topic of this workshop, and just like, beyond the defence area, the spreading Ebola virus. Such challenges require international responses based on effective capabilities delivered in a timely manner. In other words, we need to organize ourselves in ways that match the dimension of the challenges that we have to solve. In my view, this is an approach applicable to all areas and it re-imagines a modern definition of the concept of sovereignty.

"The Ukraine crisis and the terrorism are game changers, like cyber security."

But let me now focus on defence investment in light of the crisis in Ukraine. My starting point is twofold: NATO fully supports an independent, sovereign and stable Ukraine. At the same time, NATO desires to maintain a constructive relationship with Russia, which is currently in breach of its obligations under international law.

To do these two things in an effective way, NATO needs to be strong. To be strong as an Alliance of 28 countries; and to be strong through enhanced engagement with its partners. In both areas, Defence Investment matters.

A Strong Alliance

Spending More. The NATO benchmark for national defence budgets is 2% of Gross Domestic Product. And within those national defence budgets, the benchmark for Defence Investment is 20% expenditure on materiel re-capitalization including Research & Development. Only a few Allies met this benchmark in 2007 and less in 2013. At the Wales Summit, NATO leaders agreed to reverse the trend of declining Defence Investment, as a key contribution to our overall security. The Wales statement is quite a powerful one; it has no precedent at Head of State and Government level.

In practice, understandably, some Allies and partners, notably among those closer to the frontier with Russia tend to be faster at answering this call. They are speeding up the modernization of their defence capabilities and increasing their defence budgets. It is no secret that some of these countries still own legacy equipment of Soviet origin. This is not ideal for materiel interoperability among the Alliance. But more importantly, these countries are now concerned about their dependence on Russia for the maintenance of this equipment, and about the loss of strategic autonomy that this could create. This is in a way similar to the issue of European dependence on Russian gas. Regardless, the result is that Allies are now working on mitigating the risks created by this situation.

"Some countries still own legacy equipment of Soviet origin—it is not ideal for interoperability."

Another consideration related to increasing Defence Investment is the question of what this is going to change for industry. To be frank, I would say, "if nothing else changes, not a lot". This is a lean period for the defence industry. As a result of the pledge at the Wales Summit, we can expect, on

average, a slow increase of defence investment from Allies in the years to come, not a sudden windfall. Salvation will not come from increased budgets. To remain as strong as we need it to be, the defence industry will have to continue to find efficiencies, including through specialization of national competencies and consolidation in Europe. Industry will have to succeed in increasingly competitive export markets and, when possible, to find civilian markets for its products. We all know this already, but it will largely remain wishful thinking if politics and policies keep hindering efforts for consolidation and export. The imperative is for organizing ourselves, as I said in introduction, on a magnitude that matches that of the challenges we face.

Spending better. Defence Investment is not only about "spending more" but about "spending better." Let me explain by describing both the substance and the process I have in mind to achieve this.

- On substance, the question is where to spend. The Wales Summit approved a list of priority capabilities on which Allies will focus in the near to longer term. While considering the immediate and long-term effects of the Ukraine crisis, their impact is still to be fully realized. So focusing on these Wales priorities will enable NATO to prepare to address a wide range of current and future challenges. For instance, it is no surprise that Intelligence, Surveillance and Reconnaissance, cyber defence, and Command & Control are on this list. And part of my job at NATO is to facilitate consistent delivery across the Alliance on those capabilities.
- On process, we ask the question how we can all spend better? The Smart Defence initiative, and the steady progress of Joint Intelligence, Surveillance and Reconnaissance capability development, shows that multinational cooperation is more and more the technique of choice to get the most out of our defence investments, delivering the required capabilities at the right time and at the right cost. I see this trend not only in NATO, but also in other frameworks such as the European Defence Agency, Franco-British defence cooperation or the activities in NORDEFCO. And by the way, I should mention that the good cooperation between NATO and the European Union is helping to optimize defence investment.

We must ask the question, "How can we all spend better?"

A spinoff of cooperation between nations is that it facilitates the industrial cooperation and consolidation I mentioned earlier. In the end, I believe this will be the only way to maintain a strong defence industry across the Alliance, the only way to ensure capability delivery, not just now but in the longer term.

"Effective collaborations are ones which initially include few members—some call them 'minilateral'."

Multinational cooperation does not, however, guarantee success. One quick point here, on cooperation formats. My view is that the most effective collaborations are the ones which initially include very few members—maybe 2, 3, 4—some call them "minilateral" formats. As projects grow in strength and maturity, they can be extended to other willing and capable players.

Enhanced Engagement with Partners

Let me now turn to my second topic. NATO's partnerships play a crucial role in building stability across the globe. This is why enhanced engagement with partners is one of the conditions for a strong and effective NATO.

And indeed partnerships stand out as a very important element from the NATO Summit. Defence Ministers inaugurated a new format which bridges across the current partnership frameworks—Partnership for Peace, Mediterranean Dialogue, Istanbul Cooperation Initiative, etc. The Interoperability Platform involves 24 partners from around the globe[4] who have shown their

[4] Armenia, Australia, Austria, Azerbaijan, Bahrain, Bosnia and Herzegovina, Finland, Georgia, Ireland, Japan, Jordan, Kazakhstan, Republic of Korea, Republic of Moldova, Mongolia, Montenegro, Morocco, New Zealand, Serbia, Sweden, Switzerland, the former Yugoslav Republic of Macedonia*, Ukraine, and the United Arab Emirates

commitment to pursue interoperability with NATO. Practical cooperation is now being taken forward in this format, particularly in the Defence Investment area and the outcome could well be greater materiel standardization. This should be of interest to industry, I would think.

The Summit also launched a Defence and Related Security Capacity Building initiative. With this initiative, NATO will improve the support, advice and assistance it provides to partners. The goal is to contribute to security and stability and to conflict prevention, to develop stability without deploying Alliance forces.

"The goal is to help Ukraine provide for its own security."

In the current situation, enhancing engagement with partners naturally implies enhancing practical cooperation with Ukraine. The goal is to help Ukraine provide for its own security, and to improve the ability of the Ukrainian and NATO forces to operate together. We are now in the process of launching substantial new programmes. Those relevant to Defence Investment focus on Command, Control, Communications and Computers (also known as C4); on logistics and standardization; and on cyber defence. But NATO and Allied support to Ukraine goes far beyond the area of Defence Investment. It includes for instance medical treatment of wounded soldiers, participation of Ukraine in NATO exercises, and military career transition management.

Concluding Remarks

To conclude, let me say that the Ukraine crisis has reinforced for Allies that security and stability do not come without proper defence investment.

Alliance priority capabilities have been clearly defined at the Summit, and are guiding our investment decisions. Multinational cooperation in effective formats is more and more becoming the preferred capability delivery mode. And engagement with NATO partners plays an increasingly important role in achieving NATO goals and objectives.

In short, Defence Investment remains an essential enabler for the security and stability that NATO provides to its members. And the relationship with our partners remains a top priority for the Alliance.

* Turkey recognises the Republic of Macedonia with its constitutional name.

Bringing Order to Chaos: How Nations Confront the Challenges of Unstable Environments

Mr. E. J. Herold
Deputy Assistant Secretary General for Defense Investment, NATO

As nations and multinational organizations like NATO, EU and the U.N. confront emerging challenges that seem to grow more frequent and more complex, defence capacity is strained to its limits. With budget pressures as a complicating factor, how do governments respond to uncertainty? The lesson of recent years suggests that a better understanding of technological advances coupled with clearer notions of national goals and collaboration with like-minded partners can lead to increased capacity to respond to known threats and unexpected circumstances. Greater cooperation with existing partners and willingness to embrace new ones is part of the solution. More transparency in the dialogue with industry is another way to derive benefit from technological progress within budgetary constraints.

Budgets: Although It may Look like We still Spend a Lot, We Need to Spend more

Budget pressures are very real. However, Allies still account for the largest part of the world's defence expenditures. So what is the problem? Overall, doesn't the Alliance spend enough on defence?

In 2003, Allies accounted for 69% of world's defence expenditures. In 2011, this figure was down to 60%, and, for this year, it could be around 55%. Although decreasing, these overall figures are still at first glance rather reassuring. But if you examine them in more detail, you may reach a different conclusion.

"Can we accept losing our technological edge in the air, at sea, on land, in space?"

The Alliance has guaranteed the security of its members and contributed to the stability of the world through political and military means, backed by *superior defence capabilities*. Such superiority comes at the price of our defence expenditures. And *superior defence technology* is one of the drivers of this price. Can we do differently? Can we accept losing our technological edge, losing our superiority in the air, at sea, on land, in space? You can guess what I think about this, so let me quote somebody else:

> "The one who possesses high-tech superiority will have the upper hand on the battlefield."
>
> "Defense science, technology, and industry are the major material bases on which we can realize our army modernization."

Do these points sound familiar? Probably so. But where do these quotes come from? From General Ding Henggao, China, and they were written 20 years ago. So it is a widely-shared and not really new point of view that cutting-edge capabilities delivered by a strong defence technological and industrial base are key to operational superiority.

So, yes, the Alliance wants to stay ahead in the innovation race. Yes, the Alliance wants its defence industry to stay at the forefront of technology, with proper delivery capacity. And, yes, the Alliance has to accept the price tag. Because the other option would lead to less stability and security, and in the end would prove much more costly. All the more so at a time when, in many areas of the world, we see defence expenditures grow. To mention only Russia, in September, President Vladimir Putin announced the development of an array of new nuclear and conventional weapons to counter recent

moves by the U.S. and NATO.[5] According to these plans, the Russian government has appropriated 22 trillion rubles ($730 billion) over the next decade for modernization of the Russian military. Of that amount, roughly $650 billion will be spent on new equipment. [6]

"The Russian government has appropriated $730 billion over the next decade for modernization of its military."

This is why I see the Wales Summit pledge on Defence budgets and Defence Investment as so important. At a time of increasing unpredictability and risk, insurance policy premiums have to go up.

Two Key Pillars to Help Deal with an Increasingly Complex and Uncertain World: Preparation of the Future and Cooperation

Let's look into the longer term now. If the defence spending trend I presented remains valid, the ratio of Alliance's to world's defence expenditures will drop below 50% in a few years. This might be perceived as a psychological threshold below which the Alliance could be seen as in decline. But more importantly, if the trend continues further, at some point the question will become what are we going to leave to our children, to the next generations? Don't we owe them at least the same level of security as the one that our fathers built and that we are enjoying now?

"Europe needs to enhance its level of defence science and technology investment and increase its effectiveness."

This brings me to preparation of the future, to science and technology. The S&T transatlantic gap is increasing: S&T budgets' decline is said to be putting Europe's technological and industrial base at risk. The U.S. outspends Europe by about six to one in defence R&D. Moreover, R&D investment in Europe is fragmented, leading to duplications. And there is also an intra-European budgets and industrial capabilities gap. All European NATO members do not punch in the same category at all.

S&T is maybe the area where the transatlantic gap is the deepest, and this is of concern to me because it is about compromising future solidarity and burden sharing. I believe that Europe needs to enhance its level of defence S&T and increase the effectiveness of this S&T.

This should include more pooling and sharing of defence S&T of course, but also of defence and civilian S&T, which are more and more overlapping, to provide access to a larger pool of knowledge and of resources. The need to pool and share, to cooperate in order to be effective, holds for defence S&T. It holds more generally in the defence area.

It also holds more broadly. As an American man speaking in Paris, I cannot help but quote a French woman who spoke (and works) in Washington. In a speech on October 10, Christine Lagarde, the Managing Director of the International Monetary Fund, said that to "deliver the jobs, the incomes, the better living standards that people aspire to", what was needed was collective action, including what she called the choice of solidarity over seclusion, of "strengthening cooperation and multilateralism, instead of isolationism and insularity".

That is not very different from what we need to do in the defence area. The Wales Summit Declaration clearly acknowledges that cooperation of the Alliance with partner countries and with

[5] The weapons modernisation program for 2016-2025 will focus on building a new array of offensive weapons to provide a "guaranteed nuclear deterrent," re-arming strategic and long-range aviation, creating an aerospace defense system and developing high-precision conventional weapons. This is on top of the modernization plans unveiled in 2013.

[6] This grand procurement and restructuring program includes 100 new naval vessels, 600 new warplanes, and 1,000 new helicopters, to be delivered by the year 2020. Moreover, the Russian Armed Forces have been increasing their level of exercises, improving their command and control and, overall, working on removing the shortcomings that manifested themselves during the 2008 war with Georgia.

other organizations is essential. One of the reasons for this is the need to respond to the increasing uncertainty brought by more complex and global challenges. To respond to such increasing complexity, our organizations, and our "organizations of organizations" are also, inevitably, becoming more complex. The more countries in a coalition, for instance, the higher the level of complexity of operations. Such complexity is necessary because it brings advantages such as broad political support of an operation. But there is also unnecessary complexity, such as in processes, role definitions, or unclear accountabilities that must be eliminated because it only leads to chaos.

This is no piece of cake, as the economist E. F. Schumacher put it—and I will conclude with this quote: "Any intelligent fool can make things bigger, more complex, and more violent. It takes a touch of genius—and a lot of courage to move in the opposite direction."

PART TWO: CYBER SECURITY

Digital Security and Digital Freedom from Zero-sum to Win-win

Ms. Marietje Schaake, MEP
Member of the European Parliament (The Netherlands)

Ms. Marietje Schaake, Member of the EU Parliament: Major General David Senty, MITRE Corp. and Mr. Gary Gagnon, MITRE Corp. (left to right).

Introductory Remarks

I have been serving as a member of the European Parliament since 2009, working mostly on foreign policy, international trade, and technology issues. Thank you to all who made this event possible for including me and for allowing for what will be hopefully an interactive session with this audience of experts in the field of defense, technology, and politics. The previous panel showed that security sometimes takes awfully familiar patterns, but sometimes there are also new arenas, including cyber. Although I do not like the "cyber" term very much, I do think that the need to protect and advance people's freedoms and the open society are goals that we should agree on.

Security and Freedom Should Not Be a Zero-Sum Relationship

As politicians, as generals, we have constitutional responsibilities—which are sometimes agreed upon multilaterally in various forms of cooperation—to defend people, systems, critical infrastructure and territories. In any case, we are obliged to defend the open society against attacks from the outside. At the same time, we should be very wary of eroding open societies from within. I am afraid that in the digital reality, the relationship between security and freedom has become too much of a zero-sum relationship.

The speed of technological developments has led to legal and regulatory vacuums, from the use of drones to offensive capacities in cyber. There is also a question as to whether an attack on one is considered an attack on all when it happens in the digital domain. These questions remain wide open. In many of these cases, we are not sure about legality or jurisdictions. Very often, we do not need entirely new laws or entirely new frameworks, but we should ensure that the core democratic principles apply and are reinforced in these new arenas: Checks and balances, protection from the state and possibilities for redress, democratic and judiciary oversight,

"We should ensure that core principles apply…Checks and balances, protection from the state and possibilities for redress, democratic and judiciary oversight, proportionality, and competition."

proportionality, as well as competition.

All these principles require an integrated approach, which should be increasingly cross-border. They should also be integrated to the extent that they are not confined to military headquarters. The reality is that much of the dynamics that are now developing so rapidly extends beyond the territory and the jurisdiction of nation-states. This presents new challenges.

There is a new role for companies that are producing critical products or services used globally by millions and millions of people—Internet users that are empowered by gaining access to information, having potentially more freedom of expression, as well as the freedom of assembly. But these empowered individuals, connected worldwide on the Open Internet, are also faced with surveillance—sometimes mass surveillance, censorship, tracking and tracing, and intrusion technologies. And increasingly governments, particularly at this moment in time, rely heavily on private actors for the protection of critical infrastructures or for using these services themselves. So there is a whole different relationship between private actors, commercial companies, and individuals and governments.

"The most impactful intrusive technologies are becoming cheaper, faster, and smaller and available in a free market."

Governments do not have a monopoly on the development and use of the most impactful technologies. Consequently, it is especially important to realize that it is an illusion to think that we, in the EU for example, or in the democratic societies of this world, will be leading in the development of these technologies until the end of time. A lot of the most impactful intrusive technologies are becoming cheaper, faster, and smaller every day and are available in a free market. And the risk of proliferation is already a reality and I think this risk is not acknowledged sufficiently.

"Anyone who wants to can buy the most impactful technologies, including non-state

Some Key Strategic Questions

This leads to risks of human rights violations globally but, in this context perhaps more importantly, to key strategic questions. If you look at the risks of proliferation, we see that there are, at least in principle, unlimited buyers in this unregulated market. Anyone who wants to can buy the most impactful technologies, including non-state actors. There is also the risk of corporate overreach. When companies can develop ever more impactful technologies that are not bound by any regulations, where does this lead us? Where does it leave those who seek to defend societies and nation-states? Where does it leave the Internet users themselves?

We have seen that there are EU standards concerning lawful intercept technologies. Therefore, the notion that law enforcement officials should be able to gain access to mobile networks, for example, is enshrined in European laws and standards. But, if you transpose these technologies and systems into societies where the rule of law does not exist, what does it do to the notion of lawfulness? Or, what if these systems are sold to countries that become our adversaries or, if they are sold to telecom operators that may become hostile to us in the EU? What if these systems are put in a context where technical backdoors can be opened at any time by those in power?

As James Clapper has already said, lawful intercept technologies—bought or developed and sold from the United States—have come back as a boomerang and have been used against the United States. So it is also being acknowledged that this boomerang effect is really very, very, important.

Where Regulations Are Needed

Consequently, I think we need more precise regulations when it comes to trade in dual-use items, and in the kinds of technologies that I mentioned above. We need regulations that address not only technical standards but also the context in which such systems will be used and their potential for

extra-territorial impact. Many of these systems and technologies have global impact already, and we should take that into consideration.

Vulnerabilities in software, which are discovered every day, provide one example. It is in the public interest to find quick solutions or patches. Consequently, there should be reporting standards for vulnerabilities, so that solutions can be found faster. If you look at it from companies' perspectives, however, their main interest may be to prevent reputational damage or to keep costs down. So, they may be reluctant to report vulnerabilities or attacks. In other words, there is a conflict between the public interest and corporate interests.

"Markets in vulnerabilities need to be regulated, but it is difficult when both governments and companies are buyers in the same market."

Currently there is a free market for vulnerabilities. I do not think that I have to explain to anyone in this room what zero-day threats are—they are holes in widely-used software or systems that are thus far undiscovered and that can be used and abused to gain access. Such markets need to be regulated, but it is very difficult when you face the reality of both governments and companies as buyers in this market alongside non-state actors. In fact, we do not really know who is buying and selling in this market, although we know that prices are being driven up. We also know that the public is at risk when systems that are used by millions of people every day are not protected, and, in fact, are potentially used to gain access to people's devices without them knowing it.

Stronger Efforts Are Needed at the Research and Development Stage

In general, we need much stronger efforts early on in the research and development phase to assess impacts on human rights. We also need strategic impact assessment as to what technologies can become down the road. As a liberal, I do not want to over-regulate research; I do not want to over-regulate markets. Yet, I think that there is an irresponsible vacuum at the moment that we have to acknowledge and deal with more responsibly.

There are examples where research has led to taking information out of the public domain. For example, in the research on biochemical weapons, PhD. candidates have been asked not to publish their research because it would be dangerous for the public.

As some people argue, software may well be speech, but we should still consider what the collective impact can be of putting every speech out in the open.

In any case, I think we need a licensing mechanism. In the EU, for example, we need to look at the technology that a company wants to sell, to where and to whom, and make sure that we have a level playing field in Europe. At this moment, there is still a big gap, for example, in how member states enforce sanctions or dual-use regulations. I think we need a smarter licensing scheme that goes beyond the Wassenaar Arrangement, which has been updated recently and is probably going to be implemented in the EU very soon.

Concluding Remarks: Let Us Harness the Potential of the Open Internet to Move from Zero-sum to Win-win

In concluding, I would like to say that we clearly see increasing tensions between jurisdictions that are rooted in the nation state where, in principle, we have a rule-based system, and, on the other hand, a hyper-connected reality which is still largely unregulated and where there are a number of new sovereigns—not only companies, but also internet users, and non-state actors.

Open society should take the lead to make sure that we harness the potential, which is still great, for developing the Open Internet further; there is a great deal of social, economic, and political potential that is still untapped. Democratic values and norms should be at the heart of efforts by open societies

to make sure that the Internet stays open and global—which is by no means a given—so that the people using the Internet are protected from both corporate and governmental overreach and abuse.

"Democratic values and norms should be at the heart of efforts to make sure that the Internet stays open and global."

At the very least, we should not allow an erosion of norms that undermines our credibility globally or that allows for an irresponsible legal vacuum that could lead to very dangerous and unmanageable situations such as the potential proliferation mentioned above. We should move away form a zero-sum relationship between freedom and security to a win-win situation. This is certainly possible, but it will require much more leadership than what we see today.

Cyber Security as a National Priority: the Case of France

Senator Jean-Marie Bockel
French Senate, Former Minister

Translation by Dr. Roger Weissinger-Baylon

INTRODUCTION ON THE STATE OF THE CYBER THREAT

In July 2012, I presented a report on cyber defense, entitled "Cyber Defense: A Global Challenge, A National Priority." Since that time, the theme of cyber security has continued to grow in importance. Attacks against information systems have actually multiplied over the last few years. According to figures from Symantec, between 2012 and 2013, there has been a 91% increase in the number of attacks targeting companies and institutions. France has not been spared by this phenomenon, as we can see from information attacks against the Ministry of Economy and Finance, AREVA, and even the Elysée (citing only those attacks that have been reported in the press). One can expect a growth in the number of attacks against information systems in the future, given the development of the role of the Internet and information systems in all sectors. Today, portable telephones, computers, and tablets are linked to the Internet and, tomorrow, to objects ranging from cars to pacemakers will also be linked. That is why I have recommended in my report to make this issue a national priority.

Given the rapidly growing threat, I have recommended that cyber security be a "national priority."

MILITARY PLANNING LAW 2014-2019: CYBER SECURITY AS A NATIONAL PRIORITY

Where are we now as to the most recent White Paper and the Military Planning Law (LPM 2014-2019)? In accordance with the direction set out in the new White Paper of 2013, which raised cyber security to the level of a national priority, the LPM has an entire chapter dedicated to the protection of information systems against the cyber threat. The LPM contains new guidelines but also foresees, in an annexed report, the strengthening of human and financial means.

An Important Aspect of the Guidelines

Among the different guidelines related to cyber defense, the most innovative ones are those concerned with organizations of critical importance (approximately 250, belonging to the public or private sectors). Four principal measures are foreseen in the text of the LPM to reinforce the security of the information systems of these organizations.

"Critical organizations must report significant cyber incidents, under penalty of sanctions."

First, the LPM foresees the obligation for these critical organizations to report, under penalty of sanctions and with a guarantee of confidentiality, all significant incidents involving information systems to the National Agency for the Security of Information Systems (ANSSI - Agence nationale de la sécurité des systèmes d'information).

Second, the LPM also gives the government the right to require critical organizations to follow standards of information security, which will be defined sector by sector, in consultation with the organizations that are concerned. It will involve for example the obligation to install systems for the detection of attacks against information systems.

The government will have the right to conduct audits for information security—or impose drastic measures in case

Third, the government will have the right to conduct audits or inspections for information security, which is already the case for the physical security of facilities that are potentially dangerous.

Finally, the LPM foresees the ability of the government, in the case of a major crisis in information systems—for example a destructive virus infection affecting our most critical infrastructures—to impose drastic measures such as the de-connection of their information systems from the Internet.[7]

A Significant Strengthening of Human and Material Resources

According to the recommendations of the Senate, the personnel of ANSSI, which should reach 500 agents by 2015, will be continually increased, to the same degree as our principal European partners. The resources of the ministry of defense dedicated to cyber defense will continue their growth in capabilities with the recruiting of at least 350 additional staff members for the period of 2014-2019. Likewise, the cyber security staff at the department of armaments (DGA) will be significantly increased, mainly in the heart of the DGA center for information management located at Bruz. It will reach the level of 400 specialists at a high technical level between now and 2017. Finally, the ministry of defense created a few months ago a "citizen cyber reserve," which already includes more than 60 active reservists, and, as foreseen in the White Paper and the LPM, an "operational" cyber reserve should be set up very soon.

This reinforcement in cyber defense also involves capabilities. In the framework of the LPM, the resources allocated to the acquisition and the operation of equipment dedicated to cyber security should increase strongly and reach a level of 360 million euros for the period of 2014-2019.

In addition, the budgets allocated to research and development in the cyber domain should significantly increase. The minister of defense has announced a tripling of these budgets, which could reach an annual amount of 30 million euros.

SEVERAL AREAS APPEAR TO BE PRIORITIES TODAY

The Development of a True Industrial Policy

Just as there exists in France an industrial and technological base for defense (BITD), there should also be an industrial and technological base for cyber (BITC). It is truly a matter of national sovereignty, in order to guarantee the security of our critical infrastructures, but also in economic terms, with at stake thousands of highly qualified employees that are not likely to be outsourced to other countries. While our country possesses true "national treasures" and excellent technical "savoir-faire," the sector of French suppliers of solutions for information system security has several gaps: Too much fragmentation, limited access to government purchasing organizations, and a strategic positioning that is too "franco-français."

The French cyber industry suffers from "fragmentation, limited access to government purchasing, and a strategic positioning that is too 'franco-français'."

[7] The decrees of application for LPM (article 22) are currently being finalized and should be published between now and the end of the year.

ANSSI has also begun to draft the security standards that will be applied to the organizations of critical importance (OIV). They will be published, between now and the end of the year, in a series of regulations applicable to the various areas concerned.

The Agency will publish several calls for public comment, which will be useful for future " trusted suppliers," for such activities as audit, detection, incident response, or suppliers of cloud services.

It is necessary to reinforce communication between the government and companies, favor the emergence of national or European "champions," and even establish an actual industrial policy at the European level. In this respect, I am pleased by recent initiatives, such as the "Cyber Defense Pact 2014-2016" or the "Plan 33" or the "The New Industrial France", that address several points: Supporting exports, strengthening national structures, developing supply and demand, etc. We soon expect to receive a plan with the actual numbers.

Strengthen Awareness and Training

Today, there are few engineers specialized in the protection of information systems and companies find it difficult to recruit them. We need to emphasize the education and training and develop the links between universities and research centers. To me, it seems indispensable to reinforce the awareness of the public and of organizations of the need to respect the elementary rules of security i.e., hygiene for computers and information systems (which, unfortunately, are often seen as interference by users).

Establish a European Approach to Cyber Security

Even if cyber defense must remain a primary responsibility of states because it directly affects national sovereignty, it seems essential in any case—since it is a threat that crosses national borders—to strengthen European cooperation in this field.

"The EU will also impose obligations to notify intrusions into critical infrastructures."

For government administrations, companies, and organizations of critical importance, the European Union needs to plan norms for industry, research and development, and measures for training and the development of public awareness. The EU developed in 2013 a European Strategy for Cyber Security and a directive (Network and Information Security) is now being examined. This will create a requirement to notify intrusions for organizations that "possess, use, or supply critical infrastructures." It seems indispensable to me that the European Union strengthen the protection and the defense of its own networks and its information and communications systems.

Strengthen International Cooperation

France must develop in parallel its bilateral partnerships with European countries, and especially with the United Kingdom and Germany. Cyber defense is based on trust and it is easier to depend on bilateral cooperation than on cooperation with twenty-eight countries (given the risk of a "weak link.")

This cooperation already exists between specialized government groups, or bilaterally with our British or German partners. It is now on the agenda of international organizations such at the U.N. or the EU.

There are, nonetheless, two opposing conceptions at the international level: Western countries wish to preserve an environment of freedom on the Internet, while countries like Russia or China are concerned by the growing role of social networks and want to strengthen control, not only over systems, but also over the actual content of communications—a position which is naturally unacceptable to western counties.

In any case, while international cooperation is essential, notably with our British and German partners, we must not have too many illusions: There are not really any allies in cyber space.

The revelations of the ex NSA consultant Edward Snowden concerning the magnitude of the American program of information espionage, PRISM, certainly reveal a practice that is unacceptable on the part of a country that is a friend and an ally and the need to create a "code of good conduct."

Executive Summary of Cyber Security Discussions

Dr. Linton Wells II
Distinguished Senior Research Fellow, Cyber Initiative
Middlebury Institute for International Studies at Monterey and National Defense University

Admiral (ret.) Jean Betermier, Director of the Forum du Futur, and Dr. Linton Wells II, Distinguished Senior Research Fellow, National Defense University and Middlebury Institute of International Studies (left to right).

The 31st International Workshop on Global Security was held in Paris on October 27–28. It was a very rich and informative event, with 44 presentations focused on the theme of "New Challenges to Global Security: From Russia post-Crimea to Cyber Security post-Snowden." This summary emphasizes cyber security discussions and related issues.

Twenty-four speakers addressed cyber issues, included former Ministers of Defense, Members of the European Parliament, senior representatives of NATO, the European Union (EU) and national governments (France, U.S.), executives from nine companies, and academics from sponsoring institutions. The workshop was conducted under the Chatham House rule, so this paper summarizes the various presentations without identifying individuals. The cyber topics focused on five broad areas:

- Underlying Trends in Cyberspace and Related Areas,
- Transnational Cyber Positions (EU, European Parliament, NATO),
- National Cyber Positions (France and the U.S.),
- Private Sector Positions (nine companies),
- Policy, Legislative and Regulatory Issues.

Underlying Trends. Cyber issues are not stand-alone questions—they need to be considered in the context of an increasingly complex, poly-centric and volatile security environment. Within Europe there are significant differences in security interests, with northern and eastern countries focusing on threats from the east while southern and eastern countries focus more on challenges such as immigration and political instability. Budget pressures are undeniable. Though NATO partners still account for the largest part of the world's defense expenditures, few member states meet NATO's standard of 2% of GDP for defense, 20% of which is for investment, producing forces that are 80% deployable. Alliance contributions to politico-military stability must be backed by military capability if they are to be effective.

Although cyberspace incidents date from the late 1980s, one thing that is new is the advent of hybrid, asymmetric operations that leverage the 24/7 news cycle and social media. Cyber issues are gaining attention in both Europe and the U.S., but much remains to be done. Governments cannot operate effectively in cyberspace by focusing solely within their own borders. They also cannot be effective without industry. Partnerships are essential. Moreover, although many parts of cyber security have global characteristics, the threat, and the perception of it, changes from sub-region to sub-region. The legal framework is important. Traditional espionage is not illegal, but cyber crime usually is. There are also issues of technical literacy. Policy makers often are not familiar with technology and technical specialists know little of the policy context in which their handiwork is used. In the future, any commercial component of a cyber security solution will have to shift more of the onus to companies, vice the consumer.

"Governments cannot operate effectively in cyberspace by focusing solely within their own borders and cannot be effective without industry."

Any action should be considered as part of a dynamic, evolving mix of cooperation, competition and conflict. Responses must be flexible and iterative. Mutual dependencies should be examined and leveraged, and assumptions challenged. Any effective approach will have to be networked, and include civil and military, government and non-government, domestic and international participants. In this environment, strategic foresight is essential to anticipate the broad range of strategic conditions that might evolve, vice just extrapolating forecasts from present trends.

"Strategic foresight is essential, instead of just extrapolating forecasts."

There was a very rich discussion during the various question and answer sessions about cyber security in the post-Snowden, post-Crimea environment. Key topics included: Privacy, encryption, law enforcement, and operating practices.

Trans-national Cyber Positions

- *European Union (EU).* The EU's cyber policy objectives extend beyond defense, to fighting cyber crime for example. The first EU cyber security strategy was issued in 2013, based on five principles: (1) The EU's core values apply as much in the digital world as in the physical one, (2) protecting fundamental rights, freedom of expression, personal data and privacy, (3) access for all, (4) democratic and efficient multi-stakeholder governance, and (5) a shared responsibility to ensure security. The EU's goal is to uphold existing international legal principles, vice trying to develop a new U.N.-level treaty or convention. The EU supports cyber confidence-building measures (CBMs) in which a key principle is transparency, as well as capacity-building on many levels. The EU is also working towards complementarity with NATO. Cyber threats are moving quickly into areas where there are no laws, police or effective governance. The term "active cyber defense" was used in several different contexts during the workshop, without precise definition.

"Cyber threats are moving into areas where there are no laws, police or effective governance."

- *European Parliament.* A key European theme is to ensure people's freedoms and an open society while also maintaining security and protecting critical infrastructure. Protecting freedom and security does not have to be a zero-sum game, and does not need an entirely new set of laws and frameworks. Civilian organizations should cooperate across borders and not just with the military—companies and Internet users have important roles.
- *NATO.* NATO's cyber security approach has matured greatly since the first Cyber Defense Program was adopted at the Prague Summit in 2002. The Bucharest Summit in 2008 emphasized "the need for NATO and nations to protect key information systems; to share best practices; and to provide a capability to assist Allied nations, upon request, to counter a cyberattack." Since

then, this capability area has been one of the fastest growing in the Alliance. The second NATO policy was published in 2011 after the Lisbon Summit and provided for the centralized protection of 52 sites for NATO networks. The third NATO policy stems from the Wales Summit in September 2014. It involves three broad enhancements: (1) Recalibrating the cyber paradigm in NATO—clarifying the link between cyber defense and collective defense; (2) applying international law to cyber space; and (3) deciding on a framework for assistance to allies in peacetime and time of crisis. There are three key questions going forward: (a) Should NATO consider a more forward-leaning (active) cyber defense? Most participants believed it will have to become more active eventually. (2) How far should the Alliance go in protecting individual allies, vice collective NATO assets? This will be hard to define. (3) Should there be a NATO CYBERCOMMAND? This is a very sensitive issue—some see it as opening the door to offensive cyber operations.

"Should NATO consider a more forward-leaning (active) cyber defense?"

National Cyber Positions

- *France.* The French *White Paper on Defence and National Security*, published in June 2008, identified cyber attacks as one of the main threats to the nation. France's 2013 White Paper made cyber defense a national priority and the opposition joined with the government to support it. It represents a normative approach with financial, human, and industrial aspects. Based on the 2008 white paper, France stood up the National Network and Information Security Agency (ANSSI in French) in 2009. Despite the austere fiscal environment, France is allocating significant additional resources to cyber security, both offense and defense. The security of French critical infrastructures is another high priority.
- *United States.* The U.S. *International Strategy for Cyberspace* was published in 2011. It emphasized norms for responsible, just and peaceable conduct, requiring a panoply of institutions, norms and means. The U.S. seeks the international security of cyberspace in many different domains including human rights, national security, international collaboration, and economic stakeholders. A more stable international cyber environment will reduce incentives for attacks. This will require a shared understanding of norms and acceptable behavior in cyberspace, taking into account trends in Information and Communications Technology (ICT) development. There have been hopeful signs from the Group of Governmental Experts (GGE) discussions at the UN. The December 2013 U.N. agreement that "International law, especially the U.N. Charter, is applicable in cyberspace" was a huge win, since some states had been advocating for the creation of a whole new international legal framework. Support for the use of present international legal frameworks also was endorsed by NATO at the Wales summit. The State Department's emphasis in cyberspace involves both Confidence-Building Measures (CBMs) and capacity building. DoD approaches align closely with State. Three major drivers that shape DoD's approach are: (1) Take a broad, team approach with effective partners; (2) balance between opportunity and risk, which is shifting because of growing threats and impacts; and (3) develop greater transparency in the use of uniformed military cyber forces and capabilities.

"A more stable international cyber environment will reduce incentives for attacks."

Private Sector Positions

Eleven representatives from nine companies provided a rich set of insights that stimulated extensive discussion. Topics included: The need to address mobile and cloud computing challenges; the criticality of public-private partnerships, including the Defense Industrial Base; the protection of critical infrastructure; the balance between law enforcement, national security and privacy; the need to educate leaders, legislators and citizens about

"There is a rapidly growing need to address mobile and cloud computing challenges."

technical issues in cyber security; the lack of incentives to emphasize security in the information technology industry; the importance of inspiring young people through STEM (Science, Technology, Engineering and Mathematics) and STEAM (adding Art) education; the importance of information sharing and standardization; the role of citizens; the cartography of cyber security; the need for continuous threat evaluation; and online radicalization as a cyber security issue.

Policy, Legislative and Regulatory Issues

- *Technology Export Controls.* Better ways are needed to assess technology and the global impact of dual-use capabilities, such as software, which can have worldwide impacts. Standards are needed for vulnerability reporting.
- *The Role of International Law in Cyber Space.* Several speakers noted progress in recent international discussions, such as the GGE, in gaining support for the application of existing international law to cyberspace, rather than developing an entirely new legal framework.
- *Cyber legislation* is out of date. New legislation should be technology-neutral. The Budapest convention on cyber crime may be a model. It is important to keep key principles—checks and balances, avoid excessive power of the state, and so on.
- *Education.* We need to educate legislators and executive decision-makers, as well as citizens, about rapidly evolving technology to improve the quality of decisions and outcomes.

Evolution of Cyber Policy Since 2008: NATO and Czech National Perspectives

Ambassador Jiří Šedivý
Permanent Representative of the Czech Republic to NATO

The Origin of NATO's Cyber Defence Policy

Cyber defence has been on the NATO agenda for more than a decade. Allies adopted the first *Cyber Defence Programme* at the Prague Summit in 2002. It was partially in response to a number of cyber attacks against NATO and some Allies during the operation Allied Force in 1999. The most important result of the Programme was the establishment of the NATO Computer Incident Response Capability (NCIRC).

"Only after the cyber campaign by Russian hackers against Estonia did the Alliance realize the risk in the cyber space."

The "ability to protect information systems of critical importance to the Alliance against cyber attacks" was mentioned in the 2006 *Comprehensive Political Guidance* among the most important capability requirements for the ensuing ten to fifteen years. Yet, it was not until the 2007 systematic cyber campaign by Russian hackers against Estonia that the Alliance truly realized the vast risk potential in the cyber space.

Catalysed by this event, Allies developed the first *NATO Cyber Defence Policy*. It was approved in January 2008 to inform decisions adopted by the Heads of State and Government at the Bucharest Summit in April 2008. In my roles as the Assistant Secretary General for Defence Policy and Planning, I was then chairing the Executive Working Group (today´s Defence Planning Committee) that drafted the text.

Seen from the current perspective, the policy was rather a bureaucratic text with not very sharp teeth. Above all, the policy defined basic terminology, i.e. how Allies understand cyber defence, what information systems are critical for NATO, etc. It also established the main courses of action for developing cyber defence capabilities in the key areas such as "prepare and train;" "prevent;" "detect;" "respond and mitigate;" "recover;" and "learn lessons." (This capability development cycle is today standardized in the NATO Defence Planning Process). The policy also defined the roles, responsibilities and mechanisms in the cyber domain in NATO—what we call cyber defence governance.

"Mentioning collective defence or a link between cyber defence and article 5 was taboo."

Yet debates about the text, namely how far should the Alliance go in assisting individual Allies in the event of an attack, were long and difficult. Any mentioning of collective defence or even hinting at a link between cyber defence and article 5 was taboo. The event that eventually helped us find consensus on the Policy was a trip to Tallinn, where the whole working group plus experts from capitals had a unique opportunity to discuss fresh experiences from the attacks with the Estonian authorities. The group visited the then embryonic cyber defence Centre of Excellence and, above all, held two formal working/drafting sessions. We came back to Brussels with a nearly final draft.

Relatively soon after this—in the 2010 *Strategic Concept*—cyber defence was fully recognised as a part of the NATO core task of collective defence (which is established through article 5 of the *Washington Treaty*). This rapid development was motivated by the growing threat perception in the cyber area, as well as by Russia's offensive use of cyber capabilities against Georgia during the August 2008 conflict.

What We Have Learned—And Three Questions for the Future

Since Ambassador Ducaru describes in his presentation the recent progress in NATO's cyber domain, let me conclude with one main lesson learned and three questions for further debate.

It goes without saying that cyber defence has been one of the fastest growing and transforming capability areas within NATO—which is natural since the cyber operational environment has been expanding exponentially. In this context, NATO has demonstrated the virtues of flexibility and adaptability at their best. The main lesson learned is thus a simple one: Be flexible and adaptable, not only now, but in the future where some "unknown unknowns" certainly await us. A good case in point is the fact that the possibility of invoking article 5 for collective defence in the event of a serious cyber attack—i.e. something that was taboo just few years ago—is a widely accepted planning assumption today.

"Invoking article 5 in the event of a cyber attack is a widely accepted planning assumption today."

The three questions are:

- How far should NATO go in protecting individual Allies—giving full respect to the primacy of national responsibilities in defending against cyber attacks?
- Should NATO consider a more forward leaning cyber defence posture, i.e. active defence?
- Should the Alliance incorporate a form of cyber command into the NATO Command Structure?

It will not be surprising if the answers from the perspective of some mid-sized countries with reasonably well developed—but not yet "top-notch"—national cyber defence capabilities would be *yes* to a more robust and forward-leaning role for the Aliance in cyber defence

NATO's Cyber Agenda after the Wales Summit: The Enhanced NATO Policy on Cyber Defence 2014

Ambassador Sorin Ducaru
NATO Assistant Secretary General for Emerging Security Challenges

The enhanced cyber defense policy that was endorsed by the Heads of State and Government at the Wales Summit of September 2014 is actually the third NATO policy of its kind—3.0 in our internal jargon. The first cyber defense policy, which Ambassador Jiří Šedivý mentioned, was created in 2008; the second one came in 2011 after the Lisbon Summit as part of the New Strategic Concept. The most tangible result of this policy was the centralization of NATO networks, which represent 52 sites to be exact. The 2014 cyber defense policy is about enhancement and covers the Headquarters in Brussels and all the NATO commands, agencies, and points of contact for nations. The new elements in the 2014 policy go along three lines.

The Recalibration of the Cyber Debate

"The link between cyber defense and Article 5 has been deliberately given some flexibility."

The 2014 policy recalibrates or enhances the conceptual debate about cyber within NATO in several ways:

The Link between Cyber Defense and Collective Defense. The new policy creates an explicit link between cyber defense and collective defense, something that would have been inconceivable in 2008 and was not easy to conceive even one year ago when I took over this job. Now, it is one of the most powerful items and it attracts a lot of attention at the political, media, and academic levels. It is important to note that the link between cyber defense and Article 5 has been deliberately given some flexibility, which concerns "when" NATO would invoke Article 5 and "how" NATO would respond in such a context. Why is this? Because Article 5 was intended by the founding fathers to be invoked on a case-by-case basis in specific political circumstances; so there are no predefined thresholds. It is only stated that the Allies will address Article 5 at the political level on a case-by-case basis. And the first time Article 5 was invoked after September 11 was again a scenario that was never envisaged by the founding fathers. So it is not really possible to establish thresholds but, of course, when a debate on Article 5 comes up, it will have to do with the size of the attack, its characteristics, and mostly the impact of such an attack. The policy recognizes that cyber attacks could reach a level where they could be as harmful for Allies as conventional attacks, and it was in this context that the link between cyber defense and collective defense was made.

"International law is applicable in cyber space…something that was much debated in the past within NATO."

International Law is Applicable in Cyber Space. A second point that refers to this re-calibration of the cyber debate is the recognition that international law is applicable in cyber space. This was again something that was much debated in the past within NATO, but there has been a strong desire by the Allies to send a political signal that cyber space should not be an ungoverned space.

Framework of Assistance to Allies. A third important aspect that is related to this conceptual debate and has practical aspects as well is the decision to have a framework of assistance to Allies in the field of cyber defense, both in peacetime and in times of crisis. In peacetime, this framework will help Allies deliver on their responsibility to invest in their defenses, but in a coordinated manner that should bring increased protection for the Alliance as a whole. In times of crisis, it will assist through the use of the crisis response mechanism of NATO, through the use of NATO's own capabilities including information sharing and analysis that could be put at the disposal of Allies.

Cyber Defense Mandate versus Cyber Defense under Article 5. One last point on this conceptual level is linked to the debate that goes beyond the purely defensive mandate of NATO in the field of cyber. As General Davis mentioned, the mandate is about cyber defense. It is about using defensive measures. Then, the link between cyber defense and Article 5 raises a legitimate question: If NATO only has a cyber defense mandate, how is it going to work in an Article 5 situation?

The response is as follows. NATO has few capabilities of its own and its command structure is really unique as an international organization. It has some capabilities like strategic airlift or AWACS, and in the field of cyber, it has the NATO Computer Incident Response center as well as information sharing capabilities. In any kind of crisis, however, NATO uses the capabilities of its Allies in the conventional field. So in the cyber field, if we are to come to a scenario of a big crisis, it will actually be Allied capabilities that will have to be employed. Thus, the future of the conceptual debate will be about the potential use of the organization as a coordinating policy body. We mentioned the idea of a cyber command—an idea that has been floated in some informal debates. Another idea was the potential capacity to use NATO as a planning body.

The Strong Reinforcement of Capability Development and Capacity Building

The second line of action in this new policy refers to the strong reinforcement of capability development and capacity building, both within NATO and among Allies. This is done through the NATO Defense Planning Process, which is a way of establishing these capability targets in the defense planning process, both for NATO as an organization and for Allies. It can then reach those targets through so-called Smart Defense, multinational projects, and also through coherent cyber training and education and exercises. The most recent example is the decision to develop a NATO cyber range based on Estonia's offer to put the Estonian defense ministry's cyber at the disposal of NATO and then develop it further.

Redefining the Way We Do Business

The last part of this new policy is about redefining the way we do business, both within NATO but also with others. Redefining the way we do business in NATO includes streamlining governance for cyber defense. The Cyber Defense Management Board, which brings together all the key bodies in this field, will be more flexible, agile, and response-oriented. We are establishing a lead policy-body and clearing house coordinator in NATO through the Cyber Defense Committee. This new way of doing business means mainstreaming cyber across all NATO's tasks, beginning with core tasks and then through all other ways of doing business including the operations planning and field exercises.

"Redefining the way we do business in NATO includes streamlining governance for cyber defense."

A New Way of Doing Business with Partners. This means a new way of doing business with partners. Since cyber defense is, by definition, a team sport, the policy provides for increased interaction with partner nations on a case-by-case basis depending also on their own capabilities and level of engagement in the field but also with international organizations such as the EU, OECD, U.N., and Council of Europe. Here I should say that NATO has a structured dialogue with the EU, has an ad-hoc dialogue with the OECD, and is now looking forward to starting a dialogue with the U.N. and the Council of Europe.

"We are launching a cyber partnership with industry—a framework for voluntary engagement."

NATO Cyber Partnerships with Industry. We are launching a cyber partnership with industry, which is intended to create a framework for voluntary engagement. It is aimed at exchanging information as well as establishing mechanisms for risk analyses and response, simulation, training and education, and exercises—in order to keep abreast of

technological trends and implement them on a fast track, both for NATO and Allied defenses. Also, for the first time, we have extended invitations to industry to participate in a NATO exercise: This is the "Cyber Coalition" exercise which will take place three weeks from now in Estonia in what is now the NATO Cyber Range.

Looking toward the Future

We are working on several new initiatives including the potential exchange of real-time information for cyber defense, establishing a cyber defense innovation hub, and, if possible, a trust fund and program of work for cyber defense innovation. Another important goal is to see how the multi-national, multi-inter-government projects in the cyber defense (NATO now has three of them) could be opened to industry representatives so that industry can participate in NATO cyber smart defense programs.

In any case, I think that this would attract much interest and bring new ideas. So, I would hope that, a year from now, we will be exploring a structured dialogue with industry—especially since we cannot separate the approach of a multi-governmental institution from that of the private sector.

Ambassador Sorin Ducaru, Dr. Roger Weissinger-Baylon, Ambassador Jiri Sedivy, and Ms. Heli Tiirmaa-Klaar (left to right) discuss the evolution of the Cyber Threat and How NATO and European Union Cyber Defense Policies are Responding.

Strategic Response to Challenges of Cyber Security: International Cooperation and Capacity Building

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

Objectives of the EU Cyber Security Strategy

My colleagues have explained what NATO is doing in cyber security. I would like to explain what the EU is doing. The EU has a larger responsibility in cyber security than in defense and, if you allow me, I would like to introduce some of the objectives of the EU cyber policy.

The EU has been quite active in fighting cyber crime in network and information security for a long time—for ten years or so—according to different policies coming from the European commission. But it was not until 2013 that the EU produced a coherent document on cyber, which was the first EU cyber security strategy. Adopted in the beginning of 2013, the document has five objectives:

- Increase the overall resilience of all EU member states in response to cyber threats,
- Reduce cyber crime in the European Union,
- Develop cyber defense capabilities within the EU Common Security and Defense Policy,
- Bolster the industrial resources for cyber security,
- Develop a coherent international cyber space.

In my own portfolio, I have two of these five major objectives. They are *cyber defense* and *international cyber policy.*

EU Efforts in Cyber Resilience and Cyber Crime

Before discussing our cyber defense and international cyber policy, however, I would like to give an overview of the EU's efforts in the more civilian fields of cyber resilience and cyber crime. As we know, cyber actors do not recognize the institutional borders of organizations, nor do they recognize the borders between domestic and foreign, or private and public, or military and civilian. This is why our response has to take into account these somewhat fuzzy borders. It is why the EU has made significant investments in dealing with cyber crime. Each European Union member state has an effective cyber crime unit (called the High-Tech Crime Unit) that is able to investigate cyber crime. All these units are coordinated by the new European Cyber Crime Centre (EC3), which was established last year and is attached to Europol in the Hague.

"Cyber actors do not recognize the institutional borders nor those between domestic and foreign, or private and public, or military and civilian."

The European Cyber Crime Centre is already a well-known entity and has conducted joint investigations with the FBI and some other law enforcement organizations.

The EU is also getting its act together with cyber security legislation. What do we mean by cyber security legislation? It is an "EU directive," a legislative act of the EU that tasks all the member states to incorporate certain principles into their national laws.

The Network and Security Directive is now being developed and discussed by the European Parliament and by the Council of Ministers of the European Commission in Brussels. It will task all the member states to set up functioning technical organizations to provide first level incident response and incident response coordination—or for cyber techies in this room I call it a "national CERT" (or a Computer Emergency Response Team—at the national level). Such teams already exist in most of the member states, of course, but a few members do not have it yet.

The directive also tasks each of the states to have a cyber strategy—a "whole of government" cyber strategy including civilian and other aspects. In addition, it imposes important principles such as oversight mechanisms for IT risk management in critical infrastructure sectors, including transportation, energy, banking, public administration, and health care. This legislation will apply to a rather large number of companies and, hopefully, it will strengthen the cyber security situation in the EU.

"You cannot have credible cyber defense without a broad base of cyber resilience at the national level."

For those who have been active in cyber for sometime, cyber resilience is the cornerstone of the national cyber defense. You cannot have credible cyber defense (especially in a military sense) without a broad base of cyber resilience at the national level. Therefore the civil-military synergies in cyber are vital, and we are looking at how to balance threats there.

Our Approach to International Cyber Policy

Moving away from civil threats to more national and defense challenges, here are our priorities:

First, the international cyber space policy of the EU is to increase the level of international trust, understanding and confidence between the countries. We have cyber dialogues with key partner states including India, Japan, South Korea and even China. And we are considering opening up discussions with other key partners. We have strategic engagements with other international organizations, including NATO, the OSCE, the U.N., the Council of Europe, the Organization of American States, the African Union, ASEAN, etc.

Of course, in our international cyber policy, we follow the principles of the EU cyber strategy. We support existing international laws in cyber space, but we do not support the introduction of new treaties or new conventions. This means that when we discuss with various organizations whether there is a need for a new cyber warfare treaty, for example, or a new cyber crime treaty at the U.N. level, the current EU policy is not to have any new treaties. We believe that, in order to tackle the question of how to conduct warfare in cyber space, we need to apply the existing principles of national homogenic law, the laws of armed conflict, and the principles in those laws, such as the principle of proportionality among others.

The EU's Approach to Cyber Crime

As to cyber crime, we have the Budapest Convention or Council of Europe Convention on Cyber Crime, which we are promoting globally as a blueprint for national legislations. And we do not support a new U.N. convention for that reason i.e. we already have one global convention.

The OSCE has adopted the first set of cyber security confidence-building measures, and we support their efforts. This is a first set of transparency measures that asks member states to establish contacts, build dialogues, and exchange cyber strategies. This kind of confidence building is necessary in cyber space. The EU is also advocating this approach outside the European and trans-Atlantic security area, in particular, in the ASEAN regional forum, which is the security organization for Asian countries. I would also like to mention the

"The OSCE has adopted transparency measures that ask member states to establish contacts, build dialogues, and exchange cyber strategies."

necessary capacity building that we need to tackle collectively. While most of us are from technologically advanced countries, we know the cyber threats are not confined within states like ours. They move very fast to territories where there are no laws, no police, and where there is no public administration that is able to deal with cyber threats.

The EU has made substantial investments in order to promote the minimum level of cyber crime legislation in several developing countries and the emerging markets, and we are increasing our funding for these activities. At the same time, we are actively looking for good models of ways to build cyber capacity outside of the technologically-advanced states.

Our International Cyber Defense Framework

Finally, I would like to say a few words about cyber defense, which is now being discussed in Brussels. We call it the Cyber Defense Framework. Our EU cyber defense posture does not overlap with what our NATO colleagues are doing. Instead, we try to complement each other—and we are talking to NATO in order to make sure that the capability development efforts of NATO and the EU are complementary.

Industry Response to Cyber Threats in a Mobile and Cloud-based World

Mr. James R. Wylly
General Manager, Worldwide Public Safety and National Security
Microsoft Corporation

Industry's Approach to Defense against Cyber Threats

I will talk about industry's approach to defending against cyber threats. Microsoft is an interesting company in the sense that we are not a cyber security company, but we have a tremendous cyber interest in what we do. Quite a while ago, we realized that being merely reactive to cyber attacks was not good for our business or for the protection of our more than one billion customers that we have around the world. So we understood that we needed to create, if not by name, an Intelligence capability to study and examine the threats. We decided to go back and review the way we do business, the way we write code, in order to truly own up to our responsibilities to all of our customers. Since many of them are defense customers who use our products both in command and control and in tactical systems, we must ensure that those systems are safe and fully protected.

"Merely being reactive to cyber attacks was not good for the protection of one billion customers."

The Security Development Life Cycle

In about 2004, we created a new way of doing business that we call Trustworthy Computing. We created a security development life cycle (SDL) for products. This means that, instead of securing products after we have written them, security and privacy now go into every line of code, beginning with the first line that gets written on every product that we develop. It is a company-wide initiative—one that we use in order to ensure that the products that we are making are as dependable and secure as they can be for all the customers who will use them. That security development life cycle process is based on three concepts—education, continuous process improvement, and accountability—so that we can stand behind the products that we build. It is a comprehensive process for writing a more secure code. Today, the SDL is considered an industry standard for writing more secure software. Many of its key elements have been adopted by government commercial entities and it is recognized by industry guidance standard ISO 27034 as a "best practice."

"Instead of securing products after we have written them, security and privacy now go into every line of code."

The Trustworthy Cloud

The world is moving now toward mobile use and Cloud use, and, because of the economics, many of our partners are developing Cloud capabilities. As one of the global leaders in this area, we have been challenged to create a trustworthy Cloud so that people who are using our Cloud are able to trust the systems that they are using. For this reason, we developed what we call the Trustworthy Cloud Initiative (TCI). Again, it is a shared practice among large Cloud providers across the world—where we have over a billion customers using over 200 Cloud services that we offer. Over 20 million companies benefit from the Trustworthy Cloud, including many defense departments around the world to which we owe security and protection.

The goal of the Trustworthy Cloud Initiative is to make us a trusted Cloud provider so that customers and constituents, who move to the Cloud to benefit from economies of scale, can have trust that their

data is not only secure, but also that it is private from us at Microsoft and private from the governments where we operate. This has been a key turning point in the Cloud, which began after June 2013 when disclosure of information as to how data was managed really started a global debate on how we maintain privacy and how we maintain trust, as more and more companies are holding data for organizations.

"Customers and constituents who move to the Cloud can trust that their data is not only secure, but also that it is private from us and from governments."

So that led us to add privacy to the Cloud. Even though we do not have direct evidence that any of our customer data has ever been breached externally, we do want to increase the confidence factor. Therefore, we doubled our encryption efforts, as did many of our colleagues in the industry—Salesforce.com, Facebook, Google, Amazon. All of them did the same thing. In order to further ensure privacy, we have taken the legal position that no one can access any of our customer data and that includes defense data. This means that we keep our data encrypted and safe from being broken into—but it is also secure and private so that we will not look at it and governments will not look at it either.

The Cyber Crime Center

I would also like to mention the Cyber Crime Center. At this workshop, law enforcement and international law agencies have been frequently mentioned. We partner with the Defense Cyber Crime Center (DC3), we partner with Interpol—as well as its new Global Complex for Innovation (IGCI) in Singapore that is about to open. These are relationships where we are able to utilize the great set of information that we obtain from multiple sensors that we have around the world—these are actually billions of sensors that report back, in one way or another, to Microsoft. These relationships and sensors give us a unique opportunity to see what is happening in the world. And now, as the world moves beyond computers to the Internet of Things, we are going to see an explosion of devices connected to the Internet. This means that chances for attacks are going to grow much greater.

"Through the Cyber Crime Center and Digital Crimes Unit, we fight against malware, botnets, intellectual property theft, and child exploitation."

Through the Cyber Crime Center and the Digital Crimes Unit, we fight against malware, botnets, and intellectual property theft, and even technology facilitating child exploitation. Every six months, we publish a security Intelligence report that is freely available globally for anyone to read. This report covers what we see across the world and opens up an opportunity for us to share that information globally.

One Last Point: The Government Security Program

The last thing I want to discuss should be of interest to everyone in this room: It is a program that we call the Government Security Program. The Government Security Program is a trust element that permits governments who partner with Microsoft to examine all of our source code—in other words, all of the code that we write. This means that for Windows, Office, Exchange—all of the things that you use—we now let governments come in and examine the code. They can do so with their own analysis tools in order to confirm for themselves that there are no secrets in the code of the products that we are using. This is our way of providing total transparency, so that governments can look at everything that we do. The Government Security Program also provides the opportunity for us to share threat information. We can examine a threat that is occurring in your nation; we can compare that against a global threat that we have already observed, and we can then help you identify it. In order to enhance this Government Security Program, we have

"The Government Security Program permits governments to examine all of the code that we write."

opened transparency centers around the world in order to make it even easier for governments to come in and physically look at this source code.

In this brief overview, I have tried to touch on some of the key ways that we use cyber security—and what we do to protect over one billion customers who use our products, including the many defense departments that we help enable and keep secure.

Mr. James R. Wylly, General Manager, Worldwide Public Safety and National Security, Microsoft

The Changing Threat Landscape

Mr. Gavin Millard
Technical Director, EMEA, Tenable Network Security

Since the start of my career 15 years ago, the world of cybersecurity has changed dramatically. We have seen the industrialisation of cyber threats involving nation states and many highly motivated criminal organisations. These threat actors utilise hacking techniques, once the preserve of the few, to gain an advantage against the many.

Cybercriminals

"Breaches of large organisations happen weekly—TJ Maxx, Home Depot, Target, Zappos, Neiman Marcus and JP Morgan."

In recent years we have seen criminal organisations take advantage of systems to monetise the masses. The exfiltration of credit cards from organisations to commit fraud is now an everyday reality. If we look at the U.S., major breaches of large organisations seem to happen weekly, including TJ Maxx, Home Depot, Target, Zappos, Neiman Marcus and JP Morgan. Such breaches cost hundreds of millions of dollars for the organisations to recover from, but net huge amounts of money for the cybercriminals that sell the data. We have also seen cybercriminals monetise viruses and malware by encrypting the files of hapless users and demanding payment to get the files restored through ransomware. This is simple but hugely profitable.

Nation States

The Right Honourable Philip Hammond said in June of this year when he was the U.K. Minister of Defence, that "Future wars could be fought entirely on the internet and that Internet-based attacks could replace boots on the ground in the same way tanks replaced horses in the 20th century." Where once we would send tanks and troops, we can now attack another nation without a single bullet being fired or a rocket launched. For example, in 2010 a virus called Stuxnet targeted uranium enrichment plants in Iran, attacking the centrifuges by forcing them to spin out of control and setting back their nuclear program for years.

Nation States are gearing up for cyberwar but the flaws used by these Nation States can also be copied by anyone with the right motivation and skill. The infrastructure we all rely on is outdated, antiquated and exploitable by anyone with a modicum of skill and motivation.

Mr. Gavin Millard (right), Technical Director, EMEA, Tenable Network Security, with Dr. Ita Lochard, Middlebury Institute of International Studies.

We are also seeing moves from Governments around the world to monitor their citizens' online activities. For example, it was recently revealed that the Chinese government was able to snoop on encrypted iCloud data and get access to iMessages and any other documents stored on the service. It all comes down to a simple truth: If you own the connection, you control the conversation. This is something that appeals to many dictatorships and, as we saw with the revelations coming out of the Snowden leaks, it appeals to some democracies as well.

Regardless of who the threat actors are, the risks of cyberattacks affecting everyday life are real. It is not my intention to be a scaremonger nor do I want to make predictions on how easily highly motivated attackers would cripple a nation, but it could happen and it possibly will happen in the future. Good defence, investment and education are required to reduce the risk of impact from these threats. More can be done to protect from other Nation States and skilled cybercriminals the assets that both governments and their populations rely upon everyday.

Within the U.K., the Centre for the Protection of National Infrastructure, (CPNI), has been set up to protect against motivated and skilled attacks. Embedded within the guidelines are controls that should be implemented to ensure that the security of the institutions are maintained.

"Most organizations fail to cover the basic security controls suggested by the SANS Institute."

The CPNI Directive turns to the Top Twenty Security Controls from the SANS Institute as best practice, something many of us in the industry have been suggesting organisations should follow for some time. While dry and impossible to cover in the time I have today, this list of controls is full of advice that everyone should follow. Let's take a quick look at the top five:

- Discover all the systems within the network
- Discover all the software running on those systems
- Identify weaknesses in the configuration of those systems
- Identify vulnerabilities

Unfortunately most organisations I speak to fail to cover these basics. Many seem more eager to spend a significant amount of money on buying expensive technologies that carry the promise of a security silver bullet but in reality do little to reduce the attack surface.

It is said that the biggest issue we face today in securing infrastructures is the "Advanced Persistent Threat" (APT) but the uncomfortable truth is that it is less APT than apathy. The best security practices we need to implement are widely known, but the effort and investment to adopt them is rarely easy to come by.

"The truth is that the Advanced Persistent Threat is less dangerous than the risks from apathy."

New vulnerabilities are being discovered every day. Some examples of these vulnerabilities are HeartBleed, the OpenSSL bug which enabled attackers to gain access to communications assumed to be secure, and ShellShock, a 25 year old bug in one of the most widely deployed tools on Unix which enabled hackers to run any command on the affected servers from the comfort of their own basement.

Tenable has created an innovative technology to cover the top 5 controls among others with one single solution as well as giving visibility into the indicators of compromise for a continuous view of where the risks reside and if they are being taken advantage of.

When these huge holes in the software we trust are discovered that could be utilised by attackers, millions of people turn to us, including the U.S. Department of Defence and NATO CIRC, to help identify where they are affected and how to fix it.

The Known Unknowns of the Cyber Threat

LTC (USA, Ret) Timothy D. Bloechl
Director, Cyber Security, Quantum Research International

Mr. Gavin Millard, Tenable Network Security; Dr. Roger Weissinger-Baylon, Workshop Chairman; Mr. Jamie Wylly, Microsoft; and Mr. Tim Bloechl, Quantum Research International (left to right).

Recent major intrusions into corporate systems show the breadth and increasing sophistication of today's cyber security challenges. Countering the threat remains a tremendous test for those charged with defending Information Technology (IT) infrastructure and reducing risk. Reducing this risk and the "Fog of War" surrounding the evolving cyberspace struggle requires a combined effort involving technical, legal, educational, and research & development means.

Leaders of all kinds—government, business, and non-profit—and those of us engaged in cyber security face a number of known unknowns on a daily basis including:

- What will be the next major virus or worm to infect our networks?
- What will be the next zero day vulnerability hackers exploit?
- Which corporation or agency will experience the next major breach?

A free market IT Industry focuses on building the next cool game, gadget or other IT innovation which will drive revenue and share growth to stay ahead of the competition. This focus is often at odds with both building security into products during the software development process and providing the software updates necessary to reduce the cyber risk to their customers. When one considers that many of the software products we use on a daily basis have lines of code ranging from the thousands into the millions, ensuring security is next to impossible, and developers and users automatically accept a level of risk. This risk creates the unlevel playing field that hackers exploit, resulting in today's unsettling cyber threat environment in which we operate.

The focus on innovation is often at odds with building security into products.

To counter this threat we have seen a huge increase in the IT security services and products market. According to Gartner, a major IT industry analysis firm, this market is worth $71 billion today[8] and is expected to grow continuously for the foreseeable future. While these products and services do some good to help us defend our computer networks, the security capabilities offered concentrate mainly on known vulnerabilities. As the number of known computer-related vulnerabilities increase at an alarming rate, it certainly must be difficult for these security vendors to keep up with the threat. To make matters worse, it is the unknown vulnerabilities that are causing major concerns to Chief Information Officers (CIOs) around the world. In addition, the number of personnel trying to exploit these vulnerabilities is also increasing. Some are doing it for fun or as ethical hackers to uncover risk areas, but many are doing it with malicious intent.

To address the security challenge we face, in the short time I have here today, I suggest we consider where we stand while attending this workshop across four areas of discussion: Technology, Education/Work Force, Legal/Policy, and Research and Development (R&D).

Technology

Dependence on Internet-based applications and utilities permeate every walk of life and industry. Consumer craving for increased technology solutions, coupled with IT industry innovation, is driving customers to what is known as the Cloud" along with trends to improve and increase the use of mobile devices and information stored in large data centers. We are also on the verge of achieving a vision of what is termed the "Internet of things" which is "a scenario in which objects, animals or people are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction."[9] In other words, a world where virtually anything we do and how we live is somehow connected to the Internet. This technology innovation and market demand is astounding and almost every day we hear about some new and exciting solution to everyday challenges. The unfortunate reality is this innovation leads to increasing risk from cyber attack.

"Common Criteria and other "standards" are obsolete since they cannot keep up with the threat."

The threat continues to grow and new attack vectors emerge almost daily. In the past our focus was on defense-in-depth and software certification. However, in my view, Common Criteria and other "standards" are obsolete as they cannot keep up with the threat, nor do these standards keep up with IT innovation. Cyber defenders use hardware and software security solutions, which are only as good as the currently available threat information. The speed of technology advances and the slowness of certification and accreditation processes are at odds with maintaining any semblance of security to keep up with the threat. The problem is getting worse. We have now turned to risk management as the way to deal with the crisis. This is an acknowledgement the previous methods are not working. Networks are largely indefensible and a determined threat can always find a way to get in. Just ask the representatives of Tiversa here in the audience today—they see major data leakage coming from government and corporate networks at an unprecedented level in a space largely ignored by security teams—the peer-to-peer networking space.

Education/Work Force

All organizations face a supply and demand challenge when growing a competent cyber defense work force. Choices to focus on either IT development or security career paths cause tension in early career decisions. Software development positions to build the next new and "coolest" product tend to be more interesting to "techies," leaving security firms struggling to capture new talent. While

[8] The Wall Street Journal, *Global Security Spending to Grow 7.9% in 2014, Gartner Says*, August 22, 2014
[9] http://whatis.techtarget.com/definition/Internet-of-Things

educational institutions are catching up and more universities offer cyber security-related courses and degrees, we are years behind the demand for graduates. Even then, those who follow this path must have continuous learning to keep pace with the threat and technology responses. The public sector will lose candidates over time to commercial job opportunities as people respond to making money. This situation is further exacerbated by the trend in government contracting circles under severe budget constraints to accept lowest price, technically acceptable bids vice best value. The push to save money in the short term results in contractors providing people who meet the minimum requirements rather than ones who provide the best value for an organization with adaptability and advance technology skills to meet the ever-changing threats. Chief Information Security Officers (CISOs) face challenges resourcing their cyber defense teams and are forced to outsource. This reality also increases risk as CISOs do not "own" the defenders on which they have to depend. In the U.S. Government, as an example, there is action to add thousands of cyber defenders to the public sector work force. The question is: Where are they going to find these people at reduced salary levels?

"We are years behind the demand for cyber security graduates."

Legal/Policy

Current tensions between the desire for privacy versus the needs of law enforcement and Intelligence are driving debate in many countries. The IT Industry is pushing back on government as crypto constraints inhibit their approach to meet customer privacy concerns. Most publicly used crypto has already been broken. While there have been gains in the takedown of botnets and jail time for some hackers by combined industry and law enforcement efforts, these attempts only impact the tip of the iceberg. Increases in legal requirements to report incidents and breaches help us to better understand the enormity of the problem, if reported, but I contend many breaches go unreported as the economic costs and threat to brand and commercial viability forces a human reaction—hide the truth. Those who do report such incidents highlight another alarming fact: Most breaches take weeks or months to identify and the average breach to discovery time from one source is 87 days![10] Standards such as HIPAA, FISMA and European versions of the same are making gains but trail an unconstrained, free market cyber-attack threat force. Furthermore, sovereignty issues reduce sharing of high-quality and timely threat Intelligence, and reduce the possibility of attaining any useful international legal regime to fight back. So, while some hackers are going to jail, most operate from international safe havens and some are even encouraged (or largely ignored) by their host nations allowing these hackers to do more harm. Finally, the growing talk by commercial industry cyber defenders to conduct a more active defense raises the hair on the necks of those who have been doing government sanctioned attack and Intelligence gathering. Collateral damage is a constant concern and if the commercial industry goes on the offensive, who knows what damage may be caused?

"Most publicly used crypto has already been broken."

Research and Development

Attaining situational awareness on large networks, some facing millions of potential attacks a day, is a very challenging problem. Coupled with the dynamic network environment most companies and organizations face, including bring your own device (BYOD), use of the cloud, reliance on less than secure mobile applications, and a lack of security knowledge by the general work force, fuels the demand for new and innovative ways to counter the threat. Fortunately the cyber security industry is growing and getting more and more innovative, but the task the industry faces remains daunting. We desperately need means to

"We desperately need means for auto-sensing, auto-configuration and auto-control of networks."

[10] Trustwave, 2014 Trustwave Global Security Report, May 20, 2014.

attain the goal of auto-sensing, auto-configuration and auto-control of networks. Unfortunately, in my opinion, there is no single or combination of technology solutions that accomplishes this goal today.

Conclusion

I realize I paint a less than optimistic view of where we stand in the fight against cybercrime, attacks, and network exploitation, but we need to be brutally honest when judging the current situation. The known unknowns are causing tremendous challenges for cyber defenders. Until someone develops a magic solution to mitigate the risk and turn the tide against the growing cyber threat, and who knows when or if this will happen, CISOs really have only three main courses of action to keep up with this dynamic environment:

- Encrypt information at risk with the best available encryption technology, and push for government relaxation on the constraints placed on usable key lengths and strengths.
- Conduct continuous penetration testing and vulnerability assessments to constantly adjust defenses to plug holes in an ever expanding leaky dike.
- Hire cyber security personnel who truly offer the organization a best value solution with a combination of education, training, experience, and adaptability to meet the current and evolving threats.

Addressing Complexity: Trends in Cyber Cooperation

Dr. Itamara Lochard
Director, MIIS Cyber Initiative, Middlebury Institute of International Studies at Monterey

Dr. Ita Lochard, Middlebury Institute of International Studies; Mr. Gavin Millard, Technical Director, EMEA, Tenable Network Security; Dr. Roger Weissinger-Baylon; Mr. James R. Wylly, General Manager, Worldwide Public Safety and National Security, Microsoft Corporation; Mr. Tim Bloechl, Director, Cyber Security, Quantum Research International (left to right).

I would like to address several issues in order to cover the "greatest hits" concerning complexity and cooperation in cyber security.

Irregular war and hybrid attacks are not new. They have existed since the Peloponnesian war and are apparent in most great ancient texts to include those of Sun Tzu and Mao Tse Tung. What we call "cyber" threats today are also not new. The first cyber incident against NATO—a DDOS attack—occurred fifteen years ago, during the Kosovo crisis in 1999. Thus, cyber attacks did not begin with the Estonian events of 2007 as many often refer. The LTTE in Sri Lanka had a wing called the Black Tigers in 1996 that was what we would consider today their "cyber" arm. We did not call it cyber then, but it was there. It is thus critical to demystify components of cyber incidents by relating them to traditional rules and conduct of war. By doing so, we can be parse out useable categories that are more easily addressed using conventional understandings of crime, conflict and warfare.

"The first cyber attack against NATO occurred fifteen years ago during the Kosovo crisis."

A year after the major cyber events in Estonia, now-unclassified information tells us that thumb-drives were used by militias against ISAF. This led to a ban against the use of these devices throughout the U.S. Department of Defense. That same year, we witnessed the Mumbai terrorist attacks along with events in Georgia, which were considered the first real cyber-hybrid incidents. One was by a state actor, the other by a non-state actor. Both used technology to collect information,

plan, jam communications, train, communicate, as well as amplify kinetic attacks. In the Indian case, terrorists had an ops center in another country that allowed 10 men to hold 20 million people hostage over a period of a day. By monitoring social media, they determined the location of people to increase casualties and conducted targeted executions. In essence, they were controlling critical infrastructure—which we did not realize at the time. However, it is not an easy thing to assess. Critical infrastructure is not defined as the same thing every country or region, not all countries own their critical infrastructure, and very rarely is command over critical infrastructure by a non-state actors factored into analyses during fast-paced incidents.

So what is new? The operational environment has vastly changed: We are now in a net speed world with a 24/7 news cycle. Likewise there is new literacy where younger generations have a better grasp of the technology but lack the ability to make strategic assessments of seasoned leaders. We see new "weapons" in the form of thumb-drives, worms, Trojans, and bots as well as amplified traditional ways of conducting info ops and spin, activism / protest in the form of hactivism and defacements, as well as technologically-enhanced kinetic attacks. Moreover, the number of devices entering the workplace is increasing faster than the ability to create protection and patches for them and the development of new gadgets often has little to no consideration to potential security or privacy issues they present.

Plus, the number of countries has quadrupled since the end of the Second World War and most have still not fully consolidated. The past 15 years has introduced a plethora of new actors utilizing cyber means—some mixed in motivation where purpose is not always evident. They are much more flexible and adapt and re-organize much faster than any government, military, or alliance. What is also novel is that non-state actors—violent, non-violent, and with various motivations—can now project power in a way what was previously relegated only to states. Take for instance what James Wylly explained so well in his presentation: Microsoft owns most of the sensors in the world. Understanding this is key, since governments still believe they own this domain and simply do not—companies do.

"Microsoft owns most of the sensors in the world."

Governments are culprits in perpetrating this fallacy of control. You often hear many officials worldwide talking about how we own this or that and make it sound as if we can actually do something about preventing cyber incidents if only there were more regulation or enforcement of some sort or other. In reality, no single government or group of governments can do much alone without industry, simply because industry controls key cyber assets. However, this also means that industry also needs to defend those assets. It is not the state or an international body that provides security here. Complicating these issues, is that that ownership varies from region to region, and changes across sub-regions. This has tremendous implications for the formulation of effective laws, agreements, and cooperative arrangements.

For instance, once we had a discussion among like-minded countries about removing the basic blueprints of Liquified Natural Gas (LNG) terminals and other types of sensitive information related to critical infrastructures from the Internet which could be used to plan an attack. Of course, once this information is on the web, you cannot completely remove it. Still, we thought we might be able to reach agreement to not put anything new on the net. It was an effort at "norm" creation on a cyber issue that was thought to be not contentious. However, we simply could not get an agreement.

Certain European states were vehemently opposed, because the proposal went against their notions of freedom of information, even if it meant jeopardizing security. This is an example of the many cultural complexities that must be factored when looking at developing laws to try to address these problems even within one region. This is true not just in Europe but elsewhere. It is therefore essential to realize there the are significant differences in perceptions not only on sticky issues such

as privacy versus security, but also on aspects of whether or not access to information is an actual "right" of the population in each state involved in cooperative measures.

"There is no incentive for a tech person to think about policy, unless you make it part of his paycheck."

We also need cyber literacy—and not just in terms of people who are techy versus those who are not. We have had discussions with many Silicon Valley companies who argue policy people in Washington, D.C. need to better understand their perspective. We have asked them whether it is possible make tech people more fluent in policy considerations and thinking. Ironically, they report that there is absolutely no incentive for an average tech person to think about policy, unless you make it part of his (or her) paycheck. So, how can you address this issue? At least in the United States, we are beginning to put the onus on the company whenever there is a breach. But that is not enough.

For example, the recent Target, Home Depot, and TJMax incidents in the United States were among the largest breaches experienced so far in terms of costs to the consumer. Yet, none of these cases were very sophisticated cyber attacks, nor were they the work of super hackers, or particularly savvy covert groups, or even states. In fact, many of the attacks were attributed to a relatively small, Ukrainian-based group. And the TJMaxx case was made possible simply because the company did not close its network, which permitted a few people sitting in cars outside the stores to capture every credit card swipe and pin entry. In other incidents, people in the tech supply chain saw incidents as they were occurring and did not report them up not considering the policy implications and liabilities. So, while you do need more people to address technical concerns, there is also a great need for *cyber policy* education, too.

Another key issue is we need to better grasp the financial power and flexibility of transnational corporations. I would like to cite some statistics from some of my earlier research where I compared the GDP of countries to annual income of transnational corporations: In 2006, so already eight years ago, there were about 80,000 major transnational corporations. *Each* of the top 50 companies individually had more annual revenue than three-fourths of all the countries on earth combined. Think about that.

These companies are always dealing with cyber incidents in the form of espionage and crime. Not factoring in the significant economic power of these actors and the issues they face makes it difficult to understand the nature of the threat or develop effective ways to counter it. In addition, finding solutions that work for industry and for different regions is critical. It is equally important to recognize that large Fortune 100s also have had tremendous flexibility that states should try to leverage. For instance, some of these companies have been able to cooperate with China on dealing with cyber crime, an area where the U.S. government has not had as much success. Such information needs to be shared and lessons from their examples developed further.

Cooperation in Cyber Crime, Espionage, and Events in Theater

Consensus within each state is needed on determining thresholds of what constitutes a cyber event as an act of war, attack, disruption, or civil disobedience/protest before we can reach international or even regional agreement. These terms are frequently used interchangeably in news reports and articles which only further muddies the waters. Cooperative agreements have been deliberated in three categories: Cyber crime, espionage, and conflict or events in theater (whether you call it warfare, terrorism, insurgency, etc.). Cyber espionage has driven much of the debate in the post-Snowden world, but regardless of where you fall on this issue, the reality is that state-state espionage is not illegal under international law. This means that unless we can reach an agreement that traditional, state-state espionage is illegal under international law, we are not likely to get rid of, or contain,

"Espionage has led much of the debate about privacy versus security—but it is not illegal."

state-state cyber espionage. It is simply off the table. If you put the notion of state-state espionage aside, then we are dealing mainly with cyber crime (to include industrial espionage) and the use of cyber in conflict—two areas I believe are somewhat manageable.

There are criminal laws that can be applied to a multitude of cyber incidents to reflect trespass, theft, obscenity, etc. Bringing in law enforcement agencies and other entities to address these areas has been very productive and there is a burgeoning literature on legal responses to cyber crime. In terms of addressing what happens in theatre, there are now declassified examples where we see that non-state actors that we did not consider to be cyber actors actually had those capabilities and used them for both intelligence as well as to conduct cyber attacks. Here the rules and laws of war and conflict apply. Their use of cyber is merely another type of weapon, intelligence gathering device, form of command and control, training, propaganda, or communication tool.

Moving Forward: What Needs to Be Done?

So moving forward, what do you do? At this workshop, there have been many references to the Cold War. According to lessons from a 2009 paper, "New Approaches to Cyber-Deterrence: Initial Thoughts on a New Framework," by Jeffrey Cooper, he argues it is useful to look at the Cold War in terms of its lessons of containment that were part of the foundations of deterrence. Cooper argues the principles of containment were used in that era against second-order threats that were deemed not to lead to mutually assured destruction. His premise is that in the digital era, cyber is a second-order threat where these principles can be applied. He also asserts that the bi-polar world of the past has changed to a uni-polar world requiring a different response than friend or foe. He calls today's reality the 3 C's (cooperation, competition, and conflict) where one can be simultaneously cooperating, competing, and in conflict with another actor at the same time.

For instance, this is the case of U.S. and China. To address this, you need a certain type of flexible response. It cannot simply be all or nothing. And without that, you cannot move forward in this era. Likewise, he argues we must look to increase interdependence since actors are less likely to attack another on whom they rely. He also advocates measures of counter-productivity to reduce the impact of an incident when it does occur.

Often people conclude that due to the difficulties of attribution in cyber incidents, it impossible to counter. However, if you have an invisible fence, it prevents attackers from crossing the fence. You do not need to know what is traversing it to be effective. This principle of futility, or hardening your systems, is key in Cooper's analysis. He concludes by advocating a networked approach to better understand and respond to cyber incidents.

But, how can you harden systems properly if you do not know what the threats are—especially if the people who understand the issues are in the corporate sector and are not part of the dialogue? Often when we speak of intelligence sharing in the post-Snowden era many think it is a push to support surveillance or increase the use of meta-data analysis. There is no doubt there are some who advocate that view. However, a successful, networked approach means relying upon cooperation, which by default will encompass various views on digital ethics, freedom of information, free speech, and notions of privacy versus security. Therefore, it is a fallacy that advocating intelligence sharing automatically equates to promoting a reduction in privacy or rights. It is simply not possible even among allies and partners given the cultural and nationalist views on cyber topics mentioned earlier.

In addition, there are new kinds of cooperation and interaction facilitated by technology: you have gamers who created something called MMOWGLI (massive multiplayer online war game leveraging the Internet). Thus is essentially a game that can be played over multiple days, whenever there is time, even from a smart phone. It is a new form of table-top exercise at low-cost developed by the

U.S. Naval Postgraduate School. Examples are available on their website and on YouTube. It is an excellent way to conduct defense training enhanced by technology.

Also, social network analysis can be important, too. There are companies and non-profits that use this to improve their communications, internal organization, and efficiency. Likewise, it can be used in theatre to better understand your cadre, multinational efforts, as well as conflict dynamics. Companies have also created more effective and accurate surveillance technologies to be used in dense areas of large crowds—for instance, at airports or railways—to provide better information on body temperature to reduce the spread of disease as well as to find the perpetrator after an attack. Uses in theatre during an active conflict are clearly beneficial as well.

"A cyber civilian defense unit is based on the example of the Estonian Defense League."

A final example is the development and use of civilian cyber defense units such as one in the United States based on the *Küber Kaitselliit*—the Estonian Cyber Defense League. The goal of such efforts is to harness the guys and gals with the Mohawk versus the crew cut along with those with experience in industry who want to serve but not necessarily be in the military. However, by having diverse people, including the military working together, they learn from each other.

There are many, many other examples of cooperation that have been successful. In order to address all the challenges that cyber security presents in this era, interdisciplinary, international efforts across multiple sectors of society is critical. In addition, there is an urgent need to increase digital fluency—understanding the interplay of how technology impacts policy and international affairs.

Cyber Security—Keynote

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

Mr. David Grout, Director of Pre-Sales Southern Europe, McAfee, Part of Intel Security; Mr. Chris Painter, Coordinator for Cyber Issues, U.S. Department of State; Ms. Michele Markoff, Deputy Coordinator for Cyber Issues (Left to right).

Introduction

In my career, I spent about 22 years in cyber, starting as a Federal Prosecutor prosecuting cyber crime in the 90s. Our Department of Justice team, which I led, covered cyber intrusions and intellectual property cases. When President Obama was elected, I moved over to the White House and helped create both our national and international strategy. We worked closely with the French government—Patrick Pailloux, Francis Delon, and others—as they were developing their strategy and France has now done a lot of work in this area. For the past 3 years, I have been in the State Department to create a cyber diplomacy unit, the first in any foreign ministry; many others have now followed.

At this conference, we have heard about how empowering the Internet and cyber technologies are but we have also heard about the different threats we face in cyberspace. President Obama, whose campaign was hacked into when he was first elected, pointed out that:

> "It is the great irony of our Information Age that the very technologies that empower us to create and to build also empower those who would disrupt and destroy."

Over the years, government-sponsored intellectual property theft, threats to critical infrastructure, and dangers of cybercrime, have risen to the top of the policy agenda. At the same time, the worldwide growth of the Internet has intensified the debate on how cyberspace should be governed and we are witnessing a greater effort by repressive regimes to undermine human rights online because they see the open Internet as a threat to their stability.

The challenges are both technical and policy related. While senior decision makers used to consider cyber—cyber security, cyber thefts, even Internet issues—as the domain of technical people, cyber has become a major issue of national security policy, of economic policy, of human rights policy, and ultimately of foreign policy. This is true around the world and it is good because it raises awareness; but it also creates confusion and difficulties in understanding how these issues are related.

Like many other countries, we have developed a national strategy to fight cyber threats. Indeed, it is crucial for governments to coordinate their various approaches to cyber by joining government agencies together and also talking to the private sector and other stakeholders. It is equally important to articulate what the goals in cyberspace are. In 2011, the U.S. released an international strategy for cyberspace, the first of its kind in the world. It states the vision of a cyber space where norms of responsible, just, and peaceful conduct among states and people have begun to take hold, and commits to an international cyberspace policy that empowers innovation, drives the economy, and improves lives. Most importantly, this strategy reflects our conviction that, if all nations are to reap the tremendous political, economic and social benefits that cyberspace offers, cyberspace must be open, interoperable, secure, and reliable. We can have policies that integrate all these different issues.

"Governments must coordinate their approaches to cyber by bringing agencies together, and talking to the private sector."

"Cyberspace must be open, interoperable, secure, and reliable."

Building resilience and reducing risks in cyberspace is not just a technical endeavor. It requires that we stitch together institutions, norms, and cooperative mechanisms and make a concerted diplomatic effort on the international stage. That is why my office was created in the State Department a little over three years ago. I mentioned earlier that we created the first diplomacy unit. There are now about 20 around the world and more are coming.

Toward International Cyber Stability

Given that some cyber threats have the potential to constitute threats to national security, the international community needs to strive for international cyber stability. This is a more peaceful environment where all states are able to exploit the benefits of cyberspace positively, where there are benefits to state-to-state cooperation and little incentive for states to attack one another. We are currently pursuing a number of efforts to achieve this goal.

"We need a shared understanding of norms of acceptable state behavior in cyberspace."

First, we are working to develop a shared understanding of norms of acceptable state behavior in cyberspace. Senator Bockel talked about having in the long term some kind of U.N. code of conduct or binding document. I do not think we are close to being there. Because this is still such a new area, we are trying to build cyberspace norms that are grounded on the physical world norms and to get like-minded countries to endorse this approach. Over time, countries that are outside of these norms would be forced to join.

At the U.N. recently, a group of governmental experts (GGE) for cyber security from 15 countries—including the U.S., France, Germany, India, China and Russia—reached a landmark consensus that international law applies to states' conduct in cyberspace. This means that international legal principles such as the U.N. Charter and the Law of Armed Conflict that have promoted stability between states during conflicts in kinetic space, equally apply in cyberspace. This consensus was endorsed in the NATO communiqué that came out of the last Summit. Although it would seem evident that the same laws that apply in the physical world should apply in the cyber world, several states felt that a whole new legal regime had to be created; so getting this consensus among these diverging countries was very important. The group also reached consensus on other key issues such as an affirmation of the applicable law of state responsibility to cyberspace, the important role of confidence-building measures, and the vital importance of capacity building to enhance global cooperation in securing cyberspace. Finally, the group agreed that all these efforts combined supported a more secure and stable cyberspace.

Progress with Confidence-Building Measures

Second, our international security work is focused on confidence-building measures (CBMs). Confidence-building measures were born in the nuclear age and intended to build better confidence, transparency, and cooperation between countries—sometimes adversaries, sometimes "frenemies," sometimes friends. So, the concept is not new but it is applied to cyberspace as a way to prevent an inadvertent misunderstanding of an incident of national cyber security concern emanating from the U.S. or another country that could lead to inadvertent escalation. The first bilateral CBMs were reached between Russia and the U.S. and signed by Presidents Obama and Putin about two years ago at the G8 Summit. In December 2013, the first multilateral confidence-building measures were elaborated among the 57 countries of the OSCE. That was very significant and we are now in the implementation phase of these measures.

Dealing with Non-State Actors and Cyber Crime

This work addresses the activity of state actors but does not directly address the substantial risk posed by non-state actors. The U.S. government therefore believes that any attempt to increase resilience and reduce the risk in cyberspace also has to look at non-state actors. A key area for this is cyber crime and how to deal with it. In order to effectively fight cyber crime, countries around the world need to have in place three basic elements that are all addressed in the Council of Europe's Budapest Convention. This convention is not just European; it is open to all countries and is the only cyber crime convention that has strong and harmonious substantive cyber crime laws.

"The ILOVEYOU virus was traced to the Philippines—which had no law that actually punished this crime."

- *Strong cyber crime law*s. At the time of the ILOVEYOU virus many years ago, the perpetrators were traced to the Philippines but the Philippines had no law that actually punished this crime. So, with countries around the world, we have been trying to work on stronger laws because this is the weakest link issue. A smart criminal will rig his attacks through different countries to avoid detection. Therefore having strong cyber crime laws everywhere is important.
- *Investigative tools and trained forces.* At the same time, it does not matter how strong substantive laws are if there are no comprehensive investigative tools in place for addressing high-tech crimes and digital evidence. Investigative tools and trained investigative forces are required.
- *Mechanisms for formal/informal cooperation internationally.* Effective mechanisms for formal and informal cooperation internationally are also needed. The 24/7 High Tech Crime Network started in the G8 and covers over 60 countries today. Interpol also has cooperative mechanisms on hand. We are promoting all these things on a diplomatic level around the world.

In the fight against cybercrime, we are also committed to strengthening international cooperation by working on electronic evidence. President Obama announced our efforts to streamline our mutual assistance policies. Many debates about data localization and countries wanting to have local data storage are born less out of debates about surveillance and more out of debates about getting actual access to law enforcement information. So there has been a push to streamline and bolster our ability to react more quickly. It is good to have all these capabilities but countries also need capacity and we are building capacity on cybercrime around the world with our colleagues in the Department of Jus

"A key priority is due diligence: States should protect their information infrastructures and national systems from damage or abuse."

Due Diligence in Cyber Security

Another key priority, which is distinct from international security, is cyber security due diligence—the principle that states should recognize and act on the responsibility to protect their information infrastructures and national systems from damage or abuse. It is one of France's priorities and the U.S. is taking vigorous steps in that direction.

President Obama has issued an executive order to ask the National Institute of Standards and Technology (NIST) in our Commerce Department to create Voluntary Best Practices, a voluntary framework of standards for our critical infrastructure. This is not a one-size-fits-all approach but one that really looks at the different behaviors out there so that we can assess the risks and go forward in a productive way. This security framework is now being implemented and we want to make sure that it is interoperable with our international partners. So, we are engaging countries around the world to verify that they have done good cyber security due diligence, that they have institutions in place like national level Computer Emergency Response Teams (CERTS), and that they have national strategies in place.

As an example, we have been facing a number of denial-of-service (DoS) attacks against our financial institutions. These attacks, made by botnets—which are compromised computers all over the world—were not actually undermining the integrity of the institutions but affected the institutions' outward ability to deal with customers. So our technical and law enforcement teams reached out to countries around the world, including countries that we do not get along with all that well, and asked them for help. This is called a diplomatic démarche. This cooperative framework was a success and it is something that we really want to build.

Promoting Consensus on Internet Governance

I will briefly talk about two other points. One policy challenge is to promote greater consensus on Internet Governance. I just returned from Busan in Korea where this issue was being debated at the ITU. Previously, there was a big meeting in Brazil, called NETMundial, which endorsed the multi-stakeholder system of Internet Governance that led to the creation and flourishing of the Internet, versus endorsing an intergovernmental system. An intergovernmental system is not the way to go because it does not have the other stakeholders there—the technicians, the industry, and the civil society—and if you can imagine governments trying to negotiate every change in the Internet, we would still be using the abacus at this point. We would not have the Internet we do. So, there is a tectonic battle between states that believe information is a threat and talk about "information security," and states that talk about "cyber security" and see the economic, social, and other benefits of an open platform. So, this Internet governance debate is an important ongoing debate.

"There is a tectonic battle between states that believe information is a threat and states that see the economic, social, and other benefits of an open platform."

Human Rights Online and Internet Freedom

"States are often using the specter of security issues to try to curtail Internet freedom."

Finally, and closely related to that, is the idea of human rights online and Internet freedom. The Freedom Online Coalition, a partnership of 23 countries, is working to preserve an open Internet freedom. Again, states are often using the specter of security issues to try to curtail Internet freedom. We have to be very careful that this does not happen and make sure that there is a free flow of information. In the developing world, many G77 countries and countries in Africa have some sympathy for the idea of stability. These states are worried about stability but they also are worried about economic development. So we need to make a case to them that an Open Internet is a platform for economic development, one that will benefit them. Undergirding all these efforts, we are spending a lot of time on capacity building regionally, in Nairobi for the East African community, in Senegal where we are partnering with France for the French speaking West African community, in Ghana for the English speaking West African community, and in Botswana. All of us need to work on raising the capability of these states that are joining in the discussions and ultimately understand that this is a beneficial technology to them.

Establishing a Framework of Norms and Transparency Measures to Reduce the Risk of Cyber Conflict

Ms. Michele Markoff
Deputy Coordinator for Cyber Issues, U.S. Department of State

My talk will be a continuation of the conversation that Chris Painter just started. I can do a little bit more of a deep dive into some of the questions on the framework, on the norms and the confidence building measures (CBMs), and on exactly what our end goal is. It should be no surprise that we have come to believe that the evolution of cyber threats requires us to mount a very dynamic, agile, and resilient technical response. Those of us who are old enough to remember the Cold War and the advent of nuclear weapons into the security equation will not be surprised to learn that our response to the cyber threat requires a thoughtful and collective policy response—one designed to manage crises and able to reduce the prospect that conflict would actually occur.

"We are addressing these challenges not only with the help of our closest allies but also with support from Russia and China."

From the U.S. vantage point, we have approached this challenge by conceiving a framework of principles of expected state behavior supported by confidence and security building activities which are designed for all nations, in order to be universal, because it would be in their security interests. In addressing this question, it is not only with the help of our closest allies but also with support from Russia, China, and many others that we have been able to take some very key steps in this direction.

Most of you in the cyber field have heard of this term, "U.N. GGE," which stands for United Nations Group of Governmental Experts. These groups come about pursuant to a U.N. Resolution in one of the committees. In this case, there is a longstanding Russian resolution on information security that started in 1998 and, in the early 2000s, it began to call for the establishment of groups of governmental experts. We have had four of them and are in our fourth now. It was in the second one that the U.S.—in order to counter a call for an arms control type of framework which would have sought to ban offensive cyber tools—responded by saying that what all states needed to do was to affirm that the longstanding rules of international behavior and conflict should also apply to cyber space.

"All states needed to do was affirm that the rules of international behavior and conflict should also apply to cyber space."

It also recommended that, to support that effort, states needed to cooperate regularly and pragmatically against common cyber threats in order to build some transparency and predictability into their military behavior in cyberspace. This is because, unlike kinetic weaponry, there are no external observables in cyber space. You cannot learn what the intentions are by observing the movement of forces. You cannot put something on the tarmac and have it opened up and be seen by other states.

These recommendations took two Groups of Governmental Experts to come to fruition, which happened in June 2013. They received universal support from the GGE members, a very diverse group that included 15 of the most prominent cyber powers ranging from India to the U.K., France, Germany, Russia, China and others, because it was recognized that, if implemented, they could reduce the risk of conflict and misunderstanding. The conclusions by the GGE that international law applies and that CBMs ought to be adopted were affirmed at the Wales Summit by NATO members this year. This is a very important affirmation because of course we want universal affirmation.

The confidence building measures are achieving life in a number of venues. We concluded an agreement with Russia on 3 CBMs. We also agreed on a CERT to CERT relationship using the U.S. and Russian nuclear risk reduction centers, which were established in the 80s to implement nuclear arms control reduction agreements in order to manage cyber incidents appearing to emanate from the territories of either the U.S. or Russia. We are not talking about seeing something come from somewhere else in U.S./Russia talks. But in the event that something that emanates from either of our territories reaches the threshold of an international security incident, we have templates through which we can query each other about information or requests for action. In addition, we have plugged in another telephone in the White House and one in the Kremlin that are devoted exclusively to cyber incidents.

"We have a telephone in the White House and one in the Kremlin that are devoted to cyber incidents."

In the OSCE, after two years we have achieved eleven OSCE measures that we are in the process of implementing. Most of them are transparency measures where states have provided their views on how they operate in cyberspace. An extremely important one is a cyber conflict mediation measure that would permit the victim of a cyber attack perceived to be coming form another OSCE state to request mediation and assistance. This measure, together with the international legal norms that we are affirming, provides for a duty to assist and may be a much needed intermediate step—and one that was not available in Europe at the time, for example, of the cyber attacks on Estonia where Estonia kept asking for Russian assistance and none was forthcoming.

I would note that, next week in Vienna, we will have a Swiss-sponsored conference to preview potential cooperative measures that we want to take up in the coming year. These measures would go beyond transparency and put into place regional cooperative activities designed specifically to address contemporary cyber threats and challenges, including things like regional activities on cyber-enabled electrical infrastructures where electricity generation is transnational. We have not stopped with Europe either. We have also proposed taking up CBMs in ASEAN, the regional forum in Asia, and we hope to build on existing cyber coordination in our own hemisphere in the Organization of American States.

Looking forward, a new U.N. GGE which started in July in New York focuses on how international law will apply to state behavior in cyberspace. As Chris noted, what does proportionality and distinction mean when you have reached the threshold of the use of force? How does the law of armed conflict truly apply? But the U.S. submission to this new GGE goes farther by providing a detailed examination of these legal issues and also advancing three additional norms. These norms are designed to address the usability by states of offensive cyber tools below the threshold of the use of force. There are three very important norms that would appeal universally to the world which are the following:

- A state should not conduct or support online activity that damages critical infrastructure,
- A state should not conduct or knowingly support activity intended to prevent ICS-CERTS from responding to cyber incidents and,
- A state should cooperate with requests for assistance from other states in investigating cyber crimes that appear to emanate from their territory.

If I had more time, I would also like to talk about the future and about where we are going with all of this. For example, there are measures of self-restraint that are stability measures. Hopefully, this will be addressed later in our workshop discussions.

The Hyperconnected World Impact on Cyber Actors, Threat Vectors and Attack Surfaces

Mr. Haden Land
Vice President, Research and Technology; Lockheed Martin IS&GS

Dr. Roger Weissinger-Baylon: Dr. Linton Wells II; Mr. Haden Land, Vice President, Research and Technology; Lockheed Martin IS&GS, and Mr. Henri Serres (left to right).

I am speaking to you today from four integrated perspectives, that of a large global aerospace and defense employer of technology professionals, a holder of three academia university trustee board positions, member of various industry working groups such as the World Economic Forum, Hispanic IT Executive Council, and a recognized leader in the information technology field.

Giving appropriate attention to the macroeconomic drivers and trends that will influence the future cyber ecosystem is of great importance to world leaders, like many of you in this room. These drivers include Motivations, Mechanisms and Mitigations.

"We must deal with the maturation of cyber bad actors, improvement of threat vectors, and increasing attack surfaces."

- *Motivation* examples are level of trust, interstate/country tensions, corporate IP theft and deterrents to cyber crime. The maturation of the cyber bad actors, improvement of their threat vectors and a rapidly increasing attack surface all contribute to adding complexity to the cyber ecosystem.
- *Mechanisms* include the democratization and convergence of technology and the balance between offensive and defensive investments. Previously independent technologies, such as cloud computing, big data, mobility, social and many others have now become highly interdependent, driven by the Internet of Everything and resulting in the hyperconnected world that we live in today.
- *Mitigation* includes things like sophistication of institutions, interstate/country cooperation and sophistication of the workforce/end users.

The diligence for effectively managing security risks and the required skills and tradecraft to build a strong cyber security workforce are changing rapidly due to this hyper technology convergence and the evolving threat landscape with a diverse set of actors and behaviors.

"Cyber security will require individuals who can both problem solve and think creatively."

Albert Einstein once said, "Education is not the learning of facts, but the training of the mind to think." I can assure you that many jobs of the future, including the cyber security professions, will require individuals who can both problem-

solve as well as think creatively—thus combining convergent and divergent thinking. My colleague, Roya Mohadjer, will address this important topic during her speech later today.

Increasing citizen awareness of the importance and career potential of fields within cyber security is necessary. As an industry advisor to the United States National Cyber security STEM Education board, I feel we are taking prudent steps to improve educational opportunities that connect students with cybersecurity careers in order to generate an effective pipeline of future employees. Furthermore, as a founding member of the National Cyber Security Hall of Fame, we now have an exceptional platform to honor cyber security icons so that others can aspire to be like them. We have inducted fifteen individuals since 2012 with the next induction ceremony occurring this Thursday in Baltimore, MD; five more individuals will be inducted.

The speed of technology change is dramatic. Thus we need more of our workforce engaged in science, technology, engineer and math disciplines. I strongly believe that today's technology was yesterday's magic and will be tomorrow's given. Arthur C. Clarke had a wonderful quote—"Any sufficiently advanced technology is indistinguishable from magic"

The explosion in the number of IP devices along with the data growth of the world wide web has created the following Internet experience every 60 seconds:

- 200 million emails
- 2 million Google searches
- 510 thousand Facebook comments
- 100 thousand tweets
- 47 thousand Apple app store downloads.

There are almost 15 billion devices continually connected and 50 billion occasionally connected to the Internet. By the end of the decade, we will have 30 billion constantly connected and 200 billion occasionally connected. It is worth pointing out that the chip in a typical smartphone is now one million times cheaper, one hundred thousand times smaller and ten thousand times more powerful than the first computer invented by MIT—the Whirlwind.

"The information explosion brings a much greater threat from cyber security attacks."

In 2013, the global society generated over 3 zettabytes (10 to the 21st power) of new information on the Internet; in 2020, that number is forecast to be 30+ zettabytes. By the end of the century, the Internet will be measured in yottabytes, which is 10 to the 24th power. Downloading a yottabyte would take you 10 trillion years on a typical high-speed network. This information explosion brings a much greater threat from cyber security attacks.

Mega breaches are when personal details of at least 10 million identities are exposed in an individual incident. There were eight in 2013, compared to one in 2012. Approximately 67% of websites used to distribute malware were identified as legitimate, compromised websites. Ransomware attacks grew by 500 percent in 2013 and turned vicious. Attackers are starting to turn their attention to the Internet of Things: Baby monitors, printers, security cameras, and smart televisions were hacked in 2013. Furthermore, security researchers demonstrated attacks against automobiles, medical equipment, and wearable devices.

"In 2013, there were eight "mega breaches"—each leaking more than 10 million identities."

With these examples in mind, I shall share some brief recommendations regarding institutional readiness:

- Prioritize your information assets based on security risks
- Provide differentiated protection based on importance of assets

- Develop deep integration of security for the interdependence driven by technology convergence
- Develop active defenses to uncover attacks proactively
- Establish the needed pipeline for the cyber security workforce
- Integrate cyber-resilience into enterprise-wide risk management and governance processes
- Influence policy to better enable the hyperconnected world.

In closing, consider this Latin motto— “Aut viam inveniam aut faciam"—which means “Either find a way or make one.” So I personally ask each of you to stay abreast of the motivations, mechanisms and mitigations of the cyber security landscape and increase our collective focus regarding information sharing, critical infrastructure resiliency and policy development.

National security relies upon effective preparation and resilience of critical infrastructure from commercial through government assets, systems and networks.

The Security of Infrastructures

Mr. Henri Serres
High Council for Economy, Industry, Energy and Technology, French Ministry of the Economy and Finance; Member of the Board of Directors, Orange Group

Introduction

As a former Director at the DGSE (General Director for External Security) and the SGDSN (Secretariat General for Defense and National Security), on both sides of our national security agencies, I have had previous occasions to be invited by Roger Weissinger-Baylon to this workshop. Consequently, I will try to introduce my new activities at the High Council for Economy, Industry, Energy and Technology in the Ministry of Economy. I hope that they may be of interest to you.

What is the High Council for the Economy?

The High Council is chaired by the Minister of Economy, currently Emmanuel Macron. It consists of about 50 people, who have occupied senior positions in the civil service. They provide advice, expertise, and assessments relative to public policy in their fields of competence—industrial technologies, energy, information and communication technologies, roles of industry, and the economy in general.

What Recent Areas of Preoccupation are Related to Cyber Defense?

Critical Infrastructures. Recent events have shown that mobile networks, previously having a "function of comfort"—making things easier through mobility—have moved into the field of critical infrastructures. More and more "sensors," are now connected, in order to reduce costs, through mobile networks.

At the same time, security services tend to rely more heavily on mobile phones—to receive alerts, to recall off-duty resources in case of an emergency, etc.

Energy is a growing concern. Ordinary fixed telephone lines tend to have an independent electrical supply, but fixed lines may migrate to IP, which requires electrical current in order to function. And mobile phones need access to electricity to recharge batteries, and base stations depend on electrical supply as well.

"Very few studies or plans take into account the possibility of multiple causes of disruption."

Very few studies or plans take into account the possibility of multiple causes of disruption. It is assumed that critical networks are in jeopardy from only one cause at a time, which is not true in real life.

Connected Vehicles. A lot of research has been devoted to various experiments, from vehicles connected to the road to vehicles without a driver. We also have extensive contacts with industry to ensure that appropriate cyber mitigation processes are taken into account.

For example, it could be much more expensive to introduce design modifications later in the process of developing the connected vehicle technologies. As of now, we are satisfied that the industry is taking a slow, progressive path, rather than aiming at a completely new concept (which might involve greater risks).

What Incentives Could We Imagine to Enhance Cyber Security?

In cooperation with our national security agency concerned with cyber security (ANSSI) and following a report by Minister Macron, I am now involved in a mission concerning the role that insurance companies may assume in the cyber security field. At the present time, the law requires

critical infrastructure companies to report regularly to ANSSI on possible attacks, so as to share experience and provide faster alerts after new attacks. But we fear that small and medium-sized enterprises (SMEs), which are essential to the welfare of the economy, tend to lag in the process of protection against cyber threats.

"It is the small and medium-sized enterprises that tend to lag in protecting against cyber threats."

Insurance companies could be useful in proposing solutions to mitigate the consequences of attacks to their operations, to their own data, to personal data about their customers. The objective of insurance companies, of course, is to reduce the level of exposure to risks arising from their clients. Therefore, they may have strong incentives to promote best practices. IT and consulting companies could also benefit from the process and be partners with both sides.

"Insurance companies could be useful in proposing solutions to mitigate the consequences of attacks."

The French government also believes that a more innovative industrial approach could make it easier for SMEs to get access to better security services, for instance, through a specific "box "or easier access to Cloud Services.

Privacy is another areas of concern. Apart from the general rules concerning cyber security, there are new areas of investigation and concern involving the role of privacy in "big data:" anonymization of data and homomorphic encryption (a form of encryption that "allows specific types of computations to be carried out on cipher text and generate an encrypted result which, when decrypted, matches the result of operations performed on the plaintext.")

Conclusion

At this point, my conclusion would be that, although cyber threats are looming, they do provide a motivation for research and development. And this could foster the creation of new small and medium-sized enterprises. France has a strong mathematical tradition—although possibly lacking in business experience—which could contribute to new fields of investigation.

Malware Information Sharing and Standardization

Mr. David Grout
Director of Pre-Sales Southern Europe, McAfee, Part of Intel Security

First, I want to thank everyone for this great event, for this beautiful location at the Invalides, and for the talented and knowledgeable people we have in this workshop. My main duties inside Intel Security are to run technical relationships with the industrial and public sectors in Southern Europe, including Spain, Portugal, Greece, Italy, and, of course, France.

The Explosive Evolution of the Malware Landscape

This brief presentation will center around information sharing. Over nearly a decade in the security business, I have witnessed an extraordinary evolution across the malware landscape: We call it the "explosion curve." As an example, in 1995, we had to deal with five new samples per day sent over floppy disk. When I began working at McAfee in 2003, we were encountering about 5,000 new instances of malware per month. As of today, we are receiving new malware roughly every 4 seconds. This "explosion curve" highlights the fact that we need automation and standards in order to tackle and fight threats.

Even with more than 400 researchers as well as nine data centers over the world dedicated to cyber analysis, we cannot scale large enough to keep up with this explosive trend by ourselves.

The time when finding a new form of malware such as I love You, Conficker, or Kournikova could be considered a real victory is almost gone, and we need to focus more and more on sharing Intelligence and stepping up remediation capabilities.

The Need for Sharing Malware Information—and for Sharing Standards

Even a large enterprise or public entity cannot rely completely on its own research capabilities. Therefore, we need to find ways to share the essential details of the malware—which I will call the malware's DNA—and its behavior. This has led the market to be concerned with vulnerability assessment, discovery, and risk management. And it has been done through several standards including: OVAL (Open Vulnerability and Assessment Language), CVSS (Common Vulnerability Scoring System), CVE (Common Vulnerabilities and Exposures, hosted by MITRE) or XCCDF (eXtensible Configuration Checklist Description Format).

"It is time for industry and public entities to sponsor and help malware sharing standards to grow up and become adult."

Today, it is time for the industry and for public entities to sponsor and help malware sharing standards to grow up and become adult. We can already cite as examples: IOC (Indicator of Compromise), STIX™ (MITRE's Structured Threat Intelligence eXchange) or CybOX™ (the Cyber Observable eXpression).

As a company, we see several possible ways to promote such standards: The first approach is to develop and maintain products that are "standard ready." We did this by introducing to the market the first local Intelligence repository (Threat Intelligence Exchange) with the ability to rely on IOC and STIX locally without depending on our reputation Cloud. The second method is to share information through these languages, and we are investigating this approach through our Cyber Threat Alliance participation.

"The first approach is to develop and maintain products that are standard ready."

Concluding Remarks: The Vital Importance of Collaboration and Standardization

In conclusion, collaboration in fighting against the malware threat is key for the industry. It will give us the ability to focus our Intelligence on the high-level, truly bad actors, and it will eliminate the duplication of analytics.

Standardization is also a key element and a foundation for this sharing. We need to set up rules and frameworks to make exchanges available and sustainable in the future. Standardization will also open the door to interoperability and automation, which are key elements to manage the Big Data world.

And finally, we will need to create a foundation for our sharing based on trust: To be sure of what we can all share together, what we want to share, how we want to share, and what the level of confidence we can have in the shared information.

Mr. David Grout, Director, McAfee part of Intel Security; Mr. Chris Painter, Coordinator for Cyber Issues, U.S. Department of State; Ms. Michele Markoff, Deputy Coordinator for Cyber Issues, U.S. Department of State; Dr. Linton Wells, Middlebury Institute of International Studies and National Defense University; Mr. Haden Land, Vice President, Research and Technology, Lockheed Martin IS&GS; Mr. Henri Serres, High Council for Economy, Industry, Energy and Technology, French Ministry of Economy and Finance (from left to right). Panel on Cyber Security Foundations: Norms, Governance, Infrastructure, and People.

Active Cyber Defense: A Critical Analysis

Dr. Frédérick Douzet
Castex Chair of Cyber Strategy, Institut des hautes études de défense nationale (IHEDN);
Professor, University of Paris 8

Active Cyber Defense as a Geopolitical Concept

All the issues we are discussing in cyber take place in a spatial context and in a geopolitical context. In geopolitics, we study power rivalries between political forces over territories, including those taking place in cyberspace. Therefore, ideas, representations, and concepts about cyber conflicts also emerge within a spatial context. In geopolitics, we believe that the ideas, concepts, or terms that we use are not neutral. They play an authentic role in geopolitical conflicts. I also want to look at active cyber defense, because it seems to be the new buzzword. It has clearly emerged in the United States, where it is widely used in the strategic literature. And now it appears under different forms, in the various cyber strategies and doctrines of a few other nations. It may be proactive or active. It was also the topic of a cyber conflict conference in Tallinn last spring.

"In geopolitics, we believe that ideas, concepts, or terms play an authentic role in geopolitical conflicts. "

One problem is that the concept is very ill-defined and in Tallinn there were just about as many definitions as speakers. In fact, there were possibly more definitions than speakers about this term.

We all agreed that we disagreed on what "active defense" actually is. There seems to be some kind of "in between" or grey area. There is definitely a more aggressive component than just defense. And there also seems to be a widely shared assumption that strengthening defense is not enough, and that an extra step is needed. But what this extra step is about remains to be defined both technically, politically, and legally. So it has emerged clearly in a context of mounting tensions about cyber threats and increasingly strong statements about the proliferation of cyber attacks, of course, that are more targeted and more sophisticated. It has become a strategic priority for many nations.

There are many concerns about the safety of critical infrastructures but we also see many nations that have announced offensive capabilities including France, Great Britain, and many other nations that are showing muscle about their cyber capabilities. Therefore we are in a context where I think we are taking an increasingly offensive path. It is also a context of very strong rivalry between the U.S. and China, with the last step being the indictment of five Chinese officers in May 2014 for hacking U.S. companies' computers to steal trade secrets. All over the place, we seem to have a lot of tough talk. We also find a sort of discursive link in the political and media discourses between cyber espionage for economic advantage, threats against critical infrastructure, and strategic threats to national security. All of that is sort of creating confusion among the public about what we are talking about.

What Purpose Does the "Active Cyber Defense" Concept Serve?

I am not saying that the threat is not real. It is, and we need to think through the responses. Yet, my question is what is the added value of the concept of active cyber defense? What purpose does it serve? Why don't we just distinguish between what is strict defense—meaning non-offensive actions—and what is legitimate or legal offensive actions, what types of countermeasures, preemptive strikes, and so on that we want to use? Why are we using a concept that is creating so much ambiguity? My hypothesis is that active cyber defense is what we call a screen concept in geopolitics. It is a screen because it hides a lot of power rivalries and

"Active cyber defense is what we call a screen concept in geopolitics."

strategies of actors but, in turn, it plays a role in these conflicts. So what purpose could it serve? Well, it serves the purpose of showing that we are actually taking action as opposed to doing nothing. Again, there is a proliferation of cyber attacks. So, active cyber defense is among a number of strong statements that help create public pressure for action regarding cyber attacks. It also encourages various kinds of actors to take action. And it raises awareness within public agencies as well as within the private sector. Overall, being aggressive, being offensive, seems to be publicly more rewarding—and it is more sexy than just patching vulnerabilities.

Active cyber defense is "more sexy than just patching vulnerabilities."

It can be argued that it helps to justify the means that are being devoted to cyber security, whether it is the cyber arms race with the idea of raising the cost for the enemy, building capabilities to deter the enemy, but of course deterrence in cyberspace is another story. It might also sometimes justify some off-limits actions that have been tried in cyberspace. And I guess we can argue that it is good for business if you start looking at the videos advertising cyber security companies that are doing active cyber defense.

The Concept of Active Cyber Defense has a Potential for Conflict Escalation

I believe that the concept of active cyber defense raises serious questions and has a potential for conflict escalation. First of all, in cyberspace the lines are kind of blurred between the public and private sector because the critical infrastructure is run by private operators. Many governments are subcontracting to the private sector, including for defense. So we have a sort of migration of a concept that is a military concept into the business world. This raises the question of "hack back," attacking the attacker, and even sometimes tracing back the attacker. That can raise some legal issues.

"Even though many deny that active cyber defense means to hack back, a lot of companies have been crossing the line."

So, even though many deny that active cyber defense means to hack back, a lot of companies have been crossing the line, and a lot of governments too, obviously. A survey at the Black Hat security conference a couple of years ago found that a third of the respondents had engaged in hacking those who had hacked them, and a good share of them said they had done so frequently. That of course raises serious technical, legal issues, and potentially diplomatic crises.

There are high risks of escalation linked to these issues, such as unintended consequences. Since computer networks are shared, do we know what might happen when we strike back? There are all the difficulties of attribution and there are a lot of "what ifs?" And, in particular, what if there is human or computer error or miscalculation?

With automatic hack back, we can also wonder whether we know how machines will behave if something goes slightly wrong. Actually, how much do we know about how unmanned systems are likely to react?

"There is a risk that some exchanges of cyber weapons might spin out of control."

All this is linked to another powerful representation, namely, that systems are more reliable than human beings. Yet, while we know a lot about human weaknesses, we know a lot less about unmanned systems' weaknesses and what the consequences could be. Thus, I believe that the guy who pushes the buttons needs to better understand what he is doing—otherwise there is the risk that some exchanges of cyber weapons might spin out of control.

How to Build a Framework of Norms for Responsible Behavior

Last, how do we build a framework of norms for responsible behavior if the lines are not clear between what is acceptable and what is not, or between what is legal and what is not? If we blur the

lines in a way that we cannot see them ourselves, then we blur them for everybody else as well. Thus, I believe there may be major legal and ethical issues that could be raised, and many of them still need to be resolved.

"We will certainly not be on the moral high ground if we condemn actions by others that we are doing ourselves."

We do not really have a consensus as to what are appropriate countermeasures in cyberspace, or how to apply international law. In addition, it is difficult enough to build a framework among like-minded nations for active cyber defense. Therefore, we definitely do not know how things would play out with nations that are not like-minded. This raises concerns about opening a Pandora's box in the case of offensive actions. It does not mean that we will not do it anyway, but we will certainly not be on the moral high ground if we condemn actions by others that we are doing ourselves.

To conclude, I would say that active cyber defense seems to be a rather young, ill-defined, and very ambiguous concept. It reveals a clear trend in the strategic debate towards an offensive path. Moreover, I think that the potential for escalation is real, because in an absence of a clear framework and very strong safeguards, active cyber defense could take on a life on its own.

Mr. Jim Cowie, Chief Scientist, Dyn; Dr. Frédérick Douzet, Castex Chair of Cyber Strategy, IHEDN; Major General David Senty, Director of Cyber Operations, MITRE (left to right).

Remarks on Geopolitics and the Cartography of the Internet

Mr. Jim Cowie
Chief Scientist, Dyn

I am going to take a shot at describing the "Cartography of Cyberspace", even without Powerpoint. It will be difficult, but I will count on the fact that most of you have a really good grasp of geography. Hopefully I can just describe the map and it will appear in your heads.

When I hear the term "cyber strategy," I think that a lot of investment to date has been reminiscent of the people throughout history who built castles. They hardened these castles. They spent all the money that they did not spend on hardening castles on building siege weaponry to take on other people's castles. And yet when we step outside our castles on the Internet, it is as if we are equipped with a sixteenth-century map that has sort of rough outlines of continents, and sea monsters on it, and not a lot else.

"The internet is a very physical infrastructure. The Internet represents the roads among us—built by people in pursuit of specific goals"

Today I am going to try to share with you a little bit of intuition about how the Internet is a very physical infrastructure. The Internet represents the roads among us, the roads that connect our castles. Those roads are being built by people in pursuit of specific goals. Sometimes these are diplomatic goals, but more often they are simply business goals; these are companies trying to make a dollar.

The Internet as Physical Infrastructure

That physical infrastructure, the cyber infrastructure, actually mirrors a lot of other infrastructures that you are very familiar with, since they come into play during times of conflict, such as the power grid, or energy pipelines. And its physicality is really what makes it worthwhile to think about the survivability of the Internet in different kinds of conflict zones.

"The cyber infrastructure actually mirrors a lot of other infrastructures such as the power grid, or energy pipelines."

The Internet itself is made up of voluntary interoperation among about 48,000 independent networks. Some of those networks are only the size of this room, and some of those networks are on every continent. But they have voluntarily created a web of bilateral interconnections among themselves, about 350,000 in all. That map of interconnections and relationships is what I mean when I say that Dyn "makes maps" of the Internet.

Most of those interconnecting agents, most of those players, are in well-known places. We can determine where they are, and then by mapping the logistical network of the Internet, how people get traffic from one place to another to accomplish specific goals, we can understand the properties of that map. On that Internet map, as somebody mentioned yesterday, you can see all the different human behaviors at work: Cooperation, competition, and conflict, usually all at the same time.

Categories of Conflict Zones and Internet Connectivity

Today I would like to describe three different categories of conflict zones, in terms of the Internet that holds sway there. And you will see that, as a general rule, as the Internet infrastructure increases in complexity, not to say regulation, but complexity, it becomes more stable and more survivable, even in the face of some very significant conflicts.

Libya

So, for a first category, I might pick Libya as an example of a country with just a little Internet. It is a place that before the war had one primary submarine cable, and since the war has rushed to completion a second cable, the Silphium cable from Greece.

"You need to keep building the Libyan Internet to create a more survivable infrastructure."

Diversity has gone up in Libya, no doubt, indeed, doubled; there is now independent connectivity in both Tripoli and Benghazi. There is a reasonable national fiber optic network. But because that is still not "enough" diversity, we have continued to see Internet outages. The Silphium cable was taken offline shortly after going active. And as recently as July, we saw large portions of the Libyan Internet become unavailable due to fighting and blackouts and power problems. So clearly you need to keep building and diversifying the Libyan Internet to create a more survivable infrastructure.

Yemen

We might also look at a country like Yemen. This morning, about the time we were all having our coffee, Yemen lost about 80% of its Internet capacity. Yemen is basically served by two submarine cables: A newer one and an older one. And everything that was connected to the newer one is dead at the moment. That leaves them with about 20% of their total capacity; again, the result of heavy fighting. That is clearly not enough Internet diversity to preserve the cyber infrastructure in that country from the chaos that is going on there.

Iraq

We can continue from there. If I were to pick an example of a country that has more diverse connectivity, actually pretty good connectivity, I might look at either Afghanistan (ironically) or Iraq. Perhaps because it is more timely for our discussions about conflict and stability today, let's talk about Iraq.

If you can imagine somebody sending an email in Iraq, that email is going to transit the Internet to some server, perhaps in California. The Internet traffic will leave the country, and the results will come back. As it turns out, there are about five different physical paths that that traffic can travel on when it leaves Iraq. And if you picture them as I describe these to you, each of these is a very familiar, in many cases, ancient, transit zone, that should be very familiar to you from the perspective of other kinds of infrastructure and the history of regional conflict.

"Iraq has a submarine cable near Basra, which goes to the UAE…a terrestrial cable to Kuwait, which connects to other fiber-optic connectivity that goes under the Gulf to the Strait of Hormuz."

Iraq has a submarine cable that connects near Basra, at al Faw, which goes to the UAE. They have a terrestrial cable to Kuwait, which connects to other fiber-optic connectivity that goes under the Gulf to the Strait of Hormuz. They have a terrestrial connection over the highway to Jordan, which then connects to Jordan's domestic infrastructure and goes off to a Red Sea cable landing at Aqaba.

Iraq also has important additional connectivity through Kurdistan, in the north, to Turkey, and that connectivity actually follows energy pipelines. As Jamie Shea mentioned this morning, energy is critical, and there is actually a lot of linkage between energy delivery today and information delivery.

Finally, Iraq has multiple telecommunications connections to Iran terrestrially. And the Iraqi traffic that is carried by Iran can go over a couple of different paths in order to reach a European market. It can go to Southern Russia, for example, ironically following the great circle route through Ukraine to reach Frankfurt. Or it can actually go on what is known as the Caucasus Cable System (CCS), so they

may hand off the traffic in Baku, and have the CCS carry that traffic across Azerbaijan, through Georgia, underneath the Black Sea, come ashore in Bulgaria, and on to European and American markets that way.

That is an amazing range of interconnections. And it is that web of 100% commercial relationships among dozens of different telecommunications providers that keeps Iraq's Internet reasonably stable, even in circumstances where you would be led to believe that there would be interruptions in service.

Ukraine

If we want to go up even one more level of complexity to a country that has really very good Internet connectivity, we could discuss Ukraine. Ukraine has sort of a telecommunications blessing in that it has a lot of highways and rail lines, East-West infrastructure, all of which has buried beneath it quite a lot of fiber optic resources. I mean, truly a lot of Internet. Ironically, a lot of that infrastructure was built in order to service the Russian markets' demands, so a lot of Russia's Internet traffic probably still travels underground through the Ukraine.

"Ukraine has sort of a telecommunications blessing—it has highways and rail lines, East-West infrastructure, which has buried beneath it a lot of fiber optic resources."

It is perhaps interesting to note that when we were all watching the Euromaidan demonstrations, we wondered what would happen to Internet connectivity there. We started setting Internet routing alarms to alert us if anybody should attempt to shut down the Internet in Kiev.

Of course, it was not shut down. We were all able to watch that protest event from any number of live cameras placed all around Independence Square, 24 hours a day. Indeed, people were tweeting updates live on social media as the police approached the barricades, as buildings were set on fire, and everybody on Earth could watch that happen, because of the stability of the cyber infrastructure in the Ukraine.

Now there has been some significant localized impact, I think, in the East. We have seen local access networks shut down in Donetsk, and in Lugansk, which is not entirely surprising; it is like the local phone company's infrastructure being powered down or shut down. But remember, Eastern Ukraine is basically at the end of the Internet. Nobody else outside Eastern Ukraine depends on Eastern Ukraine's Internet access networks for further connectivity. So it is kind of like a leaf node in the network going out, and it is being gradually restored over time.

Crimea

"Crimea…is perhaps the most interesting example of evolution during conflict."

Finally, we might look at Crimea, which is perhaps the most interesting example of evolution during conflict. Crimea is full of natural constraints in that they depend on the Ukrainian mainland for a lot of infrastructure. Not only power and gas, but also things like water, Internet, and telecommunications. As a result, we were unsure what would happen in the weeks and months after annexation; I think a lot of people were.

What happened initially, of course, was nothing. The Crimean Internet Service Providers continued to use Ukrainian telecommunications, and got to the Internet through the mainland. But then, we read an interesting geopolitical statement by [Russian] Prime Minister Medvedev. He said, and I quote:

> *"We cannot tolerate a situation in which sensitive information and documents related to the administration of two constituent entities of the Russian Federation are relayed by foreign telecommunications companies."*

He tweeted that statement to me, along with 2.4 million of his other followers, in March 2014. He charged Russian telecoms providers to build a cable across the Kerch Strait, so that the Crimean Peninsula would have its own independent Russian connectivity. The cable was completed by April, and we saw the first Russian Internet connectivity in Crimea come up in July.

As a result of that, there is now a local agent of Rostelecom doing business in Crimea, and they are busily moving over all of the Internet connections. So in the history of regional conflict, that is kind of a unique development. In some sense, it is actually an improvement in Crimea's connectivity, because as we observed, the more diversity of connection you have, the more relations with your neighbors you have, the more likely you are to stay online, even in the event of a significant conflict. And now the Crimean Peninsula has not one, but two independent connections to the Internet.

Concluding Remarks

I am truly out of time, so perhaps I will summarize by saying that people often think of "cyberspace" or the Internet as some kind of cloud: A magic cloud that delivers attackers to your door. It is definitely not as simple as that. It is a physical infrastructure, just like energy pipelines, just like the electrical grid.

"Telecommunications infrastructures matter in international relations because they are shared by neighbors—they help contribute to stability. "

And just like those things, telecommunications infrastructures matter in international relations because they are shared by neighbors. I would argue that they help contribute to stability.

Remember, unlike a gas pipeline, it is pretty cheap to build a new Internet connection between neighbors. If you have four paths to the Internet and I take away mine, I have not seriously impacted you. It is not like shutting off your gas.

But as long as you have the connection to me, our bilateral relationship creates a net positive effect, because your Internet performance will be more stable and more predictable. You will be able to reach my markets, and I will be able to reach your markets. On balance, we think that is a good thing.

Mr. Marco Braccioli, Area SpA, Senior VP; Mr. Jim Cowie, Chief Scientist, Dyn; Dr. Roger Weissinger-Baylon, Workshop Chairman and Co-Founder; Dr. Frédérick Douzet, Castex Chair of Cyber Strategy, IHEDN; Major General David Senty, Director of Cyber Operations, MITRE (from left to right). Panel on Cartography of the Cyber Threat—Mapping the Threats and their Origins.

Cyber as a NATO Mission: Recent History, Decision Points, and Opportunities that Lie Ahead

Major General David Senty
Former Chief of Staff, U.S. Cyber Command; Director, Cyber Operations, The MITRE Corporation

Since our last Workshop meeting in Paris, there have been two notable points. One came to light this morning in articles published by the Wall Street Journal and New York Times describing the successful penetration of European and NATO networks by Russian cyber-criminals; the other is the NATO Declaration issued at the September Wales Summit, endorsing an Enhanced Cyber Defense Policy. The enhanced policy calls for the defense of NATO networks and assistance to Allies in the spirit of solidarity, and achieves a tighter focus on the commitment to mutual cyber defense under Article 5. It also communicates NATO's commitment to developing cyber defense capabilities, the importance of bilateral and multilateral cooperation, and how partnerships with industry and the joint use of resources like the Estonian cyber range will be critical to the success of Alliance missions.

Today, the media announced the "successful penetration of European and NATO networks by Russian cyber criminals."

While solidarity is based upon the sharing of commitment, advantages, prosperity, and burdens among NATO members, this more resolute approach to solidarity in mutual cyber defense also infers a preparedness for escalation, should there be a cyber or hybrid conflict. This could be a challenge for two reasons:

- First, the nature of demonstrating *operational finesse* in cyber (meaning agility, speed of action, decisiveness, and confidence) is largely based upon the immersive experience and actions of experienced operators. While capabilities can be shared in shiny black boxes or through the applications and support provided by cyber rapid reaction teams, members who are generationally behind will benefit most from the sharing of threat information and discourse among partner operators about tactics and analytic techniques. This is particularly important for strengthening our posture for Article 5 action. (There is a benefit from strong peacetime or ops normal threat sharing so that we have the mechanisms and the personal connections and relationships in place for *trusted collaboration and shared situational awareness*.)

Countries "who are generationally behind will benefit most from the sharing of threat information."

- Second, some NATO members are heavily invested in the development of capabilities that could define the state-of-the-art, so our resiliency is uneven. To support a solidarity approach to cyber defense for NATO, we need to apply common standards or formats for rapid threat information sharing. There is a challenge in maintaining standards while also striving for agility, but the overall goal is continuous improvement of the whole-of-NATO cyber defense posture. This posture should be supported by a *discreet cyber assessment capability* that will help normalize the baseline for cyber defense and will also aid the collection of supporting evidence for the response decision, in the case that Article 5 needs to be invoked.

"For NATO, we need to apply common standards or formats for rapid threat information sharing."

As nations and as NATO, we need to move to a more secure infrastructure from legacy systems that have exposed attack surfaces. Two examples of this exposed attack surface over the past few months

are the Heartbleed and Shellshock (a.k.a Bashdoor) bugs.[11] The infestation of these bugs reminds us that anti-virus protection is reactive, not proactive, and has limitations. At MITRE, we interact with a range of government, university, and private sector elements in cyber security, and we witnessed a range of response to these intrusions—the slower the reaction the more dire the consequence. And we saw the advantages of candid sharing of threat data when it takes place between people within trusted communities who share quickly, using raw information, not finished analysis.

We have also developed and now practice successful cyber threat sharing among trusted partners, using a structured format to describe and transmit the threat indicators. One example is our sharing in a regional, cross-sector coalition in the Boston area. MITRE also supports teams that conduct *brutally honest but discreet assessments* of U.S. and foreign government cyber security practices. If you were able to attend last year's 30th Workshop, you will recall my technical description of MITRE's approach to cyber security and resiliency, and how we build and sustain threat information exchanges.

"MITRE conducts brutally honest but discreet assessments of U.S. and foreign government cyber security practices."

I would like to take a moment to briefly describe the fundamentals and the role of MITRE, because the nature of our company is unique, and may not be familiar to you. MITRE was founded 56 years ago by the government to address problems of considerable complexity, analyze technical questions with a high degree of objectivity, and provide innovative and cost-effective solutions to government problems. We tackle tough problems that are integral to the mission and operation of the sponsoring agency, and figuratively we sit on the government side of the table with access to sensitive and proprietary Government information.

In a sense we are in the layer of surface tension (*meniscus*) between government needs and requirements and potential solutions and contracts, because we offer objective analysis of alternatives and support source selection decisions.

- We are not-for-profit and do not compete with nor work for industry;
- We do not build products or provide commercial services, and we transfer our technology and prototypes to the private sector;
- This work environment allows Federally Funded Research and Development Centers (FFRDCs) to work objectively in the public interest to support their government sponsors across a full spectrum of planning and concept development, research and development, and acquisition support;
- We operate several centers, including a large center for the Department of Defense, as well as centers for the Federal Aviation Administration and the Department of Homeland Security. And let me add that several weeks ago, we were awarded a new effort: The *National Cybersecurity Center of Excellence* (NCCoE) by the National Institute of Standards and Technology (NIST).

With that background, let me return to the events I described earlier regarding the Heartbleed disclosure timeline, or *who knew what and when*. The uneven ability to respond to this vulnerability

[11] The Heartbleed Bug is a vulnerability in the OpenSSL open source cryptographic library that is used to provide SSL/TLS encrypted connections between web clients and servers. The Heartbleed Bug allowed attackers to read system memory revealing sensitive information including server private keys, session data and passwords. Shellshock is a vulnerability in the Unix Bash Shell allowing attackers to attain root-level access to servers. These vulnerabilities share two common characteristics: First, the applications that contain them are both open-sourced, easing the burden of analysis to source code rather than reversed engineered binaries; second, the installation base for each of these applications is vast and central to the operational capability of each system. As cyber defenders, we often delude ourselves into a false sense of security by assuming that the longer source code publicly exists, the lower the probability of there being a bug, especially a catastrophic bug, in that source code. We then fail to discern the relative risk we are assuming between less frequently used services that are only accessible to whitelisted clients on internal interfaces and services that use libraries such as OpenSSL and are essential to information processing activities.

makes us more strident in stating the need for objective assessments of security posture, and the need for an ability to share and act on threat information. Among our concerns at MITRE is the shortening time span between identifying spurious potential malware indicators and the need to share, analyze, and act.

We are concerned by the "shortening time span between identifying spurious potential malware indicators and the need to share, analyze, and act."

Reiterating the point I made at the beginning, an important aspect of cyber competency is being immersed in the skills and tactics of experienced cyber security operators. *Sharing information on successful Cybersecurity Operation Center*[12] *practices* is helpful in building trust and solidarity and will help our less capable partners do their homework and benefit from the more capable Alliance partners.

Also, to address the white space between political decision-making and time-critical technical sharing, we recommend the fielding of *workshops and table-top exercises on rapid cyber threat sharing and analysis* across the spectrum of cyber operations, with a focus on shared analysis and decision-making. But as I described last year, our successful experience in cyber threat sharing is not hub and spoke. It is mutual collaboration among peers for crowd-sourcing information and analysis. In support of NATO's cyber future, we recommend that solidarity be bolstered by NATO-wide cyber threat sharing among the partners' Cyber Security Operations Centers.

"We recommend that solidarity be bolstered by NATO-wide cyber threat sharing among the partners' Cyber Security Operations Centers."

Last, as national and political leaders become more involved in the cyber domain and decision making, they will need access to a curated set of information from across the cyber spectrum for a common understanding—something we call *shared situational awareness or a common picture (live cartography)*. We recommend establishing a mechanism for keeping senior leaders informed with shared awareness of the cyber domain, such that their cyber awareness remains current. Through shared situational awareness and common understanding, we build solidarity.

[12] Carson Zimmerman, "Ten Strategies of a World-Class Cybersecurity Operations Center," 2014, The MITRE Corporation.

How to Investigate When the Terrorist Abroad Is One of Our Citizens—Psychological Operations and Virtual Human Intelligence over the Internet

Mr. Marco Braccioli
Senior Vice President, Area SpA

To give you an overview of our projects in Italy, I would like to describe a typical cyber project that we have under way at several companies around a Dual Information Support Operation (DISO) Command and Control. In our cyber command structure, there are several bricks:

- The real-time operation, that is cyber—CERT;
- The non-real-time operation;
- The analysis of the electro-magnetic spectrum and radio spectrum, and the non-real-time operation in which there is all the mining, the Intelligence, the support and system analysis, and of course, all the semantics, all the instruments, the HUMINT, the geolocation IP, and many other components.

There is also an additional brick, which is an academy that we are developing in order to support the level of proficiency required.

At this point, I would like to go straight to the title of my presentation: How can you investigate when the terrorist abroad is one of our citizens? Across Europe—and in many other regions as well, there is a grave danger of citizens joining ISIS. While the potential risk in Europe is very high and truly worrisome, there are thousands who are joining ISIS from various parts of Africa, as well as from Jordan, from Saudi Arabia, Morocco, Egypt, and even from Turkey (there have been 500 people joining from Turkey according to one of our sources). To this long list of countries whose citizens are joining ISIS, it is unfortunately necessary to add Australia, Kosovo, Albania, Bosnia, Macedonia, Russia (about 500 people), and various Caucasian countries. It is clear that the calls of Caliph Ibrahim are starting to resonate with many of our young people.

"Across Europe, there is a grave danger of citizens joining ISIS."

In order to illustrate the severity of this situation, I would like to mention a few actual cases that we have had in Italy: A young man by the name of Giuliano from the northeast of Italy was enrolled in ISIS. Yet, he was not recruited in a mosque, but in the gym at his prison. Thus, you can see that ISIS recruiters are not just exploiting religion, they are taking advantage of social anger. The second or third generation of Muslims that are populating our countries are feeling angry. So, at this particular moment in the economic crisis that we are all experiencing in Europe, we have no answer to give to these young people who are looking for a focus in their lives.

"ISIS recruiters are not just exploiting religion, they are taking advantage of social anger."

I would also like to tell you a story about a French man, Ahmed, who did not grow up as a Muslim. He learned the Koran on the Internet, and he joined Islamist groups through the Internet. Young people, such as these two from Italy and France, act like catalysts in the Arab world, because they are often well educated with a significant degree of culture. In short, we are in real trouble.

ISIS is far from the only concern, however. Our company, Area, has been working for a long time against a very large and powerful enemy, the mafia, and we support our authorities from the National anti-mafia Directorate. Working against the mafia is like working against an army because

they have money. Like the mafia, many criminals and illegal organizations work in the dark web—not just the deep web (which is the large portion of the Internet that is not accessible by ordinary search engines) but the dark web (which can only be searched by a special browser like Tor that permits anonymity). In the dark web, it is not easy to be admitted—you have to meet certain conditions of credibility in order to be accepted. This is the reason that, for particular crimes like pedo-pornography, we developed ways to create a "fish" that can help us look for "fishermen." In general, we join communities with certain identities, with certain machines that we have created.

"Working against the mafia is like working against an army because they have money."

Of course, just as we seek to profile a target, our targets will be profiling us as investigators. So, the best approach for us is to have a computer or a smartphone that is completely clean. This is because, if there is any way for the "fishermen" to become suspicious about who we really are, they may escape from the "fish." This makes it possible to join a criminal group without having to crack the technology. When this group of criminals is moving, for example, to using telegrams, we just have to open an account. This kind of situation is typical for all crimes that are found in the dark web.

"In investigating the dark web, the best approach is to have a computer or a smartphone that is completely clean."

At my presentation last year, I mentioned Silk Road, which is now closed. As we all know from the media coverage surrounding the closure of Silk Road, the crimes that are dealt with in the dark web are:

- Terrorism,
- Theft of data,
- Bounty hunting,
- Human experiments,
- Extreme sex which is obviously illegal,
- Homicide for payment, and
- Trafficking of every kind—drugs, weapons, anything.

"In the Marianas web, you will find state-sponsored groups that attack governments."

But inside the dark web, there is the deepest level of the Internet—the so-called Marianas web (Multiple systems Analysis and Recording Intelligence and National Alarm). In this part of the web, you will find state-sponsored groups that attack governments. It is absolutely a reality, believe me. In the Marianas web, you can buy hours of attack against any site, against any institution in the world. You can hire vast numbers of computers in less than an hour. Obviously, state-sponsored groups are acting under conditions similar to those of the privateers of Queen Elizabeth I. If you come back with the equivalent of a captured galleon, you are a hero; If you are taken by the enemy, you are fired. This is today's simple reality in the dark web.

Challenges of Cyber Security—
Cooperation between Government and Industry

Ing. Général Robert Ranquet
Deputy Director, Institute for Higher Defense Studies (IHEDN)

With two speakers from government and two from industry, we are exploring how government and industry can best cooperate in developing doctrines to deal with the cyber threat. We begin with a French official perspective: Ms. Isabelle Valentini, whose presentation follows, is the number two official at the French Cyber Command and the head of cyber policy. According to my understanding, the Cyber Command in France is as much about policy as about doctrine and operations—and it is a very effective organization, too. In her presentation, Ms. Valentini discusses the "Livres Blancs" (White Papers) that have given cyber defence a national priority, as well as the current French cyber defense doctrines, and how the defense ministry is organized to counter governmental (or other) potential attacks in order to protect armament systems. As she mentions, international cooperation is of vital importance in cyber security. Moreover, there is a need to create a broad cyber defense community, including universities, R&D organizations, and young researchers.

According to General Davis, "The balance between opportunity and risk is shifting because of growing threats."

From the U.S., Major General John Allan Davis—the Deputy Assistant Secretary of Defense for Cyber Policy, offers his own views. For our purposes, it is most convenient that his organization is, in fact, quite similar to Isabelle Valentini's (although I suppose that the U.S. has much, much more money). He offers a strategic overview of the main drivers that shape U.S. policy, including norms, and partnership efforts. In particular, he stresses the importance of a broad team, which is exactly the theme of our panel. He also argues that the balance between opportunity and risk is shifting because of growing threats; and he emphasizes the need for greater transparency in the use of uniformed military cyber forces and capabilities.

Offering an industry view point, Mr. Maurice Cashman is Director at a rather larger cyber security company, namely McAfee-Intel. He shows how industry and the private sector can play a role in developing the needed policies and doctrines (even involving private citizens in the process of developing security). The key is achieving the right balance between resiliency, personal privacy, and national security. National security, economic growth, personal privacy and mission assurance are now mutually dependent on resilient digital services and trusted data. This disruptive technology combined with an expansion of threat sophistication and motivation has created an inversion of power, which is forcing a new approach to security and collaboration.

And the final presentation is by Mr. Anton Shingarev of Kaspersky Labs, who discusses the importance of critical Infrastructure protection. One danger is due to the reality of a cyber underworld that is not only populated by independent amateur crooks, but, increasingly, by disciplined groups of cyber professionals. Worse, the latter can play into the hands of the traditional mafia, but—more alarmingly—they can be exploited by nation states. In fact, some of the most significant cyber attacks have caused real damage to critical infrastructure—which is only one short step away from full-fledged cyber warfare between nation states.

"Cyber criminals can be exploited by nations states to attack critical infrastructure."

Addressing the Cyber Threat—
The French Defense Ministry's Approach

Ms. Isabelle Valentini
Deputy to the General Officer Cyber Defence; Head of Cyber Policy, French Joint Defence Staff

Since we have just spoken about cyber war (and cyber guerilla warfare), it may be useful to present the cyber defense organization of the French Defense Ministry and the Joint Staff, our doctrine, operational aspects, as well as our offensive and defensive capabilities. First, I would like to describe our structure. The French national cyber defense organization must protect the Ministry networks, the armed forces (both during operations and in France), weapons and armament systems, as well the defense industry and critical infrastructure.

Our National Cyber Defense Doctrine: Four Main Documents

France wants to participate in the overall cyber defense framework and we are working on the establishment of a national doctrine. I would like to mention the four main documents that are the basis for our current national defense strategy:

"Cyber defense is now recognized as a priority and national doctrine has been published."

- The first document is the White Paper on Defense and National Security published in 2013. According to this White Paper, cyber defense is now recognized as a priority. A national doctrine has been published, giving an orientation to the strategic private sector in order to provide "best practices" for cyber security.
- The second document is the Military Programming Act for the period of 2014-2019. It offers a general framework for developing the Ministry of Defense (MOD) cyber capabilities and to provide resources. A one billion euro plan has been approved by the French Parliament.
- The third is the Defense Pact on Cyber Defense, approved by Defense Minister Jean-Yves Le Drian in February 2014. This plan, which is based on six points, is to:

    1. Strengthen cyber security,
    2. Prepare for the future through research and development,
    3. Promote innovative small and medium-sized companies,
    4. Develop human resources,
    5. Create a cyber defense center of excellence, which is located in Brittany,
    6. Cultivate a network of partnerships with NATO and the EU, the center of NATO excellence in Tallinn, develop bilateral relationships, and foster a national cyber defense community based on universities and a cyber citizen reserve.

- The last document is the MOD Cyber Defense Concept and Doctrine, with the objective of reinforcing the role of armed forces in cyber space, creating a centralized and unified chain of command (which is new in France), and updating the regulations concerning the protection of critical infrastructure against cyber threats. Within the Ministry of Defense, Vice Admiral Coustillière (who is my boss) has been given the responsibility for cyber defense under the authority of the Chief of Staff.

We consider that cyber space is a new area of confrontation—which may involve cyber war, guerilla cyber war assisted by states, terrorist groups, or hackers. But we must now deal with this new challenge, because we consider that a cyber attack can represent the same challenge as an aggression by another state against our national territory.

The French National Doctrine for Response to a Cyber Attack

The French national doctrine to respond to a major cyber attack is based on a global approach centered around two complementary aspects:

- First, the implementation of a strong and resilient posture for the information systems of the State, or operators of vital importance, and strategic industry. This aspect is handled by the National Agency for Information and Network Security (ANSSI), which is under the authority of the Prime Minister. This implementation is coupled with an operational organization within the Ministry of Defense.
- Second, a global governmental capacity to provide an appropriate answer to any attack. The first step would involve diplomatic, legal, and policy means. But if necessary—and we can sometimes see such situations in Iraq or Daesh, military means will be appropriate. The gradual use of military means by the Ministry of Defense will depend on the nature of the cyber threats.

As to the cyber military organization, we must acquire and maintain operational superiority. Our capabilities will be conducted within five domains: land, air, sea, outer space, and of course cyber space.

In France, the cyber defense organization must be closely integrated within the armed forces, including defensive and offensive capabilities, in order to prepare or support a military operation.

The operational organization of the cyber forces is integrated into an operational chain of command for cyber defense led by Vice Admiral Coustillière under the authority of the Chief of Staff. When French troops are in Mali, the Central African Republic, or Iraq, there is a cyber defense component. We have to develop both the defensive and the offensive aspects.

"The attribution of an attack depends not only on the direct evidence, but also on intelligence, politics, strategy, economics, and geopolitical context."

As to offense, we need to protect the systems of our armed forces. Given the importance of the cyber threats, we need to develop Intelligence activities and create the corresponding technical capabilities. Of course, we have to identify the origin of the attacks in order to estimate the offensive capabilities of the potential opponent. The attribution of an attack depends not only on the direct evidence, but also on Intelligence, politics, strategy, economics, and the geopolitical context.

According to the national doctrine, the cyber defense offensive capability in conjunction with an Intelligence capability contributes significantly to our cyber security.

In conclusion, I would just like to say that, a month ago, France organized a national cyber defense exercise that included the private sector (with a few small and medium-sized enterprises). The scenario was a major attack against the infrastructures in order to test the chain of command and its capacity to react. It seems to us that the exercise was rather successful.

Major General John Allan Davis, U.S. Dep. Assist. Secretary of Defense for Cyber Policy; Ms. Isabelle Valentini, Head of Cyber Policy, French Joint Defence Staff (left to right).

Strategic Overview of the Major Drivers of National and International Policies, Norms, and Collective Partnership Efforts

Major General John Allan Davis
Deputy Assistant Secretary for Cyber Policy, U.S. Department of Defense

It is my great honor to represent the Department of Defense among the many distinguished participants in the workshop here. My first goal today is to share with you my personal experience working in the cyber policy arena on some of the main drivers of DoD policy.

It has been a fascinating couple of days and I have really enjoyed listening to the panels and talking with many of you. When you get to the end of a workshop, you wonder what there is to say that is new, so you may not be surprised that the things I am going to talk about will reinforce what has already been said. I will focus on three main drivers that I see shaping DoD policy and other policies as well in forming strategies and doctrine for the militaries. They are also shaping the developmental priorities and the associated resources for the development of cyber forces, capabilities and processes.

Teamwork and Effective Partnerships

"No single organization has all the skills, talent, resources, capabilities, capacity or authorities to act effectively."

As you have heard many times during this workshop, the first major driver is the need for teamwork and effective partnerships. Many different organizations, both public and private, have critical roles and responsibilities in the cyber security environment but, based on my experience, no single organization has all the skills, talent, resources, capabilities, capacity or authority to act effectively in isolation. It truly does take a team approach and strong partnerships to operate effectively in the cyber environment. In DoD, we look at four different levels of teaming:

- The first one is internal. If you want to be an effective member of the team and not sit on the bench, you have to build capabilities internal to your own organization.
- The second aspect is inter-agency. The U.S. approach, and many other nations are following suit, is about a whole of government effort that is required to be effective in this type of environment. We have a policy of a whole of government effort in terms of coordination; we have a policy of restraint; and we have a policy of significant oversight: policy oversight, operational oversight, legal oversight, and we even have congressional oversight over the things that we do in DoD. That does shape the way we organize training and equip forces and it shapes the way that we impose policy limits on those forces and capabilities.
- The third aspect is industry. In DoD, we rely on many aspects of the information technology environment that we do not directly control in order to do our mission. Therefore, this requires effective partnerships with industry, critical infrastructure standards, and information sharing. We have taken a voluntary approach to that because to really do effective comprehensive information sharing and standards will require legislation. We have not yet solved that problem in the United States but we are doing what we can in the meantime about developing those information sharing and standards partnerships.

"We rely on effective partnerships with industry, and that requires critical infrastructure standards and information sharing."

- The fourth level is international. Doing cyber effectively requires international partnerships and working together. We have a concerted effort in DoD to begin building those partnerships with many of you in Europe, in the Gulf region, and in the Asia-Pacific region. Once again, the reason is that, in order to fulfill our defense alliance relationships and obligations, we must rely on critical infrastructure that we do not directly control. In order to understand what is happening in that

environment so that it can be secure and can support DoD's mission, we have to establish these kinds of relationships. And when we, DoD, come to the table with our MoD partners, we encourage a whole of government type approach because we are sharing our lessons and this must be across the government. So partnerships are important and they are driving the way that we do things in DoD.

"We rely on critical infrastructure that we do not directly control."

The Changing Balance between Opportunity and Risk

The second major driver is the changing balance between opportunity and risk. Our growing reliance, and if you listen to some of our earlier speakers, our exploding reliance on information technology stands in stark contrast to the inadequacy of the security of that environment. Technology is driven by opportunity and the security angle is always chasing behind trying to catch up. I think that balance is changing. It is changing slowly, and it is changing unevenly but I do believe it is changing. What is important in the balance? Well, you heard many of my colleagues talk about the need for an open, secure, and reliable internet; the need for establishing norms of responsible behavior; the need to protect freedom of expression, personal privacy and civil liberties; the need to drive economic development. Those are important aspects but, on the other side, the threat is growing and it is not just criminal activity, it is not just espionage, it has now moved into the realm of disruptive activities and even destruction. Let's face it: We make it pretty easy. We put our intellectual property in ways that are inadequately defended, we are not careful about who we let in the front door. In my experience, 80% of the problem could be addressed with some very basic standards and discipline. That leaves 20% that is going to be sophisticated that you are going to have to deal with but, if you can get 80% of the noise out of the way, you can focus what limited resources and capabilities you have on the really tough problems. We need to do that and I think we are, but we are not moving fast enough.

"80% of the problem could be addressed with some very basic standards and discipline."

What is at stake in getting that balance right? From my perspective, the U.S. and global critical infrastructures and key resources are at stake. National security and economic security interests are at stake and so are our public health and welfare interests. As a high priority, we have to get that balance right, not only for the Department of Defense but for others as well.

Clarity and Transparency

The last major driver is the need for clarity and transparency. This is greatly needed. Historically, most of the significant capabilities in the cyber arena grew up in the underground. They grew up in darkness and anonymity, political activism, criminal activity, espionage. Now you are seeing more and more countries that are building military forces and capabilities and when you talk about the use of uniformed military forces and capabilities in this arena, we need to shine a little bit more light on what we are doing and why we are doing it.

Why is that important? It is important to reduce uncertainty and the chances of making a mistake. It is important to increase stability and to control escalation. We know that we have to clearly explain what we are doing as a U.S. military, why we are doing it, and how we are exercising very careful, deliberate control over what we are doing as a responsible nation. Clarity and transparency are important, but once again, there is a need for balance. Obviously, when you are in the business of the military, you do not want to give away an advantage, but we need to talk more openly about what we do, and this is why the U.S. Defense Department is doing so. Also, one benefit in being clear and transparent is that you can use military capabilities more effectively in a deterrent role, and I think we are just beginning to tackle that issue within DoD.

"One benefit in being clear and transparent is that you can use military capabilities more effectively in a deterrent role."

So, just as my colleague from France described the French organizational structure, it is no surprise that DoD has been quite open about describing the forces that we are building and why we are building them. We are building forces to protect and defend our own networks, as well as combatant commands and their contingency plans and contingency operations—just like we support them with land, air, sea and space capabilities. And we are building forces to defend the nation in cyberspace from significant threats. This is not DoD protecting against the criminal threats. This is DoD being prepared to take action should we see something that is going to cause loss of life, or significant national security concern, or cause our economy to collapse, or prevent the military from being able to do its job. Those are the kinds of things for which we are building military forces. We think it is important to be open and transparent about that, and we are setting the example as a responsible nation and we expect others to follow.

Resilience, Personal Privacy, and National Security: How to Achieve The Right Balance

Mr. Maurice Cashman
Director, Enterprise Architects EMEA, McAfee, a part of Intel Security

The Rapid Emergence of New Disruptive Technologies

The role of collective cyber security has never been more important—to the nation, to business enterprise, and to everyone of us. The rapid emergence of new disruptive technologies in the social media, wearable computing, the cloud and big data analytics has opened incredible new doors for business innovation, enriched personal experience, and efficient government. Nonetheless, they have also increased our interdependence on the resilience of and cooperation between each stakeholder.

Over the past few years, we have seen the convergence of the cyber-physical domains throughout our critical infrastructure. And there is much more awareness now as to the importance of cyber security, certainly within the energy sectors if not others. We can thank several organizations, especially the National Institute of Standards and Technology (NIST), the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the European Union Agency for Network and Security (ENISA), among many others for raising that awareness and the standards of security in critical industries. Yet, the newer technologies—the so-called third platform—are creating an even deeper convergence of the cyber, physical, and personal domains. They have created new attack surfaces for a persistent threat that has increasing sophistication and motivation. They are also magnifying the speed at which cyber incidents can have an impact on personal privacy, business continuity, trusted government services and mission assurance.

"Newer technologies have created new attack surfaces for a persistent threat that is increasingly sophisticated."

A New Approach to Security and Collaboration

Industry is a key stakeholder and at the heart of solving this problem. Sometimes it seems that we keep relearning the same lessons, however. Each new technology or business domain comes with risks, but security always lags in priority. The "time to value" is always more important than the "time to protect." Take big data for example. As noted in a recent Gartner study, over 63% of businesses are investing or planning a big data project. Big Data is at the center of the privacy debate around social media and Intelligence Collection, and is a key technology for new business growth. Yet security of the platforms that house that data is rarely if ever the top priority, in fact it ranks 6th on average. Recently, I attended a conference of business leaders where the emphasis was on obtaining value, but not on risk mitigation. With threats happening at unprecedented frequency and speed, we cannot continue to take the same approach to security.

With big data, "security of the platforms is rarely if ever the top priority."

For these reasons, I would like to provide some observations as to where we need to change our approach and, at the same time, highlight where government-industry collaboration is working from my point of view.

For the security industry, there are two imperatives:

- First, we must build security capability into the devices. For example, embedded sensors throughout a power plant cannot be easily changed once they are deployed nor can a security patch be applied easily. We need to make these devices more secure through hardware and more manageable out of the box by traditional security platforms. Intel is in a unique position to address this problem and has worked with manufacturing companies to embed security capability in their products and deliver new security enhancements through hardware.
- In addition to embedded security, we should ensure that future technology solutions support open standards that allow for interoperability, particularly to share data or Intelligence more effectively. MITRE has done excellent work with standards such as STIX and CVE, which enable information sharing and assessment with automation. These are the types of standards we need to enable situational awareness of incidents in the public or private domains.

"MITRE's STIX and CVE enable information sharing and assessment with automation."

For the business enterprise, there are three imperatives:

- One, we must do a better job of balancing the controls. Too many organizations still focus only on preventative controls. Yet, developing anticipation and response capability through better data analytics, centralized security operations, and Intelligence Integration is essential in order to build resilience against targeted threats.
- Second, assessing readiness in a realistic manner is important in order to identify gaps in security technology and process. We can use the example of CBEST from the U.K. government and Bank of England. CBEST is a 'red team" style penetration test and certification process for financial institutions. The tests emulate real attacker methods and provide a realistic assessment of resilience against targeted threats.
- Third, we need to pay attention to the supply chain—this means not just the traditional business or hardware supply chain. It now includes external cloud service providers. Standards from the Cloud Security Alliance are a good place to start, but it is only a guide. Enterprises are still responsible for their data security as they are ultimately at risk.

"Too many organizations still focus only on preventative controls."

In closing, we must all strive to create a positive security culture with user involvement in the process, more transparency on security controls and "reverse mentoring" for leaders so that they can better understand how technology is being used at all levels.

Critical Infrastructure Protection as a Serious Challenge for Global Security

Mr. Anton Shingarev
Head of the CEO Office and Director of Global Government Relations, Kaspersky Lab

The Importance of Critical Infrastructure Protection

Today, we have discussed both national and international approaches to cybersecurity. My speech will be devoted to the importance of adequate protection of critical infrastructure. Usually, critical infrastructure protection—or CIP—attracts attention when major incidents involving malware become known. Stuxnet revealed how damaging attacks on industrial facility can be. Industry was also a target for malware such as Wiper and Shamoon, which caused millions of dollars in losses. Governments are already actively involved in the development of cyber weapons, and this needs to be addressed. While critical infrastructure is viewed as target number one in case of cyberwar, there are no fully reliable methods to protect it.

"Critical infrastructure is viewed as target number one in case of cyberwar."

At the same time, this issue is becoming widespread, which is cause for worry. Kaspersky Lab's recent survey of 3900 IT professionals worldwide found that 31% of businesses in the manufacturing sector believe that they are being specifically targeted by cyberattacks. Unlike *corporate* IT security, which is focused on data protection, *industrial* IT security focuses on process protection[13].

Government and Private Efforts to Establish Secure Standards

It cannot be said that Industrial Control Systems/Supervisory Control and Data Acquisition (ICS/SCADA) systems and other critical infrastructure are not in the focus of the public and private sectors at present. The U.S. National Institute of Standards and Technology presented its "Framework for Improving Critical Infrastructure Cybersecurity" this year. European Union institutions are working on adopting a directive on network and information security designed to create a minimum level of national cybersecurity capacities, ensure cooperation among the competent national authorities, and establish procedures for risk management. However, this kind of regulation is usually a trade-off between a raise in the level of protection and an unwillingness to over-regulate the industry; consequently, it is of a "framework" nature.

"Regulation is a trade-off between a raise in the level of protection and an unwillingness to over-regulate the industry."

The private sector is willing to contribute to establishing more secure standards for critical infrastructure and proposing its solutions to mitigate the risks. But the problem lies in the fact that, for the secure operation of industrial/infrastructural installations, it is vitally important for an engineer to be able to obtain reliable information from the operation/process management system. Based on that information, he will be able to control the operational processes. This avoids making mistakes in controlling the processes, and helps—where necessary—to shut them down in time and avert disaster[14].

[13] Kaspersky Lab Survey Discovers What Types of Data-Loss Keep Industrial IT Managers Awake at Night - http://www.kaspersky.com/about/news/virus/2014/What-Types-of-Data-Loss-Keep-Industrial-IT-Managers-Awake-at-Night // Virus News, 24 Sep 2014

[14] Securing Critical Information Infrastructure: Trusted Computing Base - http://securelist.com/analysis/36594/securing-critical-information-infrastructure-trusted-computing-base/ // Securelist.com, 16 Oct 2012

At Kaspersky Lab, we believe that no existing operating systems or software could be applied in industrial/infrastructural environments whose produced data on processes could be fully trusted[15]. This is why we are working on the development of a fully secure and trustworthy operating system for critical infrastructure: A solution that we believe will be a game-changer in the field of CIP. We think that there is room for joint efforts on the part of the cybersecurity industry and governments, including the following:

"No existing operating systems or software for industrial processes can be fully trusted."

- Further specification of standards and technological requirements for critical infrastructure management systems;
- Replacement of old conventional technologies with technologies that are tailored to critical infrastructure; and
- Other public-private partnership initiatives.

Joint initiatives like these can ultimately make the functioning of critical infrastructure safer and more secure.

Mr. Evgeny Grigorenko (left), Senior Public Affairs Manager, CEO Office, Kaspersky Lab; Mr. Anton Shingarev (right), Head of CEO Office and Director of Global Government Relations, Kaspersky Lab.

[15] *Ibid.*

Looking Beyond the Horizons

Dr. Gerlinde Niehus
Head, Engagements Section, Public Diplomacy Division, NATO

Since this is the workshop's final panel, our object is quite appropriately to "look beyond the horizons" by presenting and discussing a broad range of views. Using some of the analogies introduced during the previous chapters, this might be called a "decentralized" panel—or perhaps even a "deep panel." And, of course, we must face the usual challenge that often arises at conferences at this stage: Everything has been said, albeit not yet by everybody, and the audience gets the distinct feeling of déjà vu and déjà lu. However, we have brought together four "decentralized" panelists who will discuss some of the major trends that are likely to shape the future strategic context as well as their potential major implications for the global security landscape. In "looking beyond the horizons," we may take inspiration from Mark Twain who once coined the phrase, "Plan for the future because this is where you are going to spend the rest of your life."

It is in that spirit that I would like to introduce my panel members: Since 2010, Ambassador João Mira Gomes has been the Portuguese Ambassador at NATO after a significant diplomatic career extended from being the coordinator for the Western Balkans to Deputy Head of Mission for Portugal in Paris. Mr. Ernest Herold, currently Deputy Assistant Secretary General for Defense Investment at NATO, has served at the U.S. Joint Command in Stuttgart in addition to his more recent industry experience at IBM. Mr. Jean-Pierre Maulny is the Deputy Director at the prestigious IRIS institute in Paris, where he is in charge of strategic policy as well as European and transatlantic defense issues. Finally, I would like to introduce Roya Mohadjer of Lockheed Martin, where she is responsible for the development and execution of their STEM/STEAM strategies, which involves partnering with global influences across academia, industry and government.

Since we will be exploring strategic foresights, I would like to suggest four major trends: First, there are the political themes—which range from the ongoing shifts in global power and evolving political structures to advances of the polycentric world. Second, there are economic themes characterized, for example, by the diffusion of economic power, the increasing number of knowledge intensive economies, or the increasing competition for resources. As a case in point, there are the vital issues of food, water, and energy (which was discussed earlier in this workshop). Thirdly, there is the human theme characterized, for example, by changing demographics, growing urbanization, and increases in inequalities or in migration (which are closely linked to increases in religious extremism). Last, but not least are the technological themes, which are characterized, entre autres, by accelerated change through technology, with the multiple implications of the information society. These are just the major trends to set the scene for our discussion.

"Is a 'rule of power' now emerging, if not a 'rule of violence,' that is beginning to overshadow the 'rule of law'?

The next presentation is by Portugal's Ambassador Mira Gomes. Hopefully, he will help us understand whether the *pax americana* is coming under pressure, or whether we are beginning to see the effects of an imperfect (and messy) *pax sinica.* Is a "rule of power" now emerging—if not a "rule of violence" that is beginning to overshadow the "rule of law" as we are seeing in Russia and Ukraine? If so, what can or what should the international community do?

The Changing Nature of Threats to Global Security: How to Approach the New Challenges"

Ambassador João Mira Gomes
Portuguese Permanent Representative to NATO

Changing threats and new challenges are a challenging subject because finding the answer is what keeps us busy in NATO and in other international organizations. Without pretending to have definitive answers, I would like to share some thoughts with you. My point of departure is that the world has never been so prosperous, so advanced, and so connected; but, at the same time, the world is becoming more and more dangerous and we have had many examples of this in the past twelve months. So, I will ask three questions:

- Why is it that a more developed world does not lead to a more secure world?
- Where are we failing, i.e., failing to cope with the challenges and threats?
- How can we approach the current challenges?

"Why is it that a more developed world does not lead to a more secure world?

Living in a More Developed World but with Less Security

A more developed world does not necessarily imply a more secure world. Why? Firstly, because the kind of challenges that we are facing are not really new but are becoming more complex. We are witnessing new forms of terrorism, more immigration, more demographic pressure, more growing economic imbalances, more serious and more frequent epidemics, a wider gap between rich and poor and also a wider gap between developed and less developed countries.

"Terrorists are becoming more sophisticated and take advantage of the openness and freedom of our societies."

Secondly, challenges are more asymmetric and do require a more elaborated and coordinated approach. To fight back terrorism like the kind we are facing with ISIS, we need to combine political, military, security, economic, social and cultural strategies. Terrorists are becoming more and more sophisticated and take advantage of the openness and freedom of our societies to challenge not only our political ideologies but the very same values upon which we have founded our societies. Since international terrorism is global, our approach needs to be global as well.

Where Are We Failing?

If we want a simple answer to why we are failing, it would be in the failure of the international system to cope with those more complex and asymmetric challenges. First and foremost, I think that there is a failure from the United Nations and the United Nations system, mainly the United Nations Security Council, because after all the Security Council is the first responsible for peace and security in the world. But there are also some examples in Europe where we are failing. If we look at the OSCE, there is currently a big challenge to the European security architecture due to the number of existing frozen conflicts or the number of conflicts that were not prevented by the OSCE. There is also less transparency and less predictability in European relations. The European Union as such needs to be more ambitious and play a greater role as a global player by strengthening its Common Foreign and Security Policy and its Common Security and Defense Policy. And even NATO has a challenge, which is to turn the page after a decade of engagement in Afghanistan and deal with the new challenges stemming from the recent developments in Eastern Europe; but it must also find a kind of balance between its three core tasks—collective defense, crisis management, and cooperative

security—in all its areas of responsibility. So NATO also needs to have a more comprehensive approach to security and to the other challenges that we are facing right now.

The security and well-being of our populations depend on our success in dealing with climate change, refugees, public health in less developed countries, and promotion of the rights of women and children. But special attention should be given to the close relationship between international terrorism and organized crime, which is responsible for human trafficking, drugs trafficking, proliferation of weapons of mass destruction, and to the relationship between these several entities. Let us not forget a kind of new phenomenon that is also a huge new challenge: It is how to deal with foreign fighters who come from within our own societies.

There is a "new challenge: Dealing with foreign fighters who come from within our own societies."

How Do We Deal with These Challenges?

No single country or organization has the answer and no single country or organization can deal with the existing challenges on its own. We all know this, but are we all making enough efforts? I think the point of departure should be our engagement to preserve international law and international norms. All solutions that are "ad hoc" are less good than solutions that are taken within institutional frameworks.

"Now that the G8 is dead, will the G20 be enough to give representation to emerging countries and regions."

In this respect, we should offer a better representation on the international scene to emerging countries and regions. Now that the G8 is dead, we can ask ourselves whether the G20 is enough in order to give representation to those countries and regions. And this leads me to the need in my mind to reform the United Nations Security Council because we cannot continue to give twentieth century answers to twenty-first century challenges. I think we have to listen more to regions and help regions to organize themselves better. In the Asia-Pacific region, there is a deficit of regional multilateral mechanisms to diffuse tensions.

Ambassador João Mira Gomes, Portuguese Permanent Representative to NATO.

More than permanent heavy structures, we should invest in permanent light but efficient mechanisms. A good example of this kind of regional cooperation is the 5+5 Initiative, which is an informal forum of dialogue between countries of the northern and southern shores of the west Mediterranean—on the northern shore, Portugal, Spain, Italy, France and Malta and on the southern shore, Mauritania, Morocco, Algeria, Tunisia, and Libya. It serves as a kind of laboratory of ideas to deal with regional problems through a comprehensive approach. As a consequence of its flexible and informal character, it has become progressively more open and has gradually expanded to spheres that go beyond political commitment such as defense, home affairs, migration, inter-parliamentary dimension, tourism and transport. This is a good example that could be adopted by other regions because I think we need to develop a kind of a new paradigm of dialogue between regions. If we manage to encourage more dialogue between regions and more dialogue involving regional organizations, I think we will strengthen the ownership, we will strengthen and likely even enlarge platforms where countries already cooperate. We will probably be promoting a kind of peer review

mechanism inside each organization, thus giving more responsibility to countries and making dialogue easier. At the end of the day, it will also provide more predictability and a better capacity to anticipate crises.

My final reflection is that the EU is already doing a lot in its institutionalized cooperation and dialogue with other countries and regions, but I am convinced that it could do even more and act as a driving force in smoothing relations between countries with some troubled areas. The EU can use to the best extent possible its unique and vast array of diplomatic tools and should not shy away from being ready and willing to mediate when the need arises. This indeed would be a tall order for the incoming High Representative, Federica Mogherini.

Let me conclude by quoting Jean Monnet: “Better to fight around the table than on the battlefield.“

Security: The Human Factors

Mr. Jean-Pierre Maulny
Deputy Director, Institut de Relations Internationales et Stratégiques (IRIS)

Abstract: Human factors appear to be neglected as factors of security or insecurity. The 21st century is the century of the Tahrir and Maidan squares. Societies are challenged by social inequality—even inequity—and the growing gap between the rich and the poor. The imbalance is not only between the South and the North, or between the West and the Rest. It is found more and more inside our western societies. What are the likely consequences of the new trends?

I would like to offer a quick overview of the importance of human factors for global security, which are often neglected in security discussions despite their undeniable significance. There are three trends that— if brought together—can be a basis for our security in the future. And they all originate in the human factors and their involvement in foreign policy.

Social Networks Facilitate the Indiscriminate Spread of News and Ideas

The first trend is the capability for anyone to be linked with anyone else through social networks. Within these social networks, speech is almost totally free, and there is no restraint in the way that ideas and news are disseminated.

"In the future, we will see the growth of unpredictable mass movements."

Theoretically, this is a good thing, since freedom of thought is a fundamental human right. But, at the same time, the lack of restraints on the expression of new ideas by extremist political parties could constitute a risk, since they could spread non-democratic ideas or simply false news. In the future, one thing that we will certainly see is the growth of unpredictable mass movements. This will be due to the use of social networks and to a shift away from policymakers or intellectuals toward the public as new sources of political ideas.

I do not mean to say that the public has no right to make claims or spread new political ideas. I am only concerned that, without some limitations on social networks, there is a risk of non-rational ideas or even dangerous ones spreading across society.

"Our students have to learn how to discriminate between sources of news on the web."

It is partly a problem of education on how to use the web. Since I have been giving lectures in various places, I have increasingly noticed that students are saturated by news, references, and the differing analyses that they find on the web. As a result, they find it hard to rank all this information and analyses in order to discriminate between those that add value, those that add nothing, and those that are simply false. In fact, I often notice that minor blogs can have the same influence as official documents. As a result, we have to spend more and more time teaching methodologies so that our students can learn how to discriminate between sources of news on the web. But it is not an easy thing to do, since information from so many sources is freely available on the Internet.

Global Communication Is Encouraging Mass Immigration: A Security Threat to Our Societies

The second trend is also linked to this ability to communicate globally, even with areas of the world to which there was no way to communicate even ten years ago. Today, you can be anywhere in the world and still know how people live everywhere else. Ten years ago, the problem of migration—due to poverty, conflicts, or war—was limited to the regions that were the source of the poverty or conflicts. But, over the past two years, we have experienced a very high rate of immigration in the European Union. We knew that migration could be a potential challenge to our countries, but we did not really do anything about it even though we had ten years to prepare for the massive flow of

migration that is now arriving from Italy, traveling through France, and seeking to reach the UK. Now, immigration has become a real threat to our security.

"We have an obligation to give people a chance to live with dignity — if they cannot go back to their countries."

Worse, there are irresponsible policymakers who want to exploit the reactions of public opinion, and who do not hesitate to qualify these migrants as a problem (delinquency) instead of recognizing that our countries, our occidental countries, are part of the problem. We have only one obligation: To give these people a chance to live with dignity in our countries if they cannot immediately go back to the countries where they come from.

Effects on Security of the Growing Income and Wealth Disparities

The third trend combines the first two with the growing disparities in prosperity within developed countries. Thomas Piketty evoked the question of capital balance in his latest book. His analysis is correct, but the rational explanations he provides are not enough to help us understand the reality. From discussion with one of my young boys a few years ago, I understand that the transfer of Christiano Ronaldo (a famous soccer player) to the Real Madrid cost the same price as a combat aircraft like the Rafale: 96 million euros.

This raises a question: How many migrants can you host with this money? And of course this question is not limited to Christiano Ronaldo, who is truly a famous soccer player. The scale of remuneration of such athletes has been growing since the beginning of the century and especially in western countries. To continue with my example of social networks and global communications, the problem is that everybody who likes Christiano Ronaldo also knows the 96 million euro cost of his transfer. Twenty years ago, it would not have been possible for the entire world to know such things. And everyone also knows that there is no chance of having the same life as Christiano Ronaldo.

We are all shown a world filled with TVs, smartphones, beautiful cars, spectacular holidays etc.. Yet, what life is there for the under-privileged population with less education, less healthcare, too much unemployment, no money, and last—but not least—no prospect for a better future.

What Are the Consequences of These Three Trends?

"Their only hope is to go to a website that glorifies the djihad."

In France, there are about two thousand migrants in Calais with no legal status, no place to sleep, no food, and a great risk of serious incidents between migrants themselves as well as between migrants and the local population. Around nine hundred French citizens, sometimes very young, have left France to go to Syria to fight alongside Daech. They have not been recruited in the mosques by imams, but on the Internet through social networks. They live in suburbs, where the education they receive will be unable to bring them their desired social status. Often these people have no hope of ever acquiring a decent social status in their own society. Their only hope is to go to a website that glorifies the djihad: A new hope for them!

So these human factors are a challenge for us today, not for the future. It is a mistake to think that the traditional security or defense responses will resolve problems of this kind.

Connecting the Dots—Science, Technology, Engineering, Arts, & Math (STEAM) As the Foundation for a Safe Global Environment

Ms. Roya Mohadjer
STEM/STEAM Strategy Lead, Lockheed Martin Information Systems & Global Solutions

As we address the future of global security, may we also celebrate, assess, and learn from our history's heroes who have made substantial impacts toward safety and peace. Thomas Jefferson, Nelson Mandela, and Kofi Annan are three examples of heroes who shared a vision for global peace. Each is also highly educated and has the ability to visualize how their academic background could help make the world a better place. As a consortium of influencers, it is our duty to develop the next generation of heroes equipped to address the increasingly complex challenges of our global security landscape.

"Prioritizing education can reduce poverty and health challenges, enable economic growth, and foster a peaceful and safe global environment."

During my remarks, I will address the importance of academic preparedness, how technological advancements are impacting the jobs of the future, and how we can best prepare students for what lies ahead.

There exist many motivations to prioritize education across the globe. Of most significance are the reduction of poverty and health challenges, the enablement of economic growth, and of course the fostering of a peaceful and safe global environment.

The Global Partnership for Education cites that if all students in low-income countries left school with basic reading skills, 171 million people could be lifted out of poverty. If every child in the world received primary education, then in the next decade an estimated seven million cases of HIV could be avoided. Moreover, an increase in one standard deviation in student scores on international assessments of literacy and mathematics is associated with a 2% increase in annual GDP per capita *(World Bank).*

Increasing secondary schooling enrollment by 10% would reduce the risk of war by about 3%.

In the realm of peace and security, if the enrollment rate for secondary schooling is 10% higher than the current average, then the risk of war is reduced by about 3% *(Global Partnership for Education*). For every additional year that a male is educated, there will be a 20% reduction in the likelihood of him engaging in violent activity.

I share these metrics to demonstrate how critical it is that we are aware of the influence of an academically enriched environment.

With this in mind we understand that basic education is a necessity. As we look towards the future and consider technological advancements, it becomes increasingly critical to have a sizeable and strong STEM workforce of scientists, technologists, engineers, and mathematicians.

The future technology landscape will be filled with new and increasingly complex challenges on a daily, if not hourly, basis, especially in the realm of cyber. Consider for instance global financial institutions which host massive amounts of sensitive government and personal data. The ramifications of a compromised financial institution are crippling; dare we imagine the consequences of a calculated attack against the fabric of our financial institutions? This is especially relevant given the introduction of technology convergence wherein the risk of attack is multiplied through the interdependence of elements like Cloud, cyber, Big Data, and social media. Accordingly, our ability to

deal with these adverse scenarios will be measured by the ability of government, academia, and industry to not only respond to the challenges, but to predict the challenges themselves.

This will require the world to have an immense number of data scientists and cyber analysts. We will also soon begin to employ cyber fractologists and crypto-privacy engineers. Each of these professions will require the following skills: Critical thinking, creativity, data analysis, technical aptitude, visualization, statistics, and problem solving.

In order to successfully prepare the incoming and future workforce for the jobs of the future, we must consider the "how."

How do we motivate and inspire youth to take on technical fields of study? Often we hear that students find science, technology, engineering, and mathematics studies to be boring or too challenging. What is lacking is the ability for students to make the connection between their studies, the job they could have, and the positive impact they could make on the world. To answer this, I propose an increase in access to career exposure via simulation platforms and engagement by seasoned experts. I also propose that we leverage the Arts' fields to teach technical subject matter. Students retain less and are not intrigued by the practice of rote memorization. If we use the Arts disciplines as a method of application and practice, then students can more easily make a connection with the material. Furthermore, the inclusion of Arts produces professionals who are able to simultaneously think divergently and convergently, opening the doors for enhanced innovation. One example is François Jacob, a French Nobel Laureate known for his work in medicine who also exhibited visual art.

"How do we motivate and inspire youth to take on technical fields of study?"

Next, how do we build a large enough global workforce to meet our growing need for cyber professionals? As I mentioned previously, the potential for positive influence of enhanced education opportunities is vast. The number of primary school age children out-of-school in conflict-affected countries sits at 28.5 million. *(Global Partnership for Education).* We may view this statistic as an avenue for opportunity wherein the optimal solution would be to provide schooling to all youth worldwide. Albeit a significant objective, it is in fact attainable. Most recently, Germany opened their doors to Americans and all other international students to attend university for free.

"Germany has opened its doors to Americans and all other international students to attend university for free."

In closing, as I envision the future I see a world full of complex security challenges, but I also see a world full of excitement and opportunity as our once youth will be our then heroes and guide us safely to the next frontier of technological innovation.

I leave you with the following words from Winston Churchill...

"What is the use of living, if it be not to strive for noble causes and to make this muddled world a better place for those who will live in it after we are gone?"

Dr. Linton Wells II, Middlebury Institute of International Studies and National Defense University; Ms. Roya Mohadjer, STEM/STEAM Strategy Lead, Lockheed Martin Information Systems & Global Solutions (left to right).

Closing Remarks of the 31st International Workshop

Ing. Général Robert Ranquet
Deputy Director, Institute for Higher Defense Studies (IHEDN)

We have arrived at the end of the *31st International Workshop on Global Security.* If I have counted correctly, it is the fifth time that the workshop has been held in Paris, and the third time it has been held under the auspices of the Institute for Higher National Defense Studies to which I belong. So, for the third time, my institute has been hosting this seminar and we are indeed happy, proud, and honored to have welcomed all of you in Paris for the workshop. Incidentally, it is also my twelfth seminar—which is a long time—and this allows me to take a step back and make a couple of remarks based on my personal observations.

"For the third time, the workshop has been held under the auspices of the Institute for Higher National Defense Studies."

In recent years, the seminar has become a slightly smaller and more focused forum, a change that allows for more effective interaction between participants and that, I am sure, everybody appreciates. While we are still paying a lot of attention to geopolitical issues such as what is happening in Russia, Ukraine, Georgia etc., and at the United Nations Security Council, there is also growing interest in issues like cyber defense, which shows that we have definitively focused our interest. In past years, we used to talk very broadly about energy, water, resources, nuclear energy, industry, and many more issues. Today, for the final sessions of the workshop, we have focused largely on cyber, and we can actually see that cyber and geopolitical issues are closely interlinked. So, these appear to be strong new trends in our seminar.

"We have focused on cyber and geopolitical issues—which are closely interlinked."

To finish on a light tone, I have also noticed that we have made many incursions in the humanities field: We have quoted Francis Jacob, Benjamin Franklin, Marcel Pagnol, and even a Chinese novelist, which indicates that we are really inspired by the field of humanities and novels. This reminds me that France has recently been honored when a French novelist, Patrick Modiano, was awarded the Nobel Prize in literature. What is kind of funny, though, is that even our Minister of Culture—our American friends may be surprised that we have such a thing as a Minister of Culture—was unable to cite the works of our new Nobel Prize winner. That is kind of a pity, but it shows that here, by quoting all these novelists, we are collectively a very learned and much more literate group. I find this to be an encouraging first step, at least, towards wisdom.

I wish you all a safe trip back to your countries.

Ing. Général Robert Ranquet
Deputy Director, Institute for Higher Defense Studies (IHEDN)

Participant List

His Excellency Irakli Alasania
Minister of Defense of Georgia

Mr. Stéphane Aouichia
Regional Sales Manager, Southwest Europe, Tenable Network Security

Mr. Christophe Auberger
Director Systems Engineering, Fortinet

Senior Colonel Bai Zonglin (Ret.)
Senior Research Fellow, China Institute of International Strategic Studies (CIISS), Beijing

Ms. Rebecca Bash
Office of the Director, Net Assessment, U.S. Department of Defense

Ms. Caroline Baylon
Research Associate (Cyber Security), The Royal Institute of International Affairs (Chatham House)

Ms. Anne Baylon
Co-Director, Center for Strategic Decision Research

Mr. Thierry Bedos
McAfee, part of Intel Security

Ingénieur général de l'armement Patrick Bellouard (Ret.)
EuroDefence France; Former Director, Organisation conjointe de coopération en matière d'armement (OCCAR)

Ambassador Haydar Berk
Senior Advisor, Turkish Ministry of Foreign Affairs

Admiral Jean Betermier (Ret.)
President, Forum of the Future

Mr. Tim Bloechl
Director, Cyber Security, Quantum Research International

Dr. Robert Boback
CEO and Founder, Tiversa

Senator Jean-Marie Bockel
Member of the Foreign Affairs, Defense and Armed Forces Committee, French Senate; Former Minister

Mr. Marco Braccioli
Senior Vice President, Area SpA

Mr. Maurice Cashman
Director, Enterprise Architects EMEA, McAfee, part of Intel Security

Major General Eduardo Centore
Centro Militare di Studi Strategici (CeMiSS)

Ambassador Vladimir Chizhov
Permanent Representative of the Russian Federation to the EU

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

Mr. Jim Cowie
Chief Scientist, Dyn

Major General John Allan Davis
Deputy Assistant Secretary for Cyber Policy (Acting), U.S. Department of Defense

Mr. Anatoly Didenko
Counselor, Russian Mission to the EU

Ambassador Ihor Dolhov
Ambassador of Ukraine to NATO

General Hans-Lothar Domröse
Commander, Allied Joint Force Command Brunssum

Professor Frédérick Douzet
Castex Chair of Cyber Strategy, Institut des hautes études de défense nationale

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

Vice Admiral Marc Ectors
Military Representative of Belgium to NATO and the EU

Ambassador Christoph Eichhorn
Deputy Federal Government Commissioner of Germany for Disarmament and Arms Control

Mr. Andrea Formenti
CEO, Area SpA

Mr. Richard Froh
Deputy Assistant Secretary General for Operations, NATO

Mr. Gary Gagnon
Senior Vice President and Chief Security Officer, The MITRE Corporation

Mr. Thorniké Gordadze
Deputy Director of Studies and Research, Institut des hautes études de défense nationale (IHEDN)

Mr. Evgeny Grigorenko
Senior Public Affairs Manager, CEO Office, Kaspersky Lab

Mr. Patrick Grillo
Senior Director, Solutions Marketing, Fortinet

Mr. David Grout
Director for Southern Europe, McAfee, part of Intel Security

Mr. Tim Hall
Chief Technical Officer, Tiversa

Mr. D. A. Harris
Managing Director, Worldwide Defense, Microsoft

Mr. Ernest J. Herold
Deputy Assistant Secretary General for Defense Investment, NATO

Admiral Willy Herteleer (Ret.)
President, EuroDefence Belgium; Former Chief of Defense of Belgium

Ambassador Khazar Ibrahim
Ambassador of Azerbaijan to NATO

Lt. Col. Robert Kosla (Ret.)
Director, Central and Eastern Europe, National Security/Defense, Microsoft

Mr. Haden Land
Vice President, Research & Technology, Lockheed Martin Information Systems & Global Solutions

Mr. Robert Lentz
CEO, Cyber Security Strategies; former U.S. Deputy Assistant Secretary of Defense (Cyber Security)

Mr. LI Zuyang
Assistant Research Fellow, China Institute for International Strategic Studies (CIISS), Beijing

Dr. Itamara Lochard
Director, Cyber Security Initiative; Middlebury Institute of International Studies (MIIS)

Ms. Michele Markoff
Deputy Coordinator for Cyber Issues, U.S. Department of State

Mr. Bernard Marty
Director, Public Safety and National Security, Microsoft

Mr. Jean-Pierre Maulny
Deputy Director, Institut de relations internationales et stratégiques (IRIS)

Prof. Dr. Holger Mey
Head of Advanced Concepts, Airbus Defense and Space

Mr. Gavin Millard
Technical Director, EMEA, Tenable Network Security

Ambassador João Mira Gomes
Ambassador of Portugal to NATO

Ms. Roya Mohadjer
Lead for STEM/STEAM, Lockheed Martin Information Systems & Global Solutions

Dr. Gerlinde Niehus
Head, Engagements Section, Public Diplomacy Division, NATO

Ambassador Dr. Assad Omer
Ambassador of Afghanistan to France

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

Mr. Adam Palmer
Director, International Government Affairs, FireEye

Mr. Ioan Mircea Pascu MEP
Member of the European Parliament; Former Minister of Defense of Romania

Ingénieur général Robert Ranquet
Deputy Director, Institut des hautes études de défense nationale (IHEDN)

Senator Alain Richard
French Senate; Former Minister of Defense

Professor Jean-Jacques Roche
Director of Studies and Research, Institut des hautes études de defense nationale

Ms. Hélène de Rochefort
Secretary General, Association France-Amériques

General Patrick de Rousiers
Chairman of the European Union Military Committee; Military Advisor to the High Representative of the European Union for Foreign Affairs

Ambassador Omar Samad
President, Silk Road Consulting; Former Ambassador of Afghanistan to France

Ms. Marietje Schaake MEP
Member of the European Parliament

Mr. Kevin Scheid
Special Advisor to the President and CEO, The MITRE Corporation

Mr. Jean-François Sebastian
Director, Public Sector, McAfee, part of Intel Security

Ambassador Jiří Šedivý
Ambassador of the Czech Republic to NATO

Major General David Senty
Director, Cyber Operations, The MITRE Corporation; Former Chief of Staff, U.S. Cyber Command

Mr. Henri Serres
High Council for Economy, Industry, Energy and Technology, French Ministry of the Economy and Finance; Member of the Board of Directors, Orange

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

Mr. Anton Shingarev
Head, CEO Office and Director of Global Government Relations, Kaspersky Lab

Ambassador Thrasyvoulos Terry Stamatopoulos
Assistant Secretary General for Political Affairs and Security Policy, NATO

Sir Kevin Tebbit KCM CMG
Former Permanent Secretary of Defence of the United Kingdom

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

Ms. Pascale Trimbach
Head of Department of Multilateral and Sectorial Issues, French Foreign Ministry

Ms. Isabelle Valentini
Deputy to the General Officer Cyber Defense, Head of Cyber Policy, French Joint Defense Staff

Mr. Vesa Virtanen
Secretary General of the Security Committee, Finnish Ministry of Defence

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

Dr. Linton Wells II
Visiting Distinguished Research Fellow, National Defense University

Dr. Jack Wheeler
Geopolitical Strategist, Tiversa

Ambassador Dr. Bogusław Winid
Ambassador of Poland to the United Nations

Mr. James R. Wylly
General Manager, *Worldwide Public Safety and National Security*, *Microsoft*

Ambassador Fareed Yasseen
Ambassador of Iraq to France

Supporting Staff

Captain Lieutenant Jan Germer, *Aide de Camp, Allied Joint Force Command Brunssum*

Sergeant Major Dirk Wendel, *Allied Joint Force Command Brunssum*

Workshop Staff

Ms. Anne D. Baylon, *Co-Director, Center for Strategic Decision Research*

Mr. César Castelain, *Staff Member, Center for Strategic Decision Research*

Dr. Ania Garlitski, *Senior Advisor, Center for Strategic Decision Research*

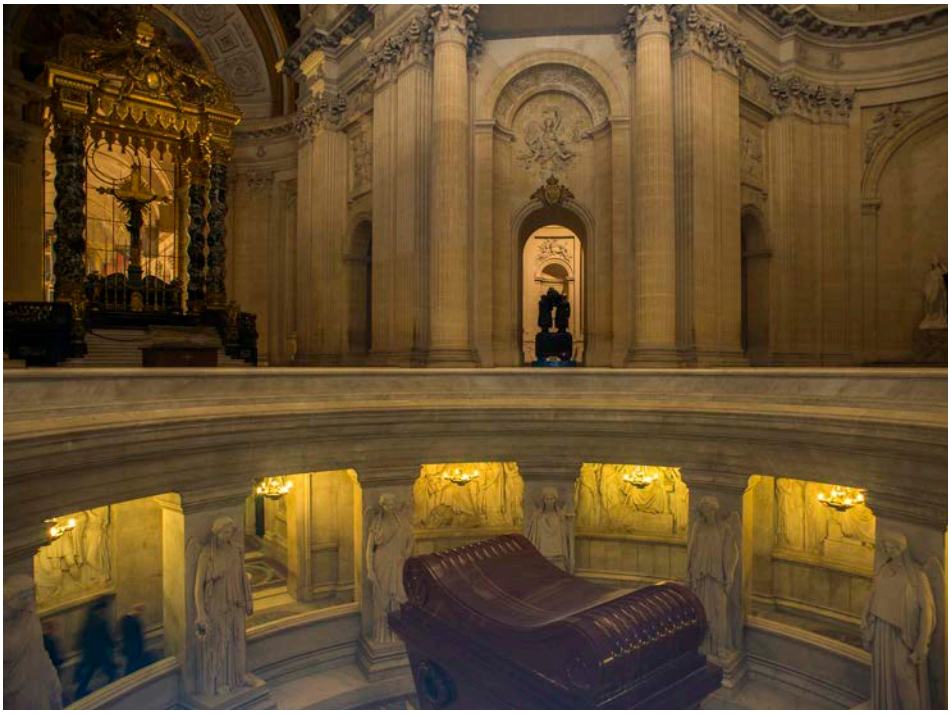
Ms. Jean Lee, *Communications/Photography and Production, Center for Strategic Decision Research*

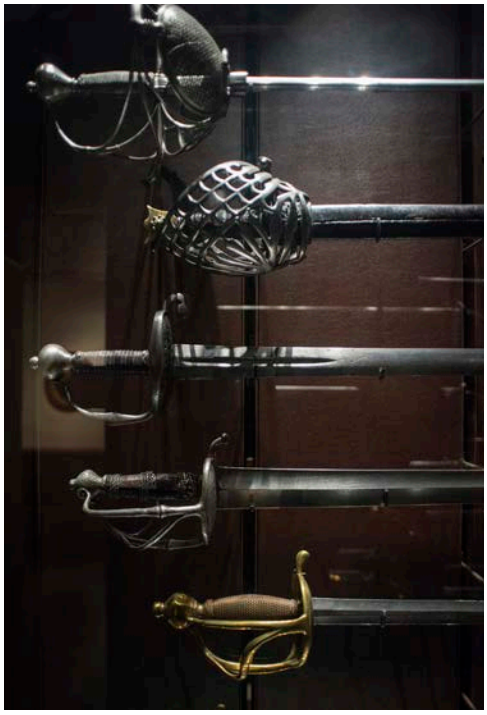
Mr. Pablo Kerblat, *Staff Member, Center for Strategic Decision Research*

Ms. Caroline Baylon, *Senior Advisor, Center for Strategic Decision Research*

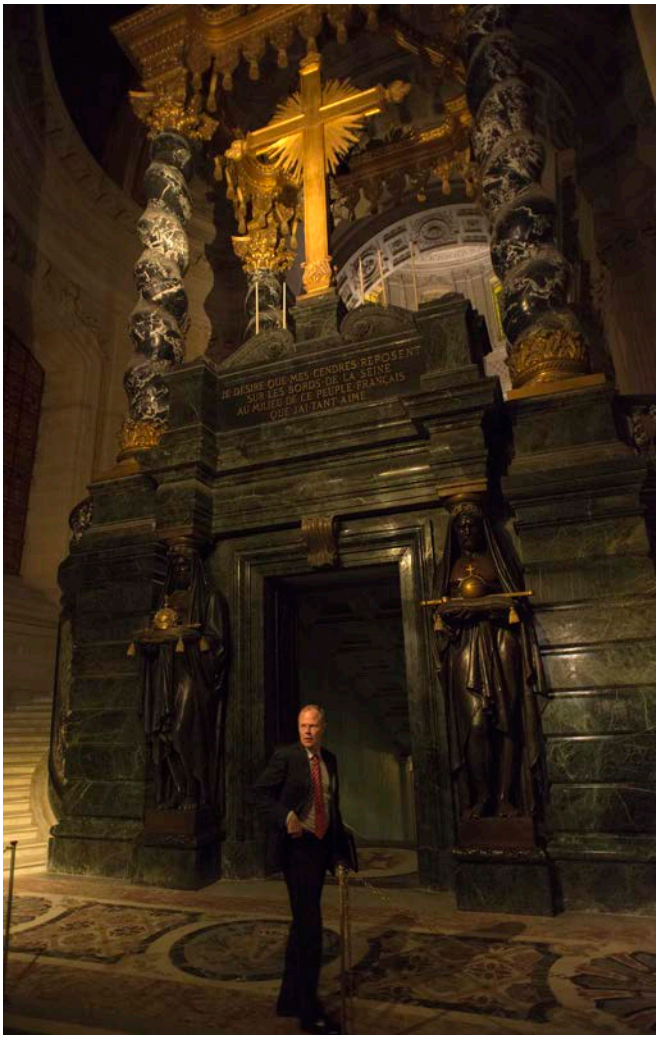
TOP PHOTO: *Opening session of the 31st International Workshop on Global Security in the Grand Salon of the Invalides National Monument, the former council chamber of King Louis XIV.* BOTTOM LEFT: *Senior Colonel Bai Zonglin (Ret.), Senior Research Fellow, China Institute of International Strategic Studies (CIISS), Beijing; General Hans-Lothar Domröse, Commander, Allied Joint Force Command Brunssum.* BOTTOM RIGHT: *General Patrick de Rousiers, Chairman of the European Union Military Committee and Military Advisor to the High Representative of the European Union for Foreign Affairs.*

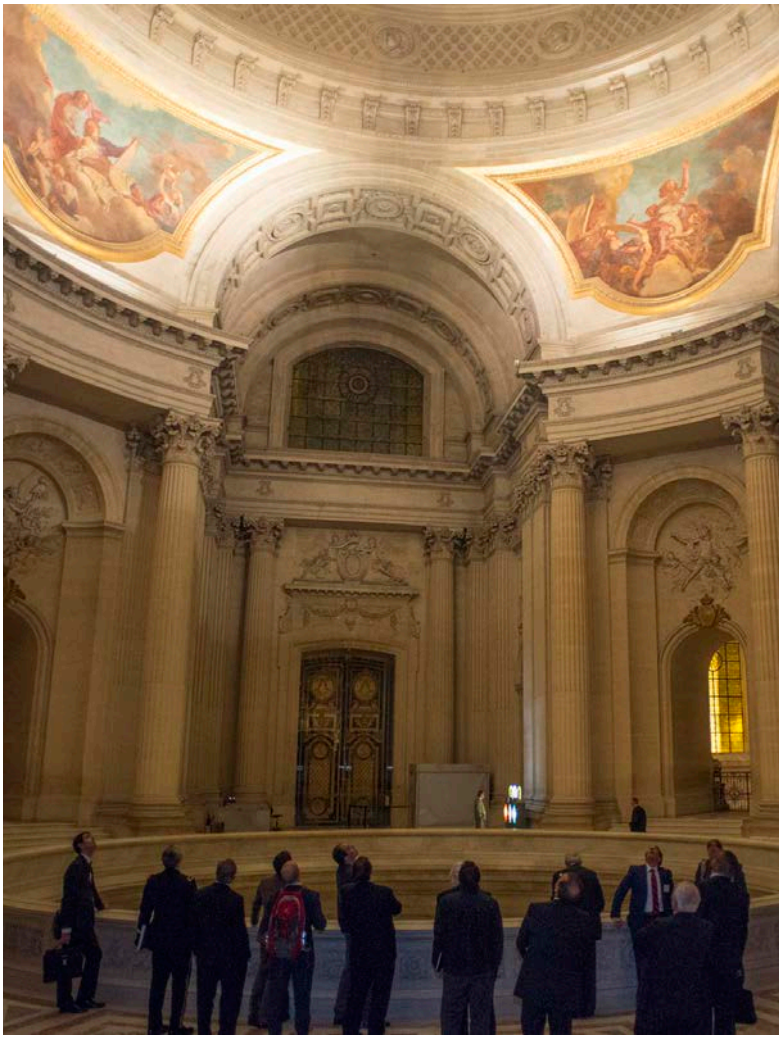
TOP LEFT: *Ingénieur général Robert Ranquet, Deputy Director, IHEDN; Ingénieur général de l'armement Patrick Bellouard (Ret.), EuroDefence France.* TOP RIGHT: *Mr. Jean-Pierre Maulny, Deputy Director, Institut de relations internationales et stratégiques (IRIS); Dr. Gerlinde Niehus, Head, Engagements Section, Public Diplomacy Division, NATO; Mr. E.J. Herold, Deputy Assistant Secretary General for Defense Investment, NATO; Ms. Roya Mohadjer, Lead for STEM/STEAM, Lockheed Martin Information Systems and Global Solutions.* MIDDLE LEFT: *Mr. Evgeny Grigorenko, Senior Public Affairs Manager, CEO Office, Kaspersky Lab and Mr. Anton Shingarev, Head of the CEO Office and Director of Global Government Relations, Kaspersky Lab, with Mr. Tim Bloechl, Cyber Security Director, Quantum Research International.* MIDDLE RIGHT: *Mr. D. A. Harris, Managing Director, Worldwide Defense, Microsoft; Mr. Bernard Marty, Director, Public Safety and National Security, Microsoft.* BOTTOM LEFT: *The Invalides courtyard at night.* BOTTOM RIGHT: *Dr. Jack Wheeler, Geopolitical Strategist, Tiversa, with Mr. Tim Hall, Chief Technical Officer, Tiversa.*





CLOCKWISE FROM TOP LEFT: *The Dôme des Invalides (Dome Church). Built as a royal chapel for Louis XIV, it now houses the tomb of Napoleon.* TOP RIGHT: *Weapons on display in the Musée de l'Armée (Army Museum) at the Invalides.* MIDDLE RIGHT: *Ms. Michele Markoff (Deputy Coordinator for Cyber Issues, U.S. Department of State).* BOTTOM RIGHT: *Mr. James R. Wylly (General Manager, Worldwide Public Safety and National Security at Microsoft) inspects a scale model of a battle from the Napoleonic era.* BOTTOM LEFT: *Participants are guided through the history and architecture of the Cathédrale Saint-Louis des Invalides.*

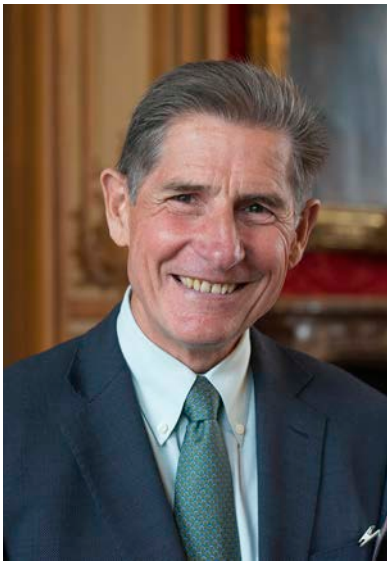




CLOCKWISE FROM TOP: *Mr. Anton Shingarev (Head, CEO Office and Director of Global Government Relations, Kaspersky Lab) touring the collection of antique weaponry on display.* BOTTOM RIGHT: *Continuing their private tour of the grounds of the Invalides, workshop participants take in the murals of the Dôme des Invalides.* BOTTOM LEFT: *Mr. Vesa Virtanen (Secretary General of the Security Committee, Finnish Ministry of Defence) heading down to Napoleon's Tomb.*

TOP PHOTO: *Looking up towards the Dôme des Invalides, which sits directly above Napoleon's tomb.* MIDDLE LEFT: *Mr. Kevin Scheid, Special Advisor to the President and CEO, The MITRE Corporation.* MIDDLE CENTER: *Ms. Hélène de Rochefort, Secretary General, Association France-Amériques.* MIDDLE RIGHT: *Welcome by the chamber ensemble of the French Army (Conservatoire Militaire de Musique de l'Armée de Terre).* BOTTOM LEFT: *Mr. Marco Braccioli, Senior Vice President, Area SpA, and Mr. Andrea Formenti, CEO of Area SpA.* BOTTOM RIGHT: *Mr. Thorniké Gordadze, Deputy Director of Studies and Research, Institut des hautes études de défense nationale (IHEDN), with Admiral Jean Betermier (Ret.), President of Forum of the Future.*

TOP PHOTO: *Admiral Willy Herteleer (Ret.), President of EuroDefence Belgium during a workshop panel Q&A session.* MIDDLE LEFT: *Mr. Gary Gagnon, Senior Vice President and Chief Security Officer, The MITRE Corporation; Major General John Allan Davis, Deputy Assistant Secretary for Cyber Policy (Acting), U.S. Department of Defense; and Major General David Senty, Director, Cyber Operations, The MITRE Corporation, and Former Chief of Staff, U.S. Cyber Command.* BOTTOM RIGHT: *Lt. Col. Robert Kosla (Ret.), Director, Central and Eastern Europe, National Security/Defense, Microsoft; Mr. James R. Wylly, General Manager, Worldwide Public Safety and National Security, Microsoft; and Mr. D. A. Harris, Managing Director, Worldwide Defense, Microsoft.* BOTTOM LEFT: *Mr. Vesa Virtanen, Secretary General of the Security Committee, Finnish MoD.*




TOP LEFT: *Dr. Roger Weissinger-Baylon with Mr. Adam Palmer, Director, International Government Affairs for FireEye.* TOP CENTER: *Mr. Richard Froh, Deputy Assistant Secretary General for Operations, NATO.* TOP RIGHT: *Mr. Stéphane Aouichia, Regional Sales Manager, Southwest Europe, Tenable Network Security.* MIDDLE LEFT: *Admiral Willy Herteleer (Ret.), President, EuroDefence Belgium and former Belgian CHOD; VADM Marc Ectors, MILREP of Belgium to NATO.* MIDDLE RIGHT: *Ms. Marietje Schaake, MEP, Member of the European Parliament and Mr. Chris Painter, Coordinator for Cyber Issues, U.S. Department of State.* BOTTOM LEFT: *Mr. Tim Bloechl, Cyber Security Director, Quantum Research International, and Mr. Robert Lentz, CEO, Cyber Security Strategies; former U.S. Deputy Assistant Secretary of Defense (Cyber Security).* BOTTOM RIGHT: *Mrs. Cathy Land, Ms. Roya Mohadjer, Lead for STEM/STEAM, Lockheed Martin Information Systems and Global Solutions and Mr. Haden Land, Vice President, Research and Technology, Lockheed Martin Information Systems and Global Solutions.*