Peace and Security *The Challenges Ahead*

PROCEEDINGS OF THE 30*th* INTERNATIONAL WORKSHOP ON GLOBAL SECURITY

His Excellency Jean-Yves Le Drian, *Minister of Defense of France* / WORKSHOP PATRON

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

Anne D. Baylon / EDITOR

Peace and Security *The Challenges Ahead*

PROCEEDINGS OF THE *30th* INTERNATIONAL WORKSHOP ON GLOBAL SECURITY

His Excellency Jean-Yves Le Drian, *Minister of Defense of France* / WORKSHOP PATRON
Dr. Roger Weissinger-Baylon, *Co-Director, Center for Strategic Decision Research* / WORKSHOP CHAIRMAN
Anne D. Baylon / EDITOR

FRONT COVER

The main courtyard of the *Hôtel National des Invalides,* with the *Dôme des Invalides* (or Dome Church) in the background.

INSIDE TITLE PAGE

Musée de l'Armée (Army Museum): armor from the 13th to 17th century.

BACK COVER

The *Dôme des Invalides.* Built as a royal chapel for Louis XIV, it now houses the tomb of Napoleon.

International Standard Book Number: 1-890664-20-0

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

Photography by Jean Lee.

Center for Strategic Decision Research
&
Strategic Decisions Press
2456 Sharon Oaks Drive, Menlo Park, California 94025 USA
Telephone: +1 (650) 854-4751 Fax: +1 (650) 854-0761
anne@csdr.org | roger@csdr.org | www.csdr.org

WITH APPRECIATION

His Excellency Jean-Yves Le Drian
French Minister of Defense
WORKSHOP PATRON

Minister Kader Arif
Vice Minister of Defense of France
CLOSING KEYNOTE ADDRESS

Lieutenant General Jean-Marc Duquesne
Director, Institut des hautes études de défense nationale
(IHEDN)

TOP ROW

Opening session of the 30th International Workshop on Global Security in the *Grand Salon* of the Invalides National Monument, the former council chamber of King Louis XIV.

MIDDLE ROW

left photo

Dr. Andrew Murrison MP, Minister for International Security Strategy of the United Kingdom.

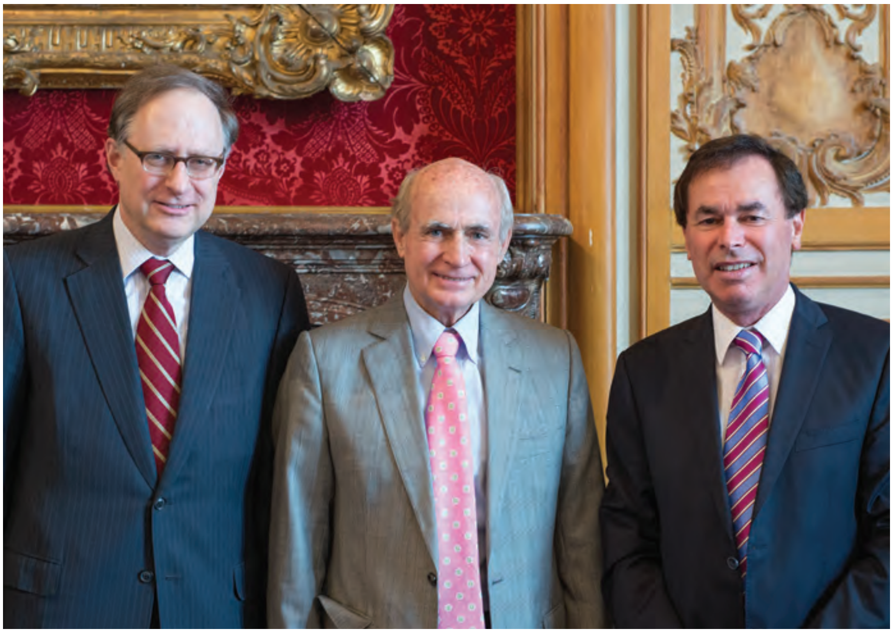
right photo, from left to right

Ambassador Alexander Vershbow, Deputy Secretary General of NATO;
Dr. Roger Weissinger-Baylon, Workshop Chairman and Founder;
His Excellency Alan Shatter TD, Minister of Justice, Equality and Defense of Ireland.

BOTTOM ROW

from left to right

His Excellency Zekerijah Osmic, Minister of Defense of Bosnia and Herzegovina;
Ambassador Michel Foucher, Director of Studies and Research, Institut des hautes études de défense nationale (IHEDN);
Dr. Roger Weissinger-Baylon, Workshop Chairman and Founder;
Minister Franco Frattini, former Vice President of the European Commission and former Minister of Foreign Affairs of Italy;
His Excellency Irakli Alasania, Minister of Defense of Georgia;
His Excellency Igor Lukšić, Deputy Prime Minister and Minister of Foreign Affairs of Montenegro.



Ambassador
Michel Foucher
Director of Studies and Research,
Institut des hautes études
de défense nationale (IHEDN)
ger Weissinger-Baylon
Co-Director,
er for Strategic Decision Research
raldi Alasania
Minister of Defence of Georgia
His Excellency Dr.
Igor Lukšić
Deputy Prime Minister and
Minister of Foreign Affairs and
European Integration of Montenegro

TOP ROW
from left to right
Minister Bogusław Winid, Undersecretary of State, Ministry of Foreign Affairs of Poland;
State Secretary Tamás Vargha, Parliamentary State Secretary, Ministry of Defense of Hungary;
Ambassador István Kovács, Ambassador of Hungary to NATO;
First Deputy Minister Daniel Kostoval, First Deputy Minister of Defense of the Czech Republic.

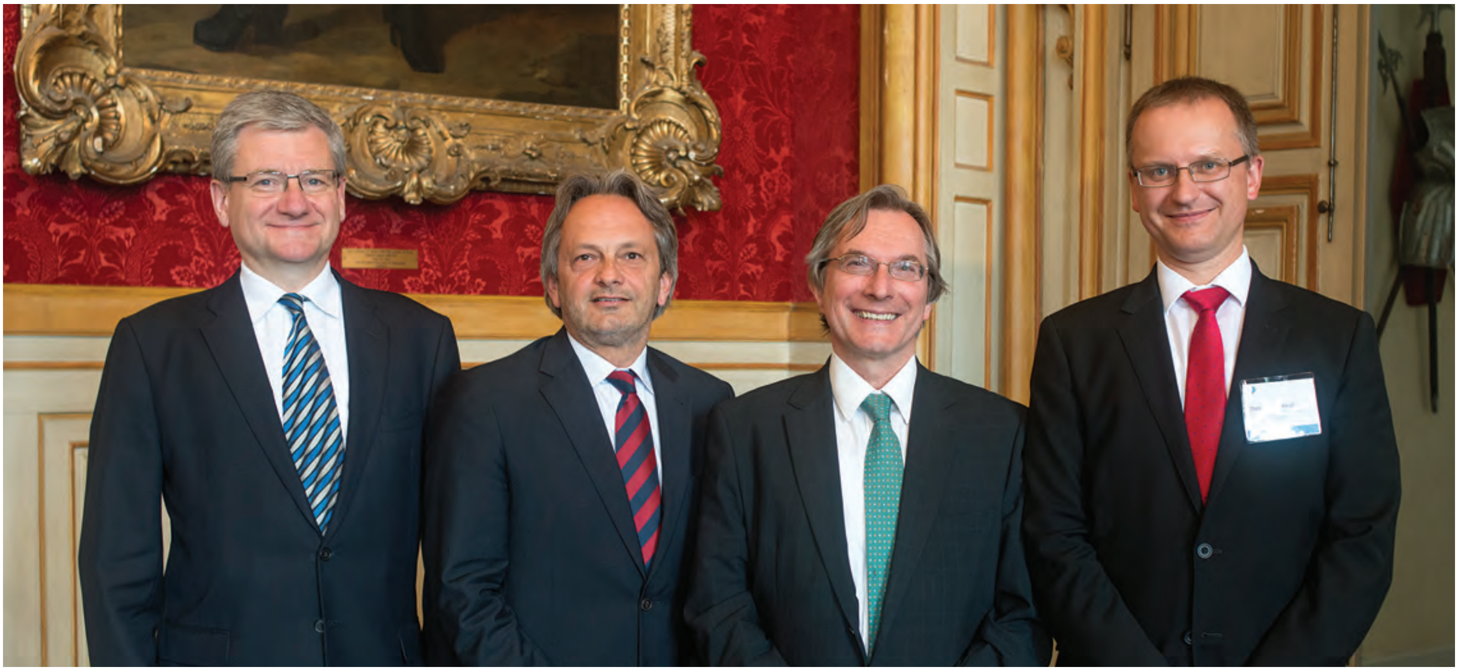
MIDDLE ROW
left photo
Ingénieur Général Robert Ranquet, Deputy Director, Institut des hautes études de défense nationale (IHEDN).

middle photo
General of the Army Bertrand Ract-Madoux, Chief of General Staff of the French Army.

right photo
His Excellency Talat Xhaferi, Minister of Defense of Macedonia.

BOTTOM ROW
left photo, from left to right
Dr. Roger Weissinger-Baylon, Workshop Chairman and Founder;
Ambassador Dr. Assad Omer, Ambassador of Afghanistan to France.

right photo, from left to right
Vice Admiral Mark Fox, Deputy Commander, U.S. Central Command;
Ambassador Larry Butler, Civilian Deputy to the Commander, U.S. European Command and Foreign Policy Advisor.



Talat Xhaferi

Assad Omer

MARK FOX

TOP ROW

left photo, from left to right

Ms. Rebecca Bash, Acquisition Advisor, Office of the U.S. Director of Net Assessment;
Admiral Jean Betermier, President, Forum of the Future.

right photo, from left to right

General Hans-Lothar Domröse, Commander, Allied Joint Force Command Brunssum;
Vice Admiral Mark Fox, Deputy Commander, U.S. Central Command.

MIDDLE ROW

from left to right

Ambassador Alejandro Alvargonzález San Martín, Secretary General for Defense Policy, Spanish Defense Ministry;
Dr. Stefanie Babst, Head, Strategic Analysis for the NATO Secretary General and Chairman of the NATO Military Committee;
Dr. Roger Weissinger-Baylon, Workshop Chairman and Founder;
Vice Admiral Mark Fox, Deputy Commander, U.S. Central Command;
Ambassador Fareed Yasseen, Ambassador of Iraq to France.

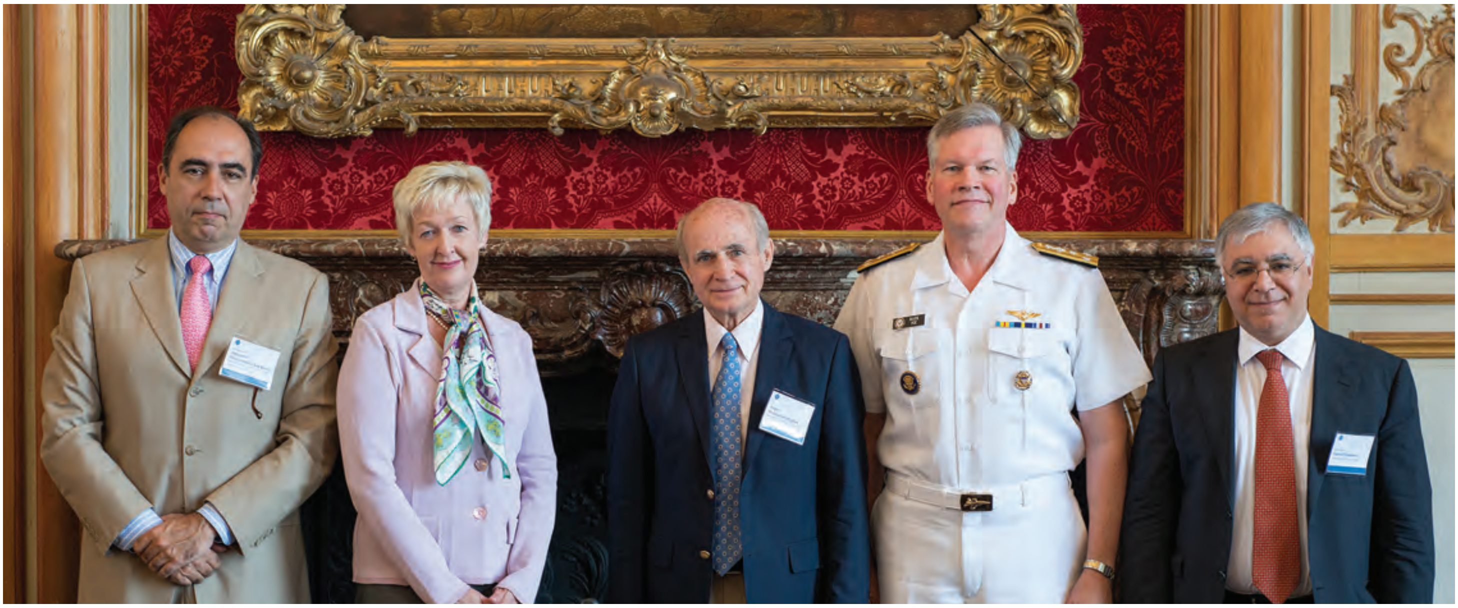
BOTTOM ROW

left photo, from left to right

Dr. Frederick Douzet, Castex Chair of Cyber Strategy, Institut des hautes études de défense nationale (IHEDN);
Major General David Senty, former Chief of Staff, U.S. Cyber Command; Director, Cyber Operations, the MITRE Corporation.

right photo, from left to right

His Excellency Dr. Jaak Aaviksoo, Minister of Education and Research of Estonia; former Minister of Defense;
Mr. Marco Braccioli, Senior Vice President, Area S.p.A.



érick Douzet
Chair of Cyber Strategy,
Major General
David Senty
Director, Cyber Operations,
BOSCH

Marco Braccioli
Senior Vice President, Area S.p.A.
TOSHIBA
BOSCH

TOP ROW

from left to right

Mr. Hervé Guillou, former CEO, Cassidian Cyber Security;
Rear Admiral Arnaud Coustillière, Cyber Lead, French Ministry of Defense;
Dr. Roger Weissinger-Baylon, Workshop Chairman and Founder;
Mr. Patrick Pailloux, Director General, French National Agency for Information Systems Security (ANSSI);
Mr. Haden Land, Vice President, Engineering and Chief Technology Officer, Lockheed Martin Information Systems and Global Solutions.

MIDDLE ROW

left photo, from left to right

Major General Cai Jihua, Senior Advisor, China Institute for International Strategic Studies (CIISS), Chinese Ministry of Foreign Affairs;
Ms. Yang Nuan, China Institute for International Strategic Studies, Chinese Ministry of Foreign Affairs.

right photo, from left to right

Minister Kader Arif, Vice Minister of Defense of France;
Lieutenant General Jean-Marc Duquesne, Director, Institut des hautes études de défense nationale (IHEDN).

BOTTOM ROW

left photo

Ambassador Ichiro Komatsu, Ambassador of Japan to France.

middle photo, from left to right

Minister Bogusław Winid, Undersecretary of State, Ministry of Foreign Affairs of Poland;
Ambassador Carsten Søndergaard, Ambassador of Denmark to NATO.

right photo

Ambassador Yves Brodeur, Ambassador of Canada to NATO.

Rear Admiral
Arnaud Coustillière
Cyber Lead, French Defense Ministry
Dr.
Roger Weissinger-Baylon
Workshop Chairman; Co-Director
Center for Strategic Decision Research
Patrick Pailloux
Director General
Agence nationale de la sécurité des systèmes d'information (ANSSI)
Haden Land
Vice President of Engineering
and Chief Technology Officer,
Lockheed Martin IS&GS-Civil

Ambassador
Ichiro Komatsu
Ambassador of Japan to France

Ambassador
Yves Brodeur
Ambassador of Canada to NATO

TOP ROW

Reception and dinner in the *Salons du Gouverneur Militaire* of the Invalides,
the private ceremonial rooms of the Military Governor of Paris.

MIDDLE ROW

left photo, from left to right

Ms. Neyla Arnas, Senior Research Fellow, National Defense University, U.S. Department of Defense;
Prof. Dr. Holger Mey, Head of Advanced Concepts, Cassidian.

right photo, from left to right

Mr. Francis Bruckmann, Deputy Director of Corporate Security, Orange;
Mr. Robert Rodriguez, Chairman, Security Innovation Network (SINET).

BOTTOM ROW

Post-workshop private visit of the French Senate, which is housed in the Palais du Luxembourg,
the former royal palace of French queen Marie de Medicis.

Robert Rodriguez

The *30th 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 sponsorship of the following governments and organizations:

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE
DE LA DÉFENSE

UNITED STATES
DEPARTMENT OF DEFENSE
Net Assessment
National Defense University

NATO
OTAN

Center for
Strategic
Decision
Research

IHEDN

MAJOR SPONSORS

NORTHROP GRUMMAN

orange™

MITRE

TIVERSA

AREA

ASSOCIATE SPONSORS

URS

JUNIPer
NETWORKS

ACKNOWLEDGEMENTS OF PAST HOST AND SPONSORING GOVERNMENTS

Czech Republic

Kingdom of Denmark

Federal Republic of Germany

Republic of Greece

Republic of Hungary

Kingdom of the Netherlands

Kingdom of Norway

Republic of Poland

Republic of Portugal

Ministry of Defense of Austria

Ministry of Defense of France

Ministry of Defense of Italy

Ministry of Defense of Turkey

Canadian Armed Forces

Russian Ministry of Industry, Science, and Technology

Table of Contents

Peace and Security: the Challenges Ahead

Contributors

His Excellency Dr. Jaak Aaviksoo
Minister of Education and Research of Estonia; former Minister of Defense

His Excellency Irakli Alasania
Minister of Defense of Georgia

Ambassador Alejandro Alvargonzález San Martín
Secretary General for Defense Policy, Spanish Ministry of Defense

Minister Kader Arif
Vice Minister of Defense of France

Ms. Neyla Arnas
Senior Research Fellow, National Defense University, United States Department of Defense

Mr. Jon Arnold
Director, U.K. Government and Defense, Juniper Networks

Dr. Stefanie Babst
Head, Strategic Analysis Capability to the NATO Secretary General and Chairman of the Military Committee

Ms. Rebecca Bash
Office of the Director, Net Assessment, United States Department of Defense

Ms. Anne Baylon
Co-Director, Center for Strategic Decision Research

Admiral Jean Betermier
President, Forum of the Future

Mr. Robert Boback
CEO, Tiversa

Mr. Marco Braccioli
Senior Vice President, Area S.p.A.

Ambassador Yves Brodeur
Ambassador of Canada to NATO

Mr. Francis Bruckmann
Deputy Director of Corporate Security, Orange

Ambassador Larry Butler
Civilian Deputy to the Commander and Political Advisor, U.S. European Command

Major General Cai Jihua
Senior Advisor, China Institute for International Strategic Studies (CIISS), Chinese Ministry of Foreign Affairs

Major General Eduardo Centore
Director, Military Centre for Strategic Studies (CeMiSS), Italian Ministry of Defense

Rear Admiral Arnaud Coustillière
Cyber Lead, French Ministry of Defense

Mr. Jim Cowie
Co-Founder and Chief Technical Officer, Renesys

Vice Admiral Robert Davidson
Military Representative of Canada 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 (IHEDN)

Lieutenant General Jean-Marc Duquesne
Director, Institut des hautes études de défense nationale (IHEDN)

Vice Admiral Marc Ectors
Military Representative of Belgium to NATO and the EU

Mr. William Ennis
Director, International Programs, Northrop Grumman

Mr. Andrea Formenti
CEO, Area S.p.A.

Ambassador Michel Foucher
Director of Studies and Research, Institut des hautes études de défense nationale (IHEDN)

Vice Admiral Mark Fox
Deputy Chief of Naval Operations for Operations, Plans, and Strategy, United States Navy

Minister Franco Frattini
former Vice President of the European Commission; former Minister of Foreign Affairs of Italy

Mr. Gary Gagnon
Senior Vice President and Corporate Director of Cyber Security, The MITRE Corporation

Mr. Hervé Guillou
former President, EADS Cyber Security

Mr. Tim Hall
Chief Technical Officer, Tiversa

Ambassador Khazar Ibrahim
Ambassador of Azerbaijan to NATO

Colonel Enver Jakupi
Former Macedonian Defense Attaché to France

Mr. Tas Kelemen
Head of Defense Policy Department, Hungarian Ministry of Defense

Ambassador Ichiro Komatsu
Ambassador of Japan to France

Mr. Daniel Kostoval
First Deputy Minister, Czech Ministry of Defense

Ambassador István Kovács
Ambassador of Hungary to NATO

Ms. Dahlia Kownator
CEO and Founder, Bacalis Public Affairs

Ambassador Artur Kuko
Ambassador of Albania to NATO

Mr. Haden Land
Vice President, Engineering and Chief Technology Officer, Lockheed Martin IS&GS - Civil

Senator Gérard Longuet
Senator of Meuse; former Minister of Defense of France

His Excellency Dr. Igor Lukšić
Deputy Prime Minister and Minister of Foreign Affairs and European Integration of Montenegro

Mrs. Ermira Mehmeti
Member of the Parliament of Macedonia

Prof. Dr. Holger Mey
Head of Advanced Concepts, Cassidian

Mr. Jean-Luc Moliner
Senior Vice President, Head of Orange Group Security

Dr. Chris Moore-Bick
Secretary to the Minister for International Security Policy, U.K. Ministry of Defense

Mr. James Moseman
Director, Europe and NATO, Northrop Grumman International

Mr. Ciaran Murphy
Assistant Secretary General and Defence Policy Director, Irish Ministry of Defense

Dr. Andrew Murrison, MP
Minister for International Security Strategy of the United Kingdom

Ambassador Dr. Assad Omer
Ambassador of Afghanistan to France

Lieutenant General Stefan Oprea
Military Representative of Romania to NATO and the EU

His Excellency Zekerijah Osmić
Minister of Defense of Bosnia and Herzegovina

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

General of the Army Bertrand Ract-Madoux
Chief of the General Staff of the French Army

Ambassador Elena Radovic
Ambassador of Montenegro to France

Ingénieur Général Robert Ranquet
Deputy Director, Institut des hautes études de défense nationale (IHEDN)

Ms. Hélène de Rochefort
Secretary General, Association France-Amériques

Mr. Robert Rodriguez
Chairman, Security Innovation Network (SINET)

Mr. Jean-François Sebastian
Director, Public Sector, McAfee | Intel

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

His Excellency Alan Shatter, TD
Minister of Justice, Equality and Defence of Ireland

Ambassador Carsten Søndergaard
Ambassador of Denmark to NATO

Mr. David Swindle
Executive Vice President, URS Federal Services

Sir Kevin Tebbit, KCM, CMG
former Permanent Secretary of Defence of the United Kingdom

Brigadier General Christine Turner
former Deputy Assistant Chief of Staff, Allied Command Transformation, SHAPE

Mr. Tamás Vargha
Parliamentary State Secretary, Hungarian Ministry of Defense

Ambassador Alexander Vershbow
Deputy Secretary General of NATO

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

Ambassador Dr. Bogusław Winid
Undersecretary of State for Security Policy, Polish Ministry of Foreign Affairs

His Excellency Talat Xhaferi
Minister of Defense of Macedonia

General Michel Yakovleff
Deputy Chief of Staff, Joint Force Command Brunssum

Ms. Yang Nuan
China Institute for International Strategic Studies, Chinese Ministry of Foreign Affairs

Ambassador Fareed Yasseen
Ambassador of Iraq to France

Diplomatic Observers

Mr. Varlam Avaliani, *Advisor to the Minister, Georgian Ministry of Defense*

Ms. Debbie Brothers, *NATO and European Policy, British Embassy*

Mr. Alessandro Gonzales, *Political Counselor, Italian Embassy*

Ms. Ksenia Kirpichenko, *Russian Embassy*

Captain Stefan Kraus, *Aide-de-Camp to the Commander, Allied Joint Force Command Brunssum*

Air Commodore John Maas, *Defence Attaché, British Embassy*

Ambassador Giandomenico Magliano, *Ambassador of Italy to France*

Ms. Mirjana Nikolic, *Chargé d'Affaires, Serbian Embassy*

Mr. Paata Patiashvili, *Chief of Protocol, Georgian Ministry of Defense*

Dr. Al Robinson, *International Policy France, British Embassy*

Mr. Mustafa Sinanovic, *Chief of Cabinet of the Minister, Bosnia and Herzegovina's Ministry of Defense*

Ambassador Ecaterine Siradze-Delaunay, A*mbassador of Georgia to France*

Mr. Rudolf Štědrý, *Defense Policy Department, Czech Ministry of Defense*

Keynote Address and Welcome

Mr. Kader Arif
Vice Minister of Defense of France

Je suis heureux de venir parmi vous pour ce 30e séminaire international sur la sécurité globale, le 4e à se tenir à Paris, cette année à l'invitation du ministre de la défense Jean-Yves Le Drian qui m'a demandé de le représenter ce soir. Il vous adresse, par ma voix, son salut le plus amical et sa gratitude pour avoir choisi à nouveau Paris cette année pour vos travaux. Cette gratitude s'adresse en particulier au Président Roger Weissinger-Baylon, fondateur de ces séminaires, et à l'Institut des Hautes Etudes de Défense nationale qui l'a soutenu dans cette organisation.

Deux décennies après la fin de la guerre froide, le temps où certains pouvaient croire à l'avènement d'un monde unipolaire est révolu. Dans cette époque qui est désormais celle des puissances relatives, il nous faut prendre conscience de nos intérêts communs de sécurité.

Partout dans le monde, et notamment en Europe et sur le continent américain, nous sommes confrontés à des menaces similaires, qui n'ont plus de frontières : le terrorisme, comme l'ont montré les événements de la bande sahélienne, et tout dernièrement au Mali ; la prolifération des armes de destruction massive dont l'Iran et la Corée du Nord nous rappellent tous les jours l'acuité ; les cyber-attaques, voire les attaques antisatellites ; mais aussi la piraterie, l'insécurité énergétique, la grande criminalité organisée et les trafics de stupéfiants dont l'ampleur nous impose d'adopter une conception de la sécurité infiniment plus large qu'auparavant.

A l'heure où les regards semblent se tourner de plus en plus vers l'Asie-Pacifique comme destinée à devenir le théâtre des grands enjeux de sécurité de notre XXIe siècle, nous ne devons pas perdre de vue que ces mêmes dangers nous guettent sur nos propres marches, et que nous devons nous préparer à y répondre par nos propres forces.

Les États-Unis effectuent un repositionnement stratégique qui impacte nécessairement les théâtres sur lesquels ils s'étaient impliqués ces dernières années. L'Europe est confrontée à une récession qui conduit plusieurs de ses membres à réduire leur effort de défense.

Dans le même temps, les ambitions des puissances émergentes s'affirment à mesure que leur poids économique se renforce. Ainsi, les dépenses militaires de la région Asie–Pacifique viennent de dépasser celles de l'Union européenne.

Trois types de menaces

Dans notre environnement proche, l'illusion peut exister que nous n'ayons plus guère à craindre les menaces de la force, et que les risques de conflits entre Etats se soient éloignés. Mais la perspective est toute différente si on prend une vue plus globale, notamment en Asie où des contentieux géopolitiques, parfois anciens, nourrissent des tensions ou des conflits, ou au Proche-Orient, si proche de nous, de notre histoire, de nos intérêts. De nombreux pays de cette zone, l'Asie, ont augmenté leurs dépenses de défense et modernisé leurs forces armées, alors même que l'architecture régionale de sécurité peine à se mettre en place. Les crises syrienne et iranienne nous montrent que le jeu des Etats est loin d'avoir disparu. En Syrie, le conflit a pris une ampleur inédite, l'usage des armes chimiques est avéré, et la stabilité de toute la région est menacée. C'est l'enjeu de la prochaine conférence de Genève, dont nous appelons de nos vœux la tenue dans les meilleurs délais possibles, mais qui doit se doubler d'un renforcement substantiel de notre soutien à l'opposition.

Le deuxième type de menaces, ce sont celles engendrées par les risques de la faiblesse. Comme nous l'avons vu au Mali, en Somalie ou en Afghanistan, l'incapacité de certains Etats à contrôler leur territoire peut renforcer l'insécurité régionale, en favorisant l'implantation de groupes terroristes, sur fond de piraterie ou trafics illicites de tous types.

Les révolutions arabes qui avaient suscité de grands espoirs soulèvent désormais de légitimes inquiétudes. En Libye, l'instabilité menace non seulement ce pays mais aussi les voisins immédiats, mais aussi l'Europe toute proche. Mais c'est surtout pour nous l'ensemble de la bande sahélienne qui peut représenter, si rien n'est fait, une menace directe contre nos intérêts de sécurité et même contre le territoire européen. C'est pour cela d'abord, pour protéger notre propre sécurité et celle de 'l'Europe que nous sommes intervenus au Mali.

Enfin, il y a les menaces et les risques transverses amplifiés par la mondialisation. Ces menaces peuvent recouvrir la tentation de la prolifération nucléaire balistique ou chimique, ou encore le développement des capacités informatiques offensives de certaines puissances. Il y a, en tout cas, nécessité urgente de mieux contrôler les flux matériels et immatériels qui sont susceptibles d'affecter notre sécurité.

Les objectifs de la France

Face à ces menaces, la France se donne des objectifs simples : à tout moment assurer sa propre sécurité, répondre aux attentes de ses partenaires comme de ses alliés, et contribuer à préserver la paix dans le monde.

La France y a vocation. En tant que membre permanent du Conseil de sécurité des Nations-Unies, elle a cette responsabilité.

La France y a vocation, parce qu'elle est un pays fondateur de l'Union européenne, elle porte un idéal de paix entre les nations.

La France y a vocation, parce qu'elle est dépositaire par son histoire, d'une capacité militaire et diplomatique, qu'elle met au service du droit international.

La France assume ses responsabilités et elle ne baissera donc pas la garde. C'est là la raison profonde de la décision du Président de la république, dont nous devons tous mesurer l'importance politique, de maintenir le budget de défense français au même niveau que 2013, pour atteindre 179,2 milliards sur la prochaine loi de programmation militaire.

Pouquoi la France s'est-elle engagée au Mali?

C'est cette vocation et cette responsabilité qui ont conduit la France à s'engager au Mali. Pourquoi ?

- Parce que nous étions appelés par un pays ami, représenté par son Président légitime.
- Parce qu'il y avait une menace terroriste qui pouvait soumettre le Mali à une emprise dangereuse.
- Parce qu'il y avait un risque pour le Sahel tout entier, à l'évidence, mais aussi pour l'Europe toute entière, et les centaines de tonnes d'armes découvertes nous ont confirmé dans la justesse de notre analyse initiale.

La France s'est engagée la première, parce que nous étions le seul pays disposant de moyens militaires pouvant agir immédiatement, à côté de nos amis africains.

Nous ne sommes pas intervenus à la place des Africains, mais avec les Africains. Nous nous sommes collectivement mobilisés, à l'échelle européenne, pour lancer une mission européenne de formation : EUTM Mali permettant maintenant qu'une opération de stabilisation des Nations Unies puisse être menée dans des conditions de légitimité internationale, d'une part, et d'efficacité d'autre part.

Nous resterons, là encore, avec des effectifs moindres dans les prochains mois. Mais nous resterons au Mali et autour du Mali parce que nous n'en avons pas terminé avec le terrorisme. Le combat que nous avons engagé contre le terrorisme, c'est un combat dans lequel tous les pays doivent, à un moment ou à un autre, être partie prenante, dès lors qu'ils portent les valeurs qui sont les nôtres. Notamment en Afrique, nous devons apporter toute notre solidarité, tout notre soutien, tout notre appui, aux pays de l'Afrique de l'Ouest qui sont confrontés à ce fléau du terrorisme. Nous continuerons à le faire.

La nécessité de travailler ensemble

Les opérations militaires récentes nous ont montré à nouveau combien nous devons travailler ensemble, dans le cadre de l'Union européenne, pour être en mesure de répondre aux crises.

C'est pourquoi la France veut ouvrir une nouvelle étape de la construction de l'Europe de la défense. Plusieurs facteurs nous y conduisent.

La nécessité partagée de redresser nos finances publiques nous invite à mutualiser des capacités, à prendre davantage d'initiatives et à nous appuyer sur les matériels fabriqués en coopération, en tenant compte des savoirs faire de chacun.

C'est ce que la France fait déjà avec le Royaume Uni, pour construire notamment une force d'intervention conjointe, la force expéditionnaire conjointe et combinée (CJEF).

C'est aussi ce que la France veut faire avec l'Allemagne, y compris pour des opérations militaires extérieures. De même, la France poursuivra ses partenariats avec la Belgique, l'Italie ou l'Espagne et associera les nouveaux membres de l'Union européenne à cette démarche. A commencer par la Pologne et les pays du groupe de Visegrád car l'Europe de la défense, cela doit être l'Europe toute entière, dans des formats ad hoc, qui ont du sens d'un point de vue concret.

La France fera des propositions en ce sens d'ici le Conseil européen de décembre 2013.

Elles porteront sur nos présences dans les Balkans, en Méditerranée, au Proche- Orient, en Asie. Partout, l'Europe doit agir de façon mieux coordonnée. Réfléchit-elle avec suffisamment d'audace à ce que nous pourrions faire mieux et peut-être à un coût moindre ?

Elles concerneront aussi nos coopérations dans les domaines du transport aérien, des satellites d'observation, du ravitaillement en vol, des drones pour ne citer que quelques exemples.

Les difficultés du passé ne doivent pas nous décourager mais au contraire nous inviter à persévérer. Notre ambition, c'est de promouvoir, pour l'industrie de défense européenne, des champions européens. C'est déterminant pour le maintien d'une base industrielle et technologique compétitive.

Le grand sujet pour l'Europe n'est pas simplement d'avoir un grand marché, d'avoir une zone monétaire stable. Cela, ce sont des conditions. C'est d'avoir aussi une politique industrielle. Et dans la politique industrielle, il y a l'enjeu de la défense.

La France est dans l'Europe mais elle agit aussi dans le cadre de l'OTAN, dont elle est membre fondateur et qui est notre Alliance. Le Président de la République a récemment confirmé notre présence dans le commandement militaire intégré de l'Alliance atlantique. Tenant tout son rôle dans les actions de l'Alliance, la France entend aussi tenir, dans le même temps, tout son rôle dans la construction de l'Europe de la Défense : il n'y a là aucune contradiction. Bien au contraire, c'est appuyer notre défense sur ses deux pieds naturels : son pied transatlantique et son pied européen.

Agir ensemble pour rétablir et maintenir la paix

C'est par le dialogue, bilatéral et multilatéral, que la politique fonde sa légitimité. Raymond Aron a dit de la guerre froide qu'elle était une « ère de guerre improbable et de paix impossible ». Je reste convaincu que, si les guerres et les crises demeurent toujours une possibilité—et les événements récents dans notre environnement proche le confirment hélas, la paix et le développement n'en constituent pas moins une exigence. Notre responsabilité, la responsabilité de la France, comme de celles des Nations ici représentées, à travers le renforcement de la coopération de défense, est d'encourager nos échanges pour transformer les risques de conflit en réassurances, pour prévenir, et circonscrire les facteurs de déstabilisation; pour, lorsque les circonstances l'exigent, agir en projetant ensemble la force des armes pour rétablir ensemble la paix et la maintenir. Incontestablement le séminaire international sur la sécurité globale apporte une pierre essentielle à cet édifice.

Keynote Address and Welcome

Mr. Kader Arif
Vice Minister of Defense of France

(Translated by Anne D. Baylon)

It is a pleasure to be with you for this 30th International Workshop on Global Security, the fourth workshop to take place in Paris, at the invitation this year of Defense Minister Jean-Yves Le Drian who has asked me to represent him tonight. The minister sends you his warmest greetings and wishes to convey his gratitude to you for selecting Paris again as the place of choice for your work. In particular, he wishes to thank Roger Weissinger-Baylon, the Chairman and Founder of this workshop series and the Institut des hautes études de défense nationale (IHEDN) for supporting him in this endeavor.

Two decades after the end of the Cold War, the time when we might have expected the dawn of a unipolar world is gone. In this new era of relative powers, we must become aware of our common security interests.

Everywhere in the world, and particularly in Europe and on the American continent, we are facing similar threats that are borderless: terrorism, as evidenced by the events in Sahel and lately in Mali; proliferation of weapons of mass destruction, an acute problem that Iran and North Korea remind us of everyday; cyber attacks and even anti-satellite attacks; but also piracy, energy insecurity, organized crime and drug trafficking on such a large scale that we have been forced to adopt a much more extensive concept of security than in the past.

At a time when the Asia-Pacific region is increasingly attracting interest as the future theater for the security challenges of the 21st century, we must keep in mind that similar dangers exist on our doorstep and that we must be prepared to face them with our own resources.

The strategic repositioning of the United States will inevitably impact the theaters in which they were actively involved in recent years. Europe is facing a recession that has led several of its members to reduce their defense contributions.

At the same time, emerging powers are gaining in economic strength and affirming their ambitions. The Asia-Pacific region's military spending now exceeds that of the European Union.

The Three Kinds of Threats

In our immediate surroundings, we may live under the illusion that we no longer need to fear the threat of force and that the risks of conflicts between States have receded. But a more global view shows a very different perspective, especially in Asia where long-standing political disputes can fuel tensions or conflicts, or in the Middle East, which is so close to us, to our history and interests. Although many Asian countries still wrestle with the implementation of the regional security architecture, they have increased their defense spending and modernized their armed forces. The Syrian and Iranian crises demonstrate that States are still playing games. In Syria, the conflict has taken on an unprecedented scale, there is proof that chemical weapons have been used, and the stability of the entire region is threatened. It will be the focus of the next Geneva conference, which we hope will take place as soon as possible and with a substantial reinforcement of our support to the opposition.

The second type of threats is caused by the danger of being weak. As we saw in Mali, in Somalia or in Afghanistan, the inability of certain States to control their territory can increase regional insecurity by making it possible for terrorist groups to become established and introduce piracy or all kinds of illicit trafficking.

At first, the Arab revolutions raised great expectations but today, they raise legitimate concerns. Instability in Libya does more than threaten the country itself, it also threatens its immediate neighbors and nearby Europe. But above all, it is the entire Sahelian zone that poses a direct threat to our security interests and even those of Europe if nothing is done about it. This is the primary reason for our intervention in Mali.

Finally, globalization exacerbates transverse threats and risks such as the temptation of nuclear proliferation, either ballistic or chemical, or the development of offensive information technology by certain powers. For all these reasons, we urgently need to do a better job of controlling the material and non-material flows that may affect our security.

French Objectives

To face these threats, France has set forth simple goals which are: to be able at all times to ensure its own security, to respond to the expectations of its partners and allies, and to contribute to maintaining peace in the world.

It is France's vocation because it falls under its responsibility as permanent member of the U.N. Security Council.

It is France's vocation because, as a founding member of the European Union, it is promoting peace between nations.

It is France's vocation because throughout its history, it has acquired a military and diplomatic capability that it places at the service of international law.

France lives up to its commitments and will not lower its guard. This is why we must understand the political importance of our President's decision to maintain the defense budget of France at the same level as in 2013—179.2 billion euros in the next military planning law.

Why Did France Intervene in Mali?

It is this vocation and sense of responsibility that have led France to intervene in Mali. Why?

- Because a friendly country that was represented by his legitimate President asked us for help.
- Because there was a terrorist threat that could subject Mali to a dangerous hold.
- Because there was obviously a risk for the whole Sahel region, and also for Europe, and our discovery of hundreds of tons of weapons confirmed the soundness of our initial analysis.

France intervened first because we were the only country with military means that was able to act immediately alongside our African friends.

We did not intervene on behalf of the Africans, but with the Africans. We mobilized collectively within Europe to launch a European training mission—the European Union Training Mission in Mali (EUTM Mali). This mission is making it possible to start a U.N. stabilization operation under conditions of both international legitimacy and efficiency.

Although our military staff will be reduced, we will remain in Mali and in the region because we are not done yet with terrorism. At one time or other, our fight against terrorism must also involve all the countries that share our values, particularly in Africa where we need to show our solidarity and our help and support to West African countries that are victims of the scourge of terrorism. We will keep doing this.

The Need to Work Together

The recent military operations have shown us once again that we must work together, within the framework of the European Union, in order to be in a position to respond to all the crises.

That is why France wants to open a new phase in the construction of a European Defense ("l'Europe de la défense"). Several factors are leading us there.

The shared necessity of restoring our public finances encourages us to pool our capacities, to take more initiatives and to base our efforts upon equipment made in cooperation, taking into consideration the know-how of each country.

This is what France is already doing with the United Kingdom, in particular to build a Combined Joint Expeditionary Force (CJEF), or "force expéditionnaire conjointe et combinée."

This is also what France wishes to do with Germany, including for military operations abroad. In the same way, France will develop its partnerships with Belgium, Italy or Spain and will involve the new members of the European Union in this approach, beginning with Poland and the Visegrád countries because the European Defense must include all of Europe, in ad hoc frameworks that make sense in practical terms.

France will make proposals to that effect before the European Council in December 2013. These proposals will address our presence in the Balkans, in the Mediterranean, in the Middle East and in Asia. In all these places, Europe must act in a more coordinated manner. Is it reflecting with enough boldness on what we could do better and perhaps at a lower cost?

These proposals will also address our cooperation programs in the fields of air transport, observation satellites, air-to-air refueling, the use of drones, just to mention a few examples.

We should not be discouraged by past difficulties; on the contrary, they should be an incentive to carry on. Our ambition is to promote European supporters for our European defense industry. This is vital if we are to maintain a competitive industrial and technological base.

The big issue for Europe is not simply to have a large market and a stable monetary zone—these are necessary conditions. It is also to have an industrial policy and with this industrial policy comes the defense challenge.

France is part of Europe but, as a founding member of the Alliance, it is also active in the NATO framework. Our President has recently confirmed our participation in the integrated military command of the Atlantic Alliance. France participates fully in allied actions and at the same time, it intends to play its role in the construction of the European defense. There is no contradiction there. On the contrary, we are propping up our defense on its two natural pillars: the Atlantic one and the European one.

Acting Together to Restore and Maintain Peace

The legitimacy of our policies is based on dialogue, both bilateral and multilateral. Talking about the Cold War, Raymond Aron once said that it was an "era of improbable war and impossible peace." I remain convinced that, if wars and crises are still possible—and recent events in our immediate environment unfortunately confirm this—peace and development are nonetheless an imperative requirement. Given the reinforcement of defense cooperation, our common responsibility, i.e., the responsibility of France and that of the other nations that are represented here, is to stimulate our exchanges as a way to turn the risks of conflicts into reassurances, and to prevent and contain destabilization factors; if circumstances warrant, it is also to act together using the force of arms to restore and maintain peace. There is no doubt that the International Workshop on Global Security can contribute to that goal.

Welcoming Remarks

Lieutenant General Jean-Marc Duquesne
Director, Institute for Higher Defense Studies (IHEDN)

Good morning and welcome to the Invalides. This is a place of history and heritage. It is with great pleasure and as director of the Institut des hautes études de défense nationale that I welcome today for the fourth time in Paris the *International Workshop on Global Security* at the invitation of the Minister of Defense, Mr. Jean-Yves Le Drian. And you know now from the media why he is not here today: the necessity of a visit to Afghanistan.

The IHEDN is co-organizing this Parisian edition of the seminar with Roger Weissinger-Baylon, Chairman and founder of the Center for Strategic Decision Research. Let me say a few words to explain the special nature of IHEDN. It is an inter-ministerial civilian and military platform that gathers and trains at national and regional levels and also a tool dedicated to European and international responsibility. This year we are honored to welcome seventy-five participants including fifteen ministers or deputy ministers of defense or foreign affairs, ambassadors and high-ranking generals representing in all twenty-six nations. During this 30th edition of the International Workshop on Global Security, you will be brainstorming for two days on the subjects of peace and security and the challenges of the future. This comes at a time when many organizations are rethinking the future—such as the EU, which is organizing a European Council in December 2013 dedicated to defense and security, or NATO, whose 2014 Summit will lay the foundation of a post-Afghanistan NATO. All this demonstrates how crucial it is to reflect upon the challenges of the future and especially the near future.

I wish you a fruitful and constructive seminar.

Overview: Avoiding Future “Pearl Harbors”

Dr. Roger Weissinger-Baylon,Workshop Chairman
Anne D. Baylon, Editor

At the invitation of French Defense Minister Jean-Yves le Drian, in partnership with the Institut des hautes études de défense nationale (IHEDN)—a high-level research institute within the purview of the Prime Minister—and with additional support from the French Senate and the Military Governor of Paris, this year’s 30th International Workshop was presented in France for the fourth time. The sessions were held in the Invalides, one of France’s most prestigious national monuments. Our discussions took place in the King’s Council Chamber under the portraits of King Louis XIV, who built the Invalides, and Emperor Napoleon III.

As Estonia’s Minister Jaak Aaviksoo remarked, these were men of action who waged numerous wars. The Invalides’ museum testifies to this, displaying a number of highly precise scale models of the fortified cities of the time, some are several dozen square meters in size. Once state secrets, these models were important instruments of the military campaigns of Louis XIV. Unfortunately, wars are costly and always risky. In fact, the Franco-Prussian War and the Battle of Sedan cost Napoleon III his empire.

Almost exactly one hundred years after the end of Napoleon III’s empire, during what we now recognize as the twilight of the Cold War, the international workshop series was founded to better understand and contribute to decision-making on security issues, bringing together senior diplomats, military leaders, and their governments. Since the international workshops now encompass three decades of meetings and discussions, it is appropriate to consider what lessons—or questions—might be drawn from this experience.

THREE DECADES OF WORKSHOPS: A FEW REFLECTIONS

Ending the Cold War

Our first annual workshops took place during the Cold War, a period that French Deputy Defense Minister Kader Arif[1] described in his keynote address as an “era of improbable war and impossible peace.” At that time, the stakes were undeniably greater than they had been under Louis XIV: the workshops’ focus was on the Cold War’s nuclear threat from the Soviet Union and its potential to obliterate human civilization. The specter of East German and Russian tanks surging through the Fulda Gap also loomed, as Ambassador Larry Butler[2] mentioned. Instead of studying intricate models of fortified cities as in the time of Louis XIV, the workshop presentations featured complex simulations involving multi-pronged attacks of tank armies storming from the East while exchanging nuclear fire with similarly-armed Allied forces seeking to block or slow their advances. Such scenarios envisioned the nuclear annihilation of large parts of Germany and even much of Europe.

This prospect was avoided due to the effectiveness of deterrence, a degree of prudence on both sides, and—it now appears—a certain element of luck. Fortunately, leaders such as Gorbachev, Thatcher, and Reagan acted to bring the Cold War to an end. Thanks to their foresight, in August 2014 we will mark the 25th anniversary of the fall of the Berlin Wall. Yet the Cold War might have ended earlier. During one of the first workshops at Schæffergården in Denmark, former Supreme Allied Commander Europe General Bernard Rogers stated that while serving as SACEUR, his Warsaw Pact counterpart had approached him to discuss “between generals” how to accomplish what political leaders eventually achieved much later. Unfortunately, the North Atlantic Council did not allow General Rogers to respond. Looking back at these events, one wonders whether an important opportunity for an earlier peace with the USSR was lost.

Opening the Door to Eastern Europe

Eventually, peace did come; Russian troops began to withdraw from Eastern Europe and the citizens of these countries

[1] Arif, Kader. *Keynote Address and Welcome*. pp. xxxv-xxxviii. The phrase is from French philosopher and journalist Raymond Aron.
[2] Butler, Lawrence. *Transatlantic Security’s New Normal.* Chapter 15. pp. 41-44.

could at last aspire to a future of freedom and prosperity. Before then, as Poland's Undersecretary of State Boguslaw Winid[3] reminded us, "To be a member of NATO was a seemingly impossible dream." Yet President Lech Walesa (and, subsequently, his successor President Aleksander Kwasniewski) invited the workshop to Warsaw, where the NATO flag flew for the first time. Czech President Vaclav Havel welcomed the workshop at Prague Castle the following year. An Austrian workshop in the Habsburg Palace followed, and the next year the workshop was opened in the Hungarian Parliament. During this historic period, two successive SACEURs, General John Shalikashvili and especially General George Joulwan, played key roles—and, in a certain sense, helped realize the earlier dreams of General Rogers.

Relations with Russia: Getting it Right

Eventually the workshop came to Moscow, where Russians were already suffering from the rapid privatization of state assets, trade liberalization, and the removal of government subsidies and price controls—an extreme version of neoliberal "shock therapy." As a result, a majority of state assets fell into the hands of a handful of people, mostly tied to President Yeltsin, while millions of Russians were reduced to poverty. Simply put, Russia's rapid transformation by "shock therapy" was a tragedy and not just an economic one. After seeing the way democracy and neoliberal capitalism arrived hand-in-hand, Russian citizens are likely to remain distrustful of democracy for some time. This period also set the stage for today's Russia, in which wealth and power remain in the hands of a narrow elite.

The relationship with Russia, and getting it right, is a priority for global security. The NATO-Russia Council can play a key role in re-establishing this relationship. In a follow-up meeting with Russia's Ambassador to NATO Alexander Grushko a few months after the Invalides workshop, Ambassador Grushko described two issues that are key for the relationship: missile defense and Syria. Since NATO's Deputy Secretary General Alexander Vershbow[4] has invited Russia to work with NATO on missile defense, there may be an opportunity for progress, at least in this area.

Facing up to Free Market Limitations as well as Inequality of Income, Information, and Opportunity

The underlying raison d'être of any security policy must be to protect the economic prosperity, health, and personal well-being of citizens. As Spain's Secretary General of for Defense Policy Ambassador Alejandro Alvargonzález San Martín[5] stated, "Security is the essential foundation for the development and progress of a free society." Yet, many nations are pursuing economic paths that can be viewed as much milder versions of the policies that did so much harm in Russia. Worse, these policies are sometimes accompanied by economic austerity programs that further depress the economy.

Consequently, the economic and other benefits are increasingly enjoyed by only small segments of the population, leading to an unacceptable degree of income inequality. In his Evangelii Gaudium, Pope Francis expresses deep concern for free market theories, which— while bringing prosperity to those at the upper end of the economic spectrum—tend to marginalize those at the lower end:

> "…some people continue to defend trickle-down theories which assume that economic growth, encouraged by a free market, will inevitably succeed in bringing about greater justice and inclusiveness in the world. This opinion…expresses a crude and naïve trust in the goodness of those wielding economic power and in the sacralized workings of the prevailing economic system."[6]

Extreme inequalities are now firmly established in income, information, and even health. Many are also experiencing inequality of opportunity—which may be one of the cruelest forms of inequality since it diminishes hope for a better life. Finally, interest groups have become so powerful that they have not only "captured" government agencies, but, as Transparency International reports, in some cases have captured entire governments.

As a result of this challenging economic situation, NATO members are finding it difficult to respond to NATO Deputy Secretary General Alexander Vershbow's plea for larger defense budgets that would share the costs more fairly with their U.S. partner. In particular, European governments are under pressure from citizens to address what citizens see as the key issues: social programs and—especially—jobs. As Minister Aaviksoo[7] mentioned, citizens often do not see defense invest-

[3] Winid, Bogusław. *Polish Security and Defense Policy: the Story of Success.* Chap 12. pg. 33.

[4] Vershbow, Alexander. *Challenges Facing NATO and the Transatlantic Community Post-2014.* Chap. 1. pp. 3-6.

[5] Alvargonzález San Martín, Alejandro. *The Spanish Security Position toward the Mediterranean*. Chap. 21. pg. 59.

[6] Pope Francis. *Evangelii Gaudium.* Chap. 2. I. No. 54. 2013.

[7] Aaviksoo, Jaak. *Dealing with Chaos, Risk, and the Cyber Threat.* Chap. 24. pg. 69.

ment as vital, particularly given the need for greater social or economic investment. For example, populations in countries that are not immediate neighbors of Syria do not see its spreading civil war as a threat. Similarly, those in countries far from Iraq, Afghanistan, or any of the other rapidly spreading conflicts in the Middle East or Africa are also unlikely to feel threatened.

Finally, extreme income inequality has been one of the driving forces behind the Arab Awakening (and a number of other crises across the globe). As NATO's Dr. Stefanie Babst[8] mentioned, "GDPs across the Levant are among the lowest in the world, growth rates are meager, income inequality is high, as is unemployment—ranging between 18% and 30% in Egypt, Tunisia, Jordan, and Morocco." In other instances, states with high income inequality are projecting instability beyond their borders: e.g. Israel (with its harsh treatment of Palestinians), Qatar (which finances radical mosques in countries including France), Saudi Arabia (which has spread its conservative Wahhabism to Afghanistan and Pakistan), and of course Pakistan (which helped create and long supported the Taliban). At least in these cases, the effects of income inequality may be further magnified when religion radicalizes the least favored elements of the population.

The Cyber Security Threat

Ireland's Minister for Justice, Equality, and Defense Alan Shatter[9] cites annual losses due to cybercrime of $388 billion. Yet, after reviewing a draft of these workshop Proceedings, one senior diplomat suggested that cyber security will not be addressed fully until some kind of digital "Pearl Harbor" event occurs. If there is doubt as to the urgency of dealing with such threats, the recent hacking at Target stores of the credit card information for 70 million customers should be a motivation to take the financial risks seriously.

While governments and international organizations are focusing on protecting their own networks and critical infrastructures and while large cyber security companies are focusing on marketing their best technologies to large corporations, cyber criminals are shifting their attacks to smaller organizations and individuals since they are the most vulnerable. At the same time, as MITRE's Major General David Senty[10] warns, "hacking is no longer an entertainment activity. It is now an industry focused on gaining information or financial access to systems." In fact, the profits of cyber criminals have grown so large that some groups are able to acquire world-class technical capabilities that equal (or exceed) those of top researchers at such places as M.I.T. or the California Institute of Technology. While Orange's Francis Bruckmann[11] reports that "the most frequent attacks—which are also increasing in number—are distributed denial of service attacks (DDOS)," more sophisticated attacks are also pervasive. Meanwhile, in the military sphere, Czech First Deputy Minister of Defense Daniel Kostoval[12] points out that there is "an emerging consensus that cyber space—just like land, sea, and air—is another space that must be included in Article 5 operations or scenarios."

Once again, there is an opportunity—and a responsibility—to address these challenges. One of the most important "next steps" is to improve international cooperation. Patrick Pailloux,[13] who heads ANSSI—the French government's cyber security body—stresses that "European and international cooperation is vital…because most large companies are international." Thus, it would make little sense for France to impose restrictions on an international company that would only apply to its operations in France.

In any case, for such efforts to be effective, further legislation will likely be necessary. France is making good strides in this realm. As Patrick Pailloux explains:

- …the first thing that we will change is to give the state the ability to set rules that operators will have to follow.
- The second idea…is to oblige operators to report to the government if they suffer an attack…
- The third idea is [to grant the government] the authority to verify the security level of [operators'] systems…
- The last idea concerns times of crisis. It establishes a legal basis…to oblige operators to take some difficult actions.

While sizeable budgets are increasingly being allocated to cyber war, some officials suggest it would be more effective

[8] Babst, Stefanie. *Syria, Iraq, and the Middle East.* Chap. 18. pg. 51.

[9] Shatter, Alan. *Key Security Challenges Facing the EU—Cyber Crime.* Chap. 2. pg. 8. While this $388 billion estimate is widely cited by government officials in both the U.S. and Europe, it is extremely difficult to gauge the actual level of cybercrime losses. In fact, figures as high as $1 trillion are sometimes given.

[10] Senty, David. *Towards Effective Cyber Security—A New Strategy.* Chap. 23. pg. 65.

[11] Bruckmann, Francis. *Orange and Cyber Security.* Chap. 15. pg. 72.

[12] Kostoval, Daniel. *Deterrence and Stability in the 21st Century.* Chap. 13. pg. 37.

[13] Pailloux, Patrick. *Dealing with the Challenge of Cyber Security: The French Government's Approach.* Chap. 29. pg. 83.

to instead use some of those funds to defend our society as a whole, and not merely our governments or other large and so-called essential elements. The stakes are high and any delay will be costly.

As Dr. Frederick Douzet,[14] who holds IHEDN's CASTEX Chair in Cyber Security, points out, in Europe the public discussion following the Snowden revelations raises important questions, including "the balance or imbalance between security and civil liberties" as well as the issue of political oversight. While government officials, especially in the U.S. and the U.K. have been extremely critical of Snowden, others consider him to be a whistle blower who has provided information of enormous value concerning a "runaway intelligence community"[15] that needs far stronger oversight.

Building International Trust and Cooperation

As for the cyber threat, global security depends on broad international trust and cooperation, which only time and effort can develop. In an address at National Defense University, SACEUR General Philip Breedlove[16] emphasized that "you cannot surge trust and engagement." And, in his Invalides workshop presentation this year, Central Command's Deputy Commander Vice Admiral Mark Fox[17] echoed these thoughts, stating that "we must be engaged and present to influence the situation...'virtual presence' is actual absence. We can surge troops and equipment, but we can't surge trust." These remarks by senior U.S. military leaders are significant since their government's policies, particularly the Sequester, have made international travel (and even domestic travel) difficult. This makes building relationships and enhancing supranational cooperation much harder for U.S. officials.

While "presence" is necessary, as Admiral Fox remarked, it is not enough to develop trust among countries: language and other skills are also necessary. At one of our first workshops in Berlin, Germany's then-Defense Minister Rudolf Scharping commented that the high cost of international educational exchanges for high school and college students was a major challenge for international security. If young people cannot afford to live and study in another country, they cannot learn languages; without languages, they cannot truly understand cultures and people; and, without developing this understanding—together with the strong personal ties formed by living in a country—real trust and cooperation is difficult to achieve. Germany is clearly one of the countries that understands the importance of language skills. The United States? Not so much. Among NATO countries, perhaps the most striking example is the so-called Five Eyes program, which shares intelligence only among five English-speaking countries and not with other NATO partners or allies.

THOUGHTS FOR THE NATO SUMMIT

With NATO's next summit announced for September 2014, attention is already turning to the important issues that must be addressed. Near the top of the list will be the key issues of burden-sharing within the transatlantic community, Smart Defense, Connected Forces, Pooling and Sharing[18] (very important given the budget constraints), strengthening the NATO-EU relationship,[19] and missile defense. Other likely contenders are the growing influence of China and cyber security. Since many of these goals depend on the economic strength of NATO member countries, Italy's former Foreign Minister and former Vice President of the European Commission Franco Frattini[20] suggests a new "transatlantic economic common space," which would be based on President Obama's proposed EU-U.S. trade agreement, as a complement to NATO.

Of course, one of the biggest issues may be NATO's future role post-Afghanistan, which NATO's "out-of-theater" commander General Hans-Lothar Domröse[21] calls "the largest military operation in modern history, with currently 50 troop-contributing nations." Most likely, there will be a long stream of crises post-Afghanistan that will require NATO's military capabilities. According to the U.K.'s Minister for International Security Strategy Dr. Andrew Murrison,[22] "events

[14] Douzet, Frédèrick. *Cyber Security: The U.S.-China Relationship*. Chap. 27. pg. 78.

[15] Editorial Board of the New York Times. *Edward Snowden, Whistle Blower."* The New York Times. pg. A18. 2 Jan 2014.

[16] Cited in Arnas, Neyla. *Coalitions, Partnerships, and Foresight: Why They Matter.* Chap. 37. pg. 99.

[17] Fox, Mark. *The Middle East: A Military Perspective.* Chapter 20. pg. 58.

[18] Vargha, Tamás. *Doing More with Less—The Management of Defense under Austerity.* Chap. 14. pg. 40. As State Secretary Vargha points out, multinational cooperation "does not necessarily lead to savings, but it does lead to delivering capabilities more effectively."

[19] Arif, Kader. *Op cit.* pg. 24. According to Minister Arif, France is working within the framework of the EU to create a Combined Joint Expeditionary Force (CJEF) with the UK. France hopes to establish a similar partnership with Germany and potentially other countries as well.

[20] Frattini, Franco. *Global Security: A New Vision for the Transatlantic Partnership.* Chap. 4. pg. 16.

[21] Domröse, Hans-Lothar. *NATO Operations in Afghanistan.* Chap. 16. pg. 45.

[22] Murrison, Andrew. *Defending Europe: A British Perspective.* Chap. 3. pg. 14.

across North Africa and the Sahel, in Syria, the Levant and in the Gulf show that Europe is exposed to an arc of instability that reaches to its doorstep." The U.S. European Command's Civilian Deputy Ambassador Lawrence Butler[23] says, "The proximity of the Levant, with the Syrian civil war and its nearly 100,000 victims and lots and lots of chemical weapons, ought to keep European leaders up at night. Instability in the Maghreb leads to terrorism and mass migration." General Bertrand Ract-Madoux,[24] the French Army Chief of Staff, gives the conflict in Mali as an example of the kinds of situations that will require future attention.

Even so, it will not be good for NATO if such future actions turn out to be coalitions of the willing in which NATO merely plays a supporting role.[25] Were this to happen (it does seem unlikely), there are concerns that NATO might evolve into an organization primarily centered on training forces of member countries. Or, it could even become a sort of high-level security think tank. A more likely suggestion is that NATO will assume a more global mission, possibly centered on its many Partner countries.

All countries need to understand that the enemy is no longer just in the form of a military force. In the words of Minister Murrison,[26] threats are typically "international terrorism; cyber security; organized crime….that respect no borders and possess no sovereignty." Most citizens, however, face other threats, too. These may include natural disasters such as floods, earthquakes, typhoons, or epidemics. More often, however, the greatest threats to their well-being are extreme inequalities of income, information, and opportunity, or other economic distortions. One of the underlying causes of insecurity, including acts of violence, is injustice. Again, according to Pope Francis:

> "…until exclusion and inequality in society and between peoples are reversed, it will be impossible to eliminate violence…without equal opportunities the different forms of aggression and conflict will find a fertile terrain for growth and eventually explode."[27]

Addressing these underlying moral and ethical issues may be one of the best ways to prevent another "Pearl Harbor," whether it be a cyber attack or a kinetic one.

[23] Butler, Lawrence. *Op cit.* pg. 42.
[24] Ract-Madoux, Bertrand. *Defending Global Security—The Role of the French Army.* Chap. 5. pg. 18.
[25] Søndergaard, Carsten. *The Way Ahead: A Danish View.* Chap. 33. pg. 91.
[26] Murrison, Andrew. *Op cit.* pg. 11.
[27] Pope Francis. *Op cit.*

Acknowledgements

Dr. Roger Weissinger-Baylon, Workshop Chairman
Anne Baylon, M.A., Editor

We would like to thank the workshop participants, speakers and sponsoring organizations—and the many others—who made the 30th International Workshop on Global Security possible. Their contributions were more important than ever this year, since economic constraints affected nearly every country. Moreover, the "sequester" and subsequent government shutdown made it unusually challenging for U.S. officials to participate.

French Ministry of Defense. French Vice Minister of Defense Kader Arif gave a keynote address—on behalf of Defense Minister Jean-Yves Le Drian, who invited the workshop to Paris in his role as Workshop Patron. (Minister Le Drian had to travel unexpectedly to Qatar with President François Hollande.) Lieutenant General Jean-Marc Duquesne, Director of the Institute for Higher Defense Studies (IHEDN), gave opening remarks since IHEDN was our partner again this year for key aspects of the workshop's organization. IHEDN's Deputy Director, Ingénieur Général Robert Ranquet, was especially helpful and we thank him wamly, as well as Ambassador Michel Foucher and Dr. Frédérick Douzet. We appreciate the support of the Military Governor of the Invalides, Lieutenant General Hervé Charpentier; and we are grateful to the Defense Ministry for making the "Grand Salon" of the Invalides available for all of the workshop sessions and for providing bus transportation, translation equipment and many other services.

French Sénat. Senator Gérard Longuet, who previously hosted the workshop in Paris in his then role as Defense Minister, invited us to a post-workshop breakfast and private visit of the Senate.

Workshop Speakers. Deputy Secretary General Alexander Vershbow gave the major opening address. He asked for Europeans to assume a larger share of NATO costs, while emphasizing the need for additional capabilities (reconnaissance and surveillance assets, or strategic lift aircraft). He highlighted the importance of Smart Defense, Connected Forces, missile defense, and cyber security. Other key opening speakers included Irish Minister for Justice and Defense Alan Shatter, British Minister for International Security Strategy Dr. Andrew Murrison, and Minister Franco Frattini, former Vice President of the European Commission and former Minister of Foreign Affairs of Italy. The Chief of the French Army General Staff, General Bertrand Ract-Madoux, discussed France's recent intervention in Mali.

IHEDN's Ambassador Michel Foucher then chaired a major panel on the Balkan and Black Sea region with the Defense Minister of Georgia Irakli Alasania, the Deputy Prime Minister of Montenegro Igor Lukšić, the Defense Minister of Bosnia and Herzegovina Zekerijah Osmic, and the Defense Minister of Macedonia Talat Xhaferi. This panel was of special interest because of the need to integrate the countries of this vital region into NATO and the European Union. Other high level panels included perceptions from the Visegrád countries with Polish Deputy Minister of Foreign Affairs Ambassador Bogusław Winid, Czech First Deputy Minister of Defense Daniel Kostoval, and Hungarian State Secretary of Defense Tamas Vargha.

The key political-military challenges of Afghanistan and Irak were addressed by two panels: First, NATO's Allied Joint Force Commander Brunssum General Hans-Lothar Domröse led a panel with Ambassador Lawrence Butler, the Civilian Deputy Commander of U.S. European Command, and Afghanistan's Ambassador to France Dr. Assad Omer. This was followed by Dr. Stefanie Babst's panel, with U.S. Vice Admiral Mark Fox, Iraq's Ambassador to France Fareed Yasseen, and Spain's Secretary General of Defense Policy Ambassador Alejandro Alvargonzález San Martín. The participation of Vice Admiral Mark Fox, the U.S. Navy's Deputy Chief of Operations and Strategy and now the Deputy Commander of U.S. Central Command, was especially valuable.

Some of the most important sessions were on cyber security, which featured MITRE's Major General David Senty, the former Chief of Staff of the U.S. Cyber Command; Estonian Minister of Research (and former Minister of Defense) Dr. Jaak Aaviksoo; Mr. Patrick Pailloux, who heads cyber defense for the French government within the office of the Prime Minister; and Rear Admiral Arnaud Coustillière, who is the Flag officer for cyber security in the Defense Ministry. These panels highlighted the cyber threats and the need to respond. As a result of the strong conclusions of this panel, it is expected that cyber security will be one of the main themes of our next workshop in 2014.

The final wrap-up panel was chaired by Ambassador Carsten Søndergaard, Denmark's Ambassador to NATO, with Canadian Ambassador to NATO Yves Brodeur, and Japanese Ambassador to France Ichiro Komatsu.

North Atlantic Treaty Organization. In addition to the officials already mentioned, we also appreciated the contributions of Ambassador Khazar Ibrahim, Vice Admiral Robert Davidson, Vice Admiral Marc Ectors, Lieutenant General Stefan Oprea, and Major General Michel Yakovleff. In 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.

United States Department of Defense. We would like to acknowledge the continuted 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. The National Defense University and Dr. Lin Wells, Center for Technology and Policy Research, have long supported the workshop; Ms. Neyla Arnas, Senior Research Fellow, Center for Technology and Policy Research, transcribed and edited some of the papers in this book and contributed the book's final chapter.

Northrop Grumman. Again this year, Northrop-Grumman has been our most important industry sponsor and we gratefully acknowledge the support of Mr. William Ennis, Director International Programs and Mr. Jim Moseman, Director, Europe and NATO, Northrop Grumman International.

Orange. Given the growing importance of Cyber Security at the workshop, it is most appropriate that Orange, the global telecommunications operator, supported the workshop for the first time. We especially appreciate the help of General Jean-Luc Moliner, Director of Group Security, and Mr. Francis Bruckmann, Deputy Director of Corporate Security, for supporting the workshop and providing financial sponsorship.

MITRE. The MITRE Corporation has sponsored the workshop for three decades. We greatly appreciate 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.

Tiversa. Tiversa sponsored the workshop for the first time this year, with the participation of Mr. Robert Boback, CEO, and Mr. Tim Hall, Chief Technical Officer. Their sponsorship is especially appreciated.

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 second time. Mr. Braccioli gave an important address concerning the deep web.

URS Federal Services. At URS Federal Services, Mr. David Swindle, Executive Vice President, was an important contributor and sponsor again this year, together with Sir Kevin Tebbit, KCM, CMG, former Permanent Secretary of Defense of the United Kingdom.

Juniper Networks. Through Mr. Jon Arnold, Director, U.K. Government and Defense, Juniper was a sponsor for the first time. Mr. Arnold addressed the final workshop breakfast at the French Senat.

Key supporters. Among the other cyber security experts were Mr. Jim Cowie, Co-Founder and CTO, Renesys; Prof. Dr. Holger Mey, Head of Advanced Concepts, Cassidian; and Mr. Jean-François Sebastian, Director, Public Sector, as well as Mr. Thomas Gann, both at McAfee/Intel. Major General Cai Jihua, Senior Advisor, represented the China Institute for International Strategic Studies (CIISS) within the Chinese Foreign Ministry.

Other French officials. Additional French officials included Admiral Jean Bétermier, President of Forum du Futur; Mme. 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 Mme. Dahlia Kownator, who was very helpful in relations with the French telecommunications and cyber security industry.

Workshop Staff. With her usual efficiency Caroline Baylon assembled an impressive and highly qualified staff that managed all aspects of the workshop organization. She is now Research Associate in Science, Technology and Cyber Security at the Royal Institute of International Affairs in London (Chatham House). Again this year, Jean Lee was a wonderful graphics expert and photographer whose beautiful work is published in this book. At the time of the workshop, Dr. Ania Garlitski, a cardiologist, was Assistant Professor of Medicine at Tufts University. Joining us for the first time this year were Adriana Balducci, who is now teaching at Sciences Po in Paris, Cecile Vié, and Jules Lecomte.

We would like to give special thanks to Mr. Tim Bloechl, Mr. Robert Rodriguez, Ms. Neyla Arnas, and Brigadier General Christine Turner who were extremely gracious with their help. Finally, we would like to acknowledge in a special way the efforts of Ing. General Robert Ranquet, since he has played a unique role in each of our five Paris Workshops.

Menlo Park, California Paris, France
December, 2013

Peace and Security:
The Challenges Ahead

Chapter 1

Challenges Facing NATO and the Transatlantic Community Post-2014

Ambassador Alexander Vershbow
NATO Deputy Secretary General

Let me start by saying how happy I am to be joining you at this year's Workshop. Although the setting is a bit more elegant than what we're used to at NATO headquarters, I feel very much at home here. Back in 2000, when I was U.S. Ambassador to NATO, I spoke to the Workshop about prospects for Missile Defense, a topic that has become even more topical since then. Three years later, when you held your first Workshop in Moscow, I had the privilege as U.S. Ambassador of talking about global security challenges in the 21st century.

Today, I again find myself looking to the future, because I want to address the "Challenges facing NATO and the Transatlantic Community post-2014." Why have I chosen that date? Quite simply, because it will be a major inflection point for the Alliance.

Our world today is very different from the one in which NATO was founded, well over six decades ago. During that period NATO has had to reinvent itself several times—after the Berlin Wall came down, in the wake of 9/11—and it has always done so successfully.

NATO's Future Missions—and the Need for a New Transatlantic Balance in Contributions

This time, however, the challenge is very different because the next adjustment will require that the Alliance achieve a new balance in the contributions made on the two sides of the Atlantic. To put it bluntly, it will require the Europeans to do more—both individually and collectively—at a time when financial conditions are bleak on both sides of the Atlantic.

It is for this reason that Secretary General Rasmussen and I have warmly welcomed France's new White Paper on Security and Defense, the Livre Blanc. It lays out clearly and succinctly the challenges that lie ahead for France, and it identifies a clear and pragmatic path to address them. I believe this can provide lessons for many other European nations and for the Alliance itself.

2014 represents a key date for NATO because it is the year when we will end our combat mission in Afghanistan. Just last week, we reached an important milestone in that mission when President Karzai announced that Afghan security forces will now take the lead for security across the whole country. Afghan forces are already showing that they have the capacity and the professionalism to plan and conduct operations and to take the fight to the Taliban. As a result, ISAF will shift from a combat role to a support role, and we are on track to complete our mission at the end of next year as planned.

We are already preparing a new, smaller mission to train, advise and assist the Afghan security forces beyond 2014. And while I have no doubt NATO will undertake other operations and missions in the future, their size and duration is likely to decrease. Post-2014, our operational tempo is likely to reduce, and that will require a change in focus for the Alliance.

Instead of being deployed on operations, we will need to be prepared for operations and other contingencies. We will need to find new ways to maintain the readiness and interoperability that we have gained during nearly two decades of operations in the Balkans, Afghanistan, Libya, and other theatres.

Let me hasten to add that, while NATO's operational tempo is likely to reduce, the transatlantic need for NATO certainly won't. The risks and threats we face will not miraculously disappear. As a transatlantic community, we will still need a full-spectrum capability ready to deal with the whole spectrum of possible threats to our interests and our security, whether in our own neighborhood or beyond.

The United States will still look to Europe as its partner of choice. Europe will still need the United States to help it conduct some of the more demanding and complex military operations. And the United States and Europe, as a community of nations united by common values and a shared history, will look to each other to defend and promote those values in an increasingly complex, globalized world.

For all these reasons, the transatlantic community will still need NATO. And NATO will need to be ready. We cannot afford to pause or take a rest after a successful transition in Afghanistan!

NATO Needs the Right Operational Capabilities

So what must NATO do to retain and sustain its operational edge, and to ensure that it is operationally ready? First and foremost, it needs the right capabilities.

Last week, at the Air Show at Le Bourget, many of the types of capability we need were on public display. What was not so publicly displayed was the price of acquiring them. As we continue to struggle with the consequences of the financial crisis and its adverse impact on Allied defense budgets, acquiring the high-tech, high-cost equipment we need will be a major challenge.

If the Alliance is to have available the essential capabilities it needs—such as reconnaissance and surveillance assets, or strategic lift aircraft—then it is clear that many individual nations will be hard-pressed to provide them on their own. It is only by working together—multinationally—that nations will be able to afford such capabilities.

The Role of Smart Defense and Connected Forces

That is the logic behind a number of initiatives we are currently pursuing at NATO. In terms of equipment and logistical support, our Smart Defense initiative encourages multinational cooperation—it can be European or Transatlantic. The Franco-British Lancaster treaty, as well as regional cooperation arrangements such as the Visegrád and Weimar groups, or the Nordic Defense Cooperation group (NORDEFCO), are all excellent examples of the Smart Defense way of working. And these initiatives are already bearing fruit.

We have agreed on around 30 multinational projects—in such diverse areas as protection against improvised explosive devices, and reconnaissance and surveillance—and more are in the pipeline. And we are working closely with the European Defense Agency to ensure that our respective work is fully coherent and complementary.

Similarly, when it comes to retaining the ability to conduct demanding operations, multinational training is key. We saw that in Libya but also in Mali. Even though the French-led operation was outside NATO, it was the Alliance's multinational standards that enabled Allied and partner nations to connect their contributions together, quickly and efficiently. Here again, through our Connected Forces Initiative, we are encouraging nations to exercise their forces together on a more regular basis post-2014 so that we can maintain the readiness and interoperability gained in recent years through operations.

Taken together, these two initiatives—Smart Defense and Connected Forces—underpin the development of what our leaders, at last year's Chicago Summit, called "NATO Forces 2020"—the modern, tightly connected forces we need that are equipped, trained, exercised and commanded so that they can operate together, and with partners, in any environment.

Striking a Better Balance

At the same time, these initiatives will also create the conditions to address the other fundamental issue for the Alliance post-2014, namely, burden-sharing. Complaints about burden-sharing are as old as the Alliance itself, but this time they can't be swept under the carpet.

Currently, too many key operational capabilities have to be provided by the United States—as we saw during our Libya operation in 2011, and as France saw during its Mali operation this year. This over-reliance on American asset—surveillance drones, aerial refueling tankers, heavy transport planes, electronic warfare capabilities—is unsustainable in the long term, especially as the U.S. rebalances to Asia and grapples with fiscal challenges of its own. Multinational approaches will be key for getting a bigger bang from our defense Euros, and also for helping Europe deliver more of the key capabilities that we need as an Alliance.

But it is not just within NATO that nations can help to redress this balance. There is a clear role, too, for nations within the European Union, because there is also an over-reliance on a few key nations within Europe. The European Council meeting dedicated to security and defense at the end of the year is an excellent opportunity for nations to make concrete commitments to do more to boost European military capabilities. With 21(and soon, 22) nations members of both the

EU and NATO, a stronger “Europe de la défense” is also a benefit to Euro-Atlantic security. In addition, the December meeting is an ideal occasion to promote greater cooperation among our defense companies so that we can sustain a strong defense industrial base on both sides of the Atlantic.

Alongside well equipped and well trained deployable forces, NATO also needs to develop new capabilities to deal with the new threats we face—such as ballistic missile proliferation and cyber threats.

NATO’s Ballistic Missile Defense

As far as protection against potential attacks from missiles is concerned, we are already making good progress. Just over a year ago, in Chicago, we declared an Interim Capability for our NATO missile defense. This protects our Allies in Southern Europe. Within a few years, we will expand the system to include missile defense interceptors in Romania and Poland, and achieve Full Operational Capability for NATO’s command and control system. This will then ensure the full coverage and protection for all NATO European populations, territory and forces that our leaders pledged to provide three years ago.

We continue to work on making sure that Allies are able, at all times, to exercise full political control, while allowing for swift military action when necessary. And we are constantly assessing the potential threats on a regular basis, so that we can adapt our missile defense plans if necessary.

There are two very important points I would wish to make about missile defense. First, there is a clear and agreed understanding among Allies that missile defense can complement the deterrent role of nuclear weapons, but not replace those weapons.

And second, our work has been, and will remain, true transatlantic teamwork. Many different assets are being brought together with sizeable U.S. assets to deliver a common, integrated and shared NATO capability. Several European nations are providing Patriot units, and others are adding missile defense radars to their ships. France’s plans to develop an early-warning capability and long-range radar will play an important part in our overall system.

In sum, our work on missile defense demonstrates a strong commitment, on both sides of the Atlantic, to address this particular emerging security challenge.

Dealing with the Cyber Threat

Another emerging security challenge we are addressing is the cyber threat. Earlier this month, our Defense Ministers had a first, thorough discussion of cyber defense. Protecting our own computer networks is NATO’s primary task. But that is the minimum I believe we should aim for. Indeed, I would argue that our ability to defend against cyber attacks will be central to NATO’s role as a collective defense alliance in the coming years, especially given the fact that cyber attacks could have consequences for our societies on the scale of armed attacks.

For this reason, I would like to see NATO do more. For example, we could share best practices among Allies. We could coordinate with the European Union and other organizations on the standards necessary for protecting national infrastructure. And we could develop ways to help Allies who request assistance in strengthening their cyber defenses or mitigating the effects of cyber attacks if they occur.

Relations with Partner Nations

So far, I have focused my remarks on forces and capabilities. But a second vital element to NATO’s ability to provide security in the coming years is its ability to project stability beyond its borders. Key to carrying out this role will be NATO’s relations with its partner nations.

In recent years, our partnerships have been most visible when it comes to NATO operations. Indeed, it is quite extraordinary to think of the dozens of nations—from Europe, the Middle East, the Asia-Pacific region, and even South America—that have put their soldiers in harm’s way under NATO command in the Balkans, Afghanistan and Libya. This has added capability—and political legitimacy—to our operations. We intend to retain this by offering partners the chance to join our Connected Forces Initiative so that, like us, they can stay operationally ready and able to operate alongside Allied forces.

But the original purpose—and the enduring purpose—of our partnerships has been to promote reforms and enable the development of strong security institutions so that partners can become sources of stability in their own regions.

This approach was particularly successful in Central and Eastern Europe, as well as in the Western Balkans, in the framework of Partnership for Peace. In fact, it was so successful that many of our former partners are now valued Allies in NATO and members of the European Union.

As we look beyond 2014, we need to identify where—and how—NATO's partnership experience can help other countries cope with the difficult transition to democracy. In this regard, I see particular scope for NATO to assist partner countries in the Middle East and Northern Africa, where the Arab Awakening has brought new opportunities, but also new uncertainties.

Indeed, many countries in this region—on NATO's doorstep—are undergoing changes as dramatic as those that Eastern Europe experienced at the end of the Cold War. Although the situations are very different, NATO's expertise could be very helpful to Middle Eastern countries in transition in several ways: helping them to modernize their security sectors; training their forces to cope with internal challenges; or enabling them to operate together with their neighbors' militaries to manage crises together. (In this regard, NATO could complement and reinforce the capacity building efforts of the EU.)

We are already looking into a request by the Libyan Prime Minister for NATO to provide advice in the development of Libya's national security forces, in tandem with ongoing efforts by the EU, the U.N. and individual nations. I believe more of our southern neighbours could benefit from NATO's experience and expertise. Down the road, NATO might also be able to assist regional organizations—such as the African Union or the Arab League—as they seek to assume greater responsibility for regional peacekeeping and crisis management.

Concluding Remarks—Syria and Russia

In this context, let me say a few words on Syria. We all want to see a quick political resolution of this crisis, and a transition to a new leadership that can gain the support of the Syrian people. NATO has no plans to get involved beyond the steps we have taken to protect Turkey. But once the fighting is over, there will need to be a strong international effort to get the country back on its feet. The U.N. will likely be in the lead, but I believe NATO nations—and perhaps NATO itself—should be prepared to play their part.

I have tried to give you some food for thought on how NATO should meet the security challenges of the coming years. As we look to the future, we must, at the same time, protect the investments we have made in recent years. This includes continued support for a peaceful, stable, and multi-ethnic Kosovo. It includes continuing efforts to counter terrorism, curb piracy, and prevent the proliferation of weapons of mass destruction. And it includes, above all, staying engaged in Afghanistan so that it can secure and govern itself and never again become a haven for terrorists.

One area where NATO has made considerable investment is in our relationship with Russia. But here, I have to be honest and say that the return has not been as substantial as we would have wished. Russia has provided some valuable assistance in countering terrorism and in support of the ISAF mission in Afghanistan. We want to build on that as we seek to bring lasting stability to Afghanistan and the wider region post-2014.

But I also hope that we can do more to tap the full potential of the NATO-Russia partnership. In this regard, all of us at NATO believe that cooperation on missile defense could be a real game-changer for our relationship with Russia. We both face the same dangers from the proliferation of missile technologies and WMD to states like Iran and North Korea. It makes eminent sense—for political, practical and military reasons—to combine our missile defense capabilities and thereby protect our territories and populations more effectively.

Moreover, by building a cooperative missile defense system, Russia could see—from the inside—what our leaders have said at the highest level: that NATO's missile defense system is not directed at Russia and is incapable of undermining Russia's strategic deterrent. Missile defense would, in short, transform the NATO-Russia partnership, and bring greater stability and security to the entire Euro-Atlantic area.

I have laid out for you the work that NATO and the transatlantic community need to undertake as they look beyond 2014. And I could not have found a better place to do that.

Paris was NATO's first permanent home. In the last few years, France has resumed its full place in NATO—and, as the recent Védrine report concluded, this is good news both for France and for NATO.

This International Workshop on Global Security has, over 30 years, established a reputation for supporting NATO and the transatlantic relationship. It is an ambitious agenda I have laid out. But with your help, it is an agenda I am confident we can achieve.

Chapter 2

Key Security Challenges Facing the EU–Cyber Crime

Minister Alan Shatter TD
Minister for Justice, Equality and Defence of Ireland

The international security environment has changed profoundly in recent decades in a way that requires a new, more co-ordinated response to emerging threats. If we wish to safeguard the security of individual Member States and that of the Union, then active and positive engagement is required by all concerned in the EU's Common Security and Defence Policy.

In the rapidly changing world in which we now live, our values and interests are being continually challenged. The European Security Strategy (ESS) clearly sets out the threats and challenges we face in the global security environment: transnational terrorism, organised crime, cyber-crime, proliferation in weapons of mass destruction, regional conflicts, failing States, climate change, energy insecurity, population migration, trafficking in drugs and people, in particular women and children, and piracy. All of these are real and substantial threats to the security of individual EU Member States. One of the key priorities of the Irish Government is to provide for the defence and security of our own people in Ireland while contributing through multilateral action to international peace and security.

Dealing with Blurred Divisions between Domestic and International Security

It is striking that in our globalised world these threats, while not necessarily new, have become more difficult to address and more interrelated. Traditionally, domestic and international security issues were addressed separately by different security actors. Police and law enforcement agencies primarily dealt with domestic issues, while diplomats and military dealt with international security issues. The traditional divide between domestic and international security threats, and the challenges they present, has become increasingly blurred. The experience being felt by all EU Member States is that threats like terrorism, uncontrolled migration, cyber attacks and people and drug trafficking have blurred the internal and external dimensions of security. The European Security Strategy emphasises the truth that today's threats and challenges are not purely military and are not resolvable by purely military means. Each requires a mix of modalities, expertises, instruments and responses.

Over the past years, the EU has and continues to develop an overarching/comprehensive approach to tackling security issues. This is being done through establishing closer coordination and cooperation between the EU and international institutions and actors, primarily dealing with internal and external security issues.

I firmly believe that collaboration among States to meet these challenges self-evidently serves a common interest. From my unique vantage point as Minister for both Defence and Justice, I readily acknowledge that the approach of the EU is a soundly practical one. All Member States face the same security threats so it is imperative that all Member States, together with the relevant institutions and organisations, work together to find ways to negate or mitigate the adverse impact of these threats.

Throughout Ireland's Presidency of the European Council, I have, in various foras, discussed the issue of security challenges and threats that we, as a Union, are facing. At a recent Presidency seminar on Maritime Security and Surveillance held in Dublin, I highlighted the importance of building EU-wide consensus and cooperation in relation to security and surveillance in the maritime domain. In my address I acknowledged the many threats and challenges in the Union's maritime domain and noted that these have the potential to impact adversely on the security and safety of the Union as a whole and on our citizens and economies. I am of the opinion that the security and safety on our oceans and seas is extremely important to the Union, both as a key world trading block reliant on safe and secure sea-lanes for commerce and trade, and also in terms of our own internal security. To understand the risks, challenges and vulnerabilities that we face in this regard, it is necessary to have a full picture of what is happening at sea—an integrated maritime picture.

I have also addressed other areas where I believe there is a requirement for us to have a full picture of what is happening within the EU and outside, and between various security actors. There are many other areas where, I believe, opportunities exist to develop synergies between civilian and military operations, and research and development. A particular area of interest in this regard is Cyber.

As I have previously said, I am in the unique position as Minister for both Defence and Justice. This means that I attend the Justice and Home Affairs meetings as well as Defence meetings. At these meetings Defence Ministers discuss cyber security and also Justice Ministers discuss cyber security, but there does not appear to be a discussion ongoing between Defence and Justice Ministers. Cyber security is an area that imposes existential and internal threats, in the context of European Union States, both with regard to terrorism, with regard to protecting industry, with regard to protecting essential utilities and Government information that is of a confidential nature and that is important. I believe, and this is totally a personal view, that there is a need now for expanded dialogue between the Defence and Justice sides in the European Union on the issue of Cyber Security and Defence. I perceive it as an issue that requires greater connectivity and less fragmentation and it is an important issue in the area of the EU's Common Security and Defence Policy.

Over the past years, the use of information and communications technology has escalated. Technology now impacts on all aspects of our lives. The private and public sectors across the globe have become increasingly dependent on digital information systems and infrastructures. Therefore, access to secure and free flowing information is more crucial today than it has ever been. It is true to say that technologies, such as the Internet, mobiles phones, iPads etc., when used in a productive way, have the power to transform economies and provide all of us with instant, borderless access to information. However, the technologies when used in a destructive or a malicious manner equally have the power to cause untold damage to our economy, but also on our safety, security and health.

Cyber Security Depends on Broad Cooperation

Cyber security is a complex issue that requires cooperation across all sectors to ensure the safety of our networks and infrastructures. As our dependence on technology has grown, research has revealed that there has been an increase in cyber crimes/incidents, which I am sure many of you are very aware of. Symantec, the makers of Norton antivirus and anti-spyware software, released a report in 2011 which contained statistics on cybercrime. According to this report, threats to cyberspace have increased dramatically afflicting 431 million adult victims globally—or 14 adult victims every second—over one million cybercrime victims every day. The total bill for cybercrime footed by online adults in 24 countries topped $388 billion between 2010 and 2011. At $388 billion, cybercrime is more than 100 times the annual expenditure of UNICEF. Also, as has been noted by the United Nations Economic and Social Council "Cybercrime has now become a business which exceeds a trillion dollars a year in online fraud, identity theft, and lost intellectual property, affecting millions of people around the world, as well as countless businesses and the Governments of every nation." In comparison, it is estimated that piracy off the Horn of Africa costs in the region of $6 billion and our reaction to that has been to launch a robust military mission to deal with this crisis.

I believe it is self evident that the cyber security threat is not going away. With this in mind, and at my request, as part of our Presidency Programme, the Irish Presidency hosted a seminar in Brussels last week, in association with the Estonian Ministry of Defence and the European Defence Agency. This seminar dealt with the issue of Cyber Security Co-operation in the European Union. The objective of the seminar was to advance the debate on Cyber Security and the capacity of European Union Member States to counter cyber threats at national level and across the EU as a whole. This is an important discussion which has implications for Governmental administration, for industry, for our economic well-being and for the security and safety of our citizens.

As I said at the seminar, cyber threats are asymmetric by their very nature, because attacks can be perpetrated by the few upon the many, with little cost and limited resources. Cyber attacks are typically anonymous, launched from any one of billions of sources worldwide. Impacts may be immediate and obvious, or dormant and subtle, eluding recognition for years. Degrees of damage can range from inconvenient downtime of personal systems to the life-threatening interference with or destruction of critical infrastructures.

The range of actors taking part in cyber-attacks is increasing. These perpetrators may seek financial gain or they may have a more ideological reason. Even over the past month I have noted a significant escalation in the frequency and indeed the seriousness of these attacks.

Over the course of the last few weeks we have had the United States and China engaged in controversy over cyber attacks by hackers with links to the Chinese military. It is becoming increasingly apparent that State actors are the most capable threat, as they have the ability to funnel significant resources and talents into these efforts, and see cyber attacks as an appropriate countermeasure to what they perceive as a threat. State actors can have several motivations for conducting cyber attacks, ranging from economic espionage or political blackmail to the desire for a military advantage in the form of asymmetric warfare. State actors can deem cyber warfare to be a vital national interest and put the full force of Government resources behind it.

We all recognise the importance of cyber security. However, I think it is appropriate to say that the challenge is how we, as Ministers, policy makers and the private sector, can collectively develop a multi-lateral and multi-dimensional approach to address the challenges the we face in cyber security from a technical, operational and policy perspective.

The European Union's Approach to Cyber Crime and Attacks

In acknowledging the growing dependence globally on the information network, and indeed the steady increase in cyber crime/attacks, I welcome the publication of the European Commission's Cyber Security Strategy, entitled "An Open, Safe and Secure Cyber-space." This is the first comprehensive policy document that the European Union has produced in this area, which aims to improve security and indeed resilience of network and information systems, fight cybercrime, and facilitate an adequate response to cyber disruption. It comprises internal market, justice and home affairs and Foreign Policy angles of cyberspace issues. The Strategy is also accompanied by the technical legislative proposal by the European Commission's Directorate General Connect, to strengthen the security of information systems in the EU. Also, progress in advancing co-operation, in addressing the cyber crime, was made at the recent G8 Summit where the United States and Russia signed a landmark agreement to reduce the risk of conflict in cyberspace. This agreement will involve the sharing of real-time communications about incidents of national security between both parties—this is certainly a step in the right direction.

But it is not enough to publish a Cyber Security Strategy or to enter into agreements—in our fight against cyber crime it is incumbent upon all of us to fully support implementation of these strategies and agreements. To fail to co-operate in the area of Cyber would be to undermine our collective security and to fail to understand the escalating threat that we face. We are stronger together and safer together. With that in mind, let's ensure that we also work collaboratively together.

Clearly, it is the case that no one organisation or State has the capacity to address the cyber security issue alone and that this is a shared multi-faceted responsibility at national and EU level. This is clearly recognised within the EU, with the acceptance of the need to develop and implement a comprehensive approach at EU level for cyber security. The EU approach to this issue must advance our efforts to promote international cooperation in cyber security as well as promote effective and improved cyber security across the EU and beyond.

To successfully counter this emerging cyber threat, cooperation between national law enforcement, defence, and technical incident response organisations, within and between Member States, needs to be encouraged. This is essential to enable us to identify and exploit potential and existing synergies. We need to recognise the broad cross-sectoral nature of cyber matters and the need to provide for individual freedoms. But, we also need to provide safeguards for interdependent networks and information structures and to protect the cyber domain. For this reason we need a comprehensive approach to cyber security. We need to build on existing models of international cooperation to make cyberspace more stable and more secure. To minimise the risks of successful cyber attacks, we need everyone from EU institutions, Government, industry partners, academia and individual citizens to do their part.

The European Council on Defence meeting in December will provide the Union, for the first time in four years, with the opportunity to address defence related issues at the highest political level. While the fiscal and sovereign debt crisis has necessarily been the primary focus for Heads of State and Government over the past few years, we now have the opportunity, prior to the European Council meeting, to discuss and agree on the key defence issues that should be prioritised at this meeting. I am of the opinion that cyber security must be one of the key priority issues to be discussed.

To conclude, let me say again that it is incumbent on us all to take personal responsibility and collective responsibility to address this crucial and critical issue.

Chapter 3

Defending Europe: a British Perspective

Dr. Andrew Murrison MP
U.K. Minister for International Security Strategy

Introduction

I am delighted to be here in these most opulent of surroundings in a building founded by Louis XIV who—I think it is fair to say—knew a thing or two about statesmanship and warfare. Fortunately, Europe is more tranquil today and today's politicians discuss collective security and common defence against external threats rather than hatch plots against each other. Today, I want to lay out the U.K.'s perspective on some of the issues relating to our collective security, particularly focussing on the European context.

Britain and Europe's Place in an Interconnected World

The U.K.'s view of this subject is coloured by our history. We have long-standing global interests, based on historic ties, international trade and continuing commitments—including to our Overseas Territories. To protect these interests we have to maintain global influence and global reach. But we understand that the world is changing:

- The global financial crisis has imposed fiscal constraints on many countries;
- Emerging nations are altering the balance of power in many regions;
- The advent of new technologies is changing the way we do business;
- The world is more multipolar and our economies and cultures are more integrated than ever before.

The U.K., its traditional allies and new partners must all adapt to this new reality. But how best to respond?

- Well, many of the security threats we face today have a common theme: international terrorism; cyber security; organised crime. These are all threats that respect no borders and possess no sovereignty;
- But, of course, we must also continue to prepare for threats posed by other states;
- Capabilities and intents can change, and we must be postured to deal with emerging adversaries.

The only effective way to tackle all of these threats is to work collaboratively with other nations—particularly when you consider the resource constraints under which we are all operating. No nation can afford to maintain all possible capabilities to deal with all possible eventualities. So we are compelled to work together.

Multilateral Frameworks

I don't think that anyone here would disagree with the need to cooperate in Defence. But there are different opinions on how best to cooperate, especially on the issue of security in this continent, our continent.

For the U.K., it is about the defence of Europe, not European defence. There is a subtle, but important distinction. It means we are committed—first and foremost—to developing the military capabilities of European nations—contributing to our overall security, burden sharing and operations. But we are not committed to building new military structures and organisations within European institutions.

Wars are not won by organisation charts and wiring diagrams. They are won by well-trained personnel, using the best equipment, given the right support, and operating under effective command. Defence and security are too important to be subordinated to the designs of Europe's political engineers.

This is not to say that we eschew multilateral cooperation, far from it. Indeed, we are its greatest advocates, we have been doing it for years and we helped to build many of the institutions that form its foundations. But in Defence, multilateral cooperation must be underpinned by investment, deployable capabilities and, crucially, the political will to use them.

NATO as the cornerstone of the U.K. Defence strategy. This is one of the reasons that NATO remains the cornerstone of our Defence strategy. It must not be challenged or put at risk by a competing European Union defence identity. NATO is the most powerful military alliance in the world and it has demonstrated enduring relevance through operations in the Balkans, Afghanistan, Libya and the Mediterranean. The Alliance has delivered high-end war fighting capabilities in short time frames and in very challenging circumstances. For these tasks, it is tested and it is effective, and for the U.K., it will always be our first port of call during crises that require this kind of response.

We believe that developing parallel structures in other institutions is above all inefficient, but also risky and unnecessary. But, the provision of our collective security is a very complex issue and it requires a wide range of capabilities and approaches. NATO may be the guts of our toolkit, but it is only one tool.

The creation of the National Security Council as an integrated approach. Sometimes you need a power tool, but on other occasions something with a softer edge is more appropriate. Very few scenarios that threaten our security in the 21st century can be solved by military means alone. We have recognised this nationally through the creation of our National Security Council, which brings together our Department for International Development, our Ministry of Defence, our Treasury, our Intelligence agencies and our Foreign and Commonwealth Office, under the chairmanship of our Prime Minister.

The National Security Council drove forward our National Security Strategy and our Strategic Defence and Security Review. And it continues to drive forward many of our national responses to situations that affect Britain's security, providing an integrated approach that draws on all the instruments of government.

Multinational integrated approach. We understand that this integrated approach is also very valuable at the multinational level, bringing co-ordination to the work of partner nations. That is why we are committed to our involvement in the EU's Common Security and Defence Policy (CSDP) operations, including Althea in Bosnia, counter-piracy operations and training missions in Somalia, and Mali, where we have made a major effort to support these important French-led activities. And it is why we fully support the EU Battle Group concept, looking forward to being the framework nation starting on July 1st. We recognise the significant potential for CSDP to deliver security through a comprehensive approach, and we think the EU Battle Group could be more involved in this activity.

For us, NATO and CSDP must be partners, not rivals. Their respective capabilities should complement, not duplicate. We would like to see a renewed focus on an outward looking CSDP agenda because Europe cannot afford to be introspective about its security. The global nature of the threats we face means that we cannot expect to protect our citizens merely by patrolling our own borders.

Willingness to deploy. European nations in the EU and NATO must invest in deployable capabilities and be prepared to engage in expeditionary operations, tackling threats upstream where necessary, focussing particularly on those regions close to Europe's near abroad. In many cases, an intervention sooner involving hundreds may prevent an intervention later involving thousands.

This means cost effectiveness and earlier and more effective resolutions. Having the will and the capabilities to deploy beyond our national borders when necessary is vital to conflict prevention and all European nations must accept their responsibilities for this work, whether in capacity building, training, peacekeeping or peace-enforcing roles.

Bilateral Partnerships and Working in Smaller Groups

Developing international networks. In addition to the willingness to deploy, European nations must also develop international networks to allow them to operate alongside regional partners. Many of us have historic relationships with countries across the world. Collectively, our network of bilateral Defence relationships is a force multiplier, enabling us to build consensus, gain local knowledge and use regional infrastructure.

The need to develop this reach was a key principle behind our International Defence Engagement Strategy, which we published earlier this year. It brings coherence to our Defence Engagement efforts and ensures that our bilateral relationships support our multilateral engagement.

In the last three years Britain has signed five new Defence treaties and around 50 MOUs with countries in all regions:

- In the Gulf, for example, we have nearly 300 members of our Armed Forces permanently deployed on non-operational tasks, including resident Defence Attachés in all Gulf states.

- In Asia, we will be opening three new Defence Sections in our embassies this year.
- In Africa, we continue to work closely with all our partners, including the new government of Somalia to help it rebuild vital national security forces.

Developing bilateral defence relationships. But we are also working hard to deepen our bilateral Defence relationships with our European partners. The Lancaster House Treaties with France indicate that we are building a key strategic partnership committed to nuclear deterrent, expeditionary reach and maintaining capabilities, whilst reducing procurement costs. We are entirely clear that our bilateral cooperation with France does not undermine NATO, but very much strengthens it.

The Combined Joint Expeditionary Force (CJEF) we have formed with the French will provide us with an early-entry combined force capable of conducting complex interventions. This versatile capability will enable us to respond to the widest range of threats to our security. The CJEF will form a powerful embodiment of the Lancaster House Treaty and is on track to be available in 2016 for bilateral, NATO, EU, U.N. or other coalition operations.

Cooperation in smaller groups is quicker, easier and often achieves more. The Benelux countries, the Nordic Defence Cooperation (NORDEFCO) and our cooperation under the Lancaster House Treaty are good examples of close collaboration between like-minded partners, which build NATO's capability.

Often it makes sense for bilateral cooperation to focus on specialist areas where there is already a track record of collaboration. A good example of this is the U.K.-Netherlands Amphibious Force, a truly interoperable capability with embedded officers, compatible equipment and regular joint training exercises. In May in Rotterdam, Dutch Defence Minister Jeanine Hennis-Plasschaert and I marked 40 years of Anglo-Dutch amphibiosity, a great example of how like-minded nations can add value to defence by working together.

I predict that examples like this—partners within NATO and the EU collaborating closely on a multi or bilateral basis—will be an increasingly prominent part of defence and security in this continent. This kind of cooperation is 'Smart Defence' or 'Pooling and Sharing' in action. Developing these combined capabilities in small groups, in a co-ordinated fashion across Europe, can create a tapestry of capabilities that can be used for various roles.

Europe as a leader in NATO. It is important that European Allies take more of the lead in NATO, especially on issues of reform and providing security within our own spheres of influence. America has been one of Europe's most steadfast allies. But faced with its own fiscal pressures, and with its attention increasingly and rightly drawn to the Asia Pacific region, Washington is setting us the challenge of addressing deficiencies in European nations' capabilities—asking us to act as producers, not consumers of security. The U.S. is not omnipotent, and we cannot expect them to continue to write us a blank cheque when it comes to our collective security.

Conclusion

Europe has been at peace for nearly 70 years. The Berlin Wall was torn down nearly a quarter of a century ago. Conflict at scale in Europe is now unconscionable and, for some, external threats to European security seem distant and unlikely. But events across North Africa and the Sahel, in Syria, the Levant and in the Gulf show that Europe is exposed to an arc of instability that reaches to its doorstep.

If we want to be able to respond to these threats and shape the solution to crises, we must be able to draw upon capable and deployable Armed Forces as part of our overall response. This means the willingness to make the right level of investment, the willingness to collaborate in a coordinated fashion and the willingness to deploy our personnel and expose them to risk.

A failure to do this will leave us all merely shouting from the sidelines of world events. Yet, if we get this right, we have a real opportunity. Working together, we can save our taxpayers' money and increase our collective security—goals we can all agree on.

Chapter 4

Global Security: a New Vision for the Transatlantic Partnership

Minister Franco Frattini
Former Minister of Foreign Affairs of Italy
Former Vice President of the European Commission

Security and foreign policy are the main fields where political guidance and strong political leadership are needed. These fields impact the core of national sovereignty; and defending citizens and their security is and should remain a top priority for all democratic governments. So, on the one hand, states in NATO and in the EU should not run the risk of underestimating serious, multifaceted, and asymmetric threats to all of us in the rapidly changing world. On the other hand, by showing leadership and better public communication capacities, states and multinational organizations should explain that money spent for preventing and facing threats is not wasted but invested for the good of our citizens.

Multilateral Cooperation

The first political key principle is multilateral cooperation. For NATO, it is clear that, in the near future, the financial burden for capabilities should be shared reasonably between European and American allies. And for us Europeans, we need to work harder toward complementarity rather than duplication by making full use of the existing Pooling and Sharing and Smart Defence initiatives. So, rather than cutting national defence budgets horizontally, we need political decision on better spending with a focus on some priorities.

"Soft Power" Is Not Enough

In general terms, EU allies should avoid considering that simply representing a "soft power" would be enough to play the European indispensable role as security provider. We cannot run the risk to be seen as the "soft power" appendix to the strong U.S. security producer.

In times of economic crisis, NATO's most important political goal for the future is to involve its EU partners better by encouraging coordinated political choices on where we can cut ("static" spending, or areas that are not "interoperable") and, on the contrary, where we need new and fresh investments (new technologies, or cyber security). Another goal is how to organise a better division of labour among Allies.

Resources Must Be Pooled Effectively

In particular, we indicated areas where we have started to pool resources (common projects on smart munitions, surveillance/reconnaissance, military satellite communications) and areas where we already share capabilities (air policing or air refuelling, in which Italy actively participates); these areas of closer cooperation are proving to be quite successful.

In order to guarantee access to common capabilities, important initiatives are being discussed within NATO and EU Allies. But once a national political decision has been made, a key issue is how to guarantee that each member of the Alliance actually provides a predetermined capability after it has received notice that this is required. In my view, a first step should be a political and national strategic decision where the government of each state involves its parliament; after that, it would make the commitment to keep a given asset available for the Alliance once and for all, except in the case where a new opposite strategic political decision would be taken.

A second, necessary step is to agree among the Allies who would be responsible for somehow "certifying" what is made available and by whom. Even though this is not an easy issue, I think NATO and the European Defence Agency should have a key role to play.

Understandably, some partners are reluctant. But so far, the system to use common assets was based on capabilities' redundancies or deficiencies. And this is what we will have to change by moving towards transparency, efficiency, optimization, and also refraining from discouraging further investments on the needed assets.

If we want to adapt to the evolving global security context, another issue at stake is how to better cooperate with private industrial sectors on defence and security. A first step is to improve our procurement systems, particularly among EU Allies, where fragmentation and duplication cases largely exceed collaborative programs. Now, we should think of a Pooling and Sharing production alongside procurement. The existing fragmentation duplicates production and leads to different standards of equipment, thus hindering the development of logistic support systems; it also weakens military interoperability.

Again, in order to improve private-public cooperation, Europeans should quickly implement an EU common market on defence, after the adoption of important EU directives and the strengthening of the EU Defence Agency, that would go exactly in that direction.

Partnerships

One of the most important strategic imperatives for our Alliance is to build a globalised, flexible and quickly reachable network of partnerships. This is equally important for European and American allies for several good reasons: First, major threats come from outside the "transatlantic space"; so, we need reliable partners that are strong players in the regions where these threats originate. Second, we have to protect "common goods"—from cyber-security to sea lanes of communication or energy supply routes to the stabilization of failing and failed States. There, Allies and partners have these goods in common, and so a common strategy is needed.

We know well that NATO and its members cannot be "fighters for the good" everywhere in the world, especially in times of economic crisis. So, with Asia and the Pacific or Africa and the broader Middle East in mind, we need to rely heavily on partners to globalize together our response to the crises. In the near future, NATO should evolve toward a stronger partner involvement, first by enabling partners to become stronger providers of security: targeted education, training and mentoring projects should be key elements of this strategy. This would permit members and partners to develop together a better comprehensive interoperability that would benefit initiatives like the NATO response force, where rapid and coordinated action is needed. For example, we still do not have shared standards on cyber security and prevention measures.

Cooperation with partners on counterterrorism and counter-intelligence should be deepened, starting with a more comprehensive approach for Special Forces' cooperation. Since a prevention strategy became and will become more and more crucial, we could involve partners in each region of the world of interest to NATO in the "threat assessment," also encouraging regional organisations to participate. This would provide the Alliance with a more comprehensive and also regionally–based evaluation of a given situation of threat or crisis.

On the involvement of partners, the Alliance should count and rely on the experience and the added value represented by member states themselves, in particular Europeans, when it comes to some priority regions, namely the Mediterranean, Middle East or North Africa. In this framework, Europeans are a crucial pillar of the Alliance again to indicate and develop with their neighbours and partners a comprehensive approach to conflict prevention as well as post conflict strategies.

A New Transatlantic Bargain

I think there are some promising perspectives and a common awareness on the re-launching of our transatlantic community, which was born and has always been based on common values:

- A new transatlantic community with a broader concept on the one hand—a new transatlantic security bargain where Europeans and Americans share the burden and the opportunity to be both providers and not just consumers of security.
- On the other hand, a transatlantic new economic common space, starting from the visionary perspective opened by President Obama's proposal to negotiate a EU-U.S. trade agreement.

A highly political complementarity exists between these two pillars since both (a) require political choices and vision, (b) require mutual trust, (c) have an economic impact.

Vision and preparedness are more effective and less expensive than reaction in case of crisis. This is why, in times of crisis and of multiplication of global players, a broader Euro-Atlantic cooperation is more necessary than ever.

Chapter 5

Defending Global Security—the Role of the French Army

General of the Army Bertrand Ract-Madoux
Chief of Staff of the French Army

I am very glad to be here with you in the Honor Room of the Invalides. When King Louis XIV ordered the building of this edifice, which was intended to care for the soldiers wounded at war, the first patients used to come to this room to pray and meditate. In the XVIIIth century, it became a council room before being transformed into a library by Napoléon.

It is thus a place that has been dedicated to introspection and reflection, and I hope it will inspire your debates as you keep in mind those who continue to fight as well as those who are victims of wars.

In that respect I would like to mention the battle of Solférino, which took place precisely 154 years ago on June 24, 1859. The public reaction to the horrible suffering of the wounded prompted the foundation of the International Committee of the Red Cross as well as the signature of the first Geneva Convention.

The Role of the Armed Forces in Defense of Global Security

The defense of global security is a major stake for the future. Along with diplomacy, the armed forces play a most prominent part in preventing crises and solving them when the situation requires it. Being able to rely on a reactive and efficient military tool that can create favorable conditions to restore stability and open discussions is therefore of paramount importance. The Malian crisis offers an interesting analysis framework to discuss the contribution of the armed forces to the preservation of global security.

As you know, 2013 is marked by a strong commitment of France to international peace. The involvement of France materializes its determination to guarantee its own security but also its will to participate in stability in the most sensitive regions of the world. Remaining faithful to its vocation, our country fulfills its responsibilities. The current geopolitical context shows the extent to which the instability of the world makes this duty unavoidable. In the White Paper, France repeats its determination not to depart from it.

Our defense tool fully participates in this ambition. The deployment of French military forces in the Indian Ocean, in Sahelian and Subsaharan Africa, on the shores of the Western Mediterranean or in Southeast Asia is significant. This military engagement cannot be envisaged without the legitimacy and lawfulness granted by the United Nations and the enforcement of treaties uniting France to friendly countries. It is most often exerted alongside our allies and partners, within the structured framework provided by the North Atlantic Treaty Organization or the European Union because France does not envisage acting alone.

In most cases, in the face of the drift caused by bankrupt states or states that are too weak to defend themselves and provide assistance to threatened populations, military intervention is obviously the best solution to this urgent situation. As a recognized military power, France maintains a credible intervention capability to be implemented by a prepared and equipped force, ready to be projected, on its own initiative or in a multinational framework.

The whole of the French military components brings a significant contribution to stabilization and crisis management operations. However, the engagement of ground units is obviously common to these types of missions which take place nearly exclusively on the ground, for and among the populations. Indeed, the deployment of land forces, in sufficient numbers and on a long-lasting basis, best guarantees the achievement of political objectives and the restoration of a stable security situation. We know how important time is to reconcile the belligerents, rebuild a state and lay the foundations for durable development. Troops on the ground know how to accompany these slow transitions. They know it, because they have progressively acquired the experience of how to integrate their actions into those of the international agencies within a comprehensive approach, combining security reinforcement, restoration of governance, and development. They also know how to maintain a secure environment by quelling the acute crises which unavoidably emerge during these sometimes very long transformation processes. Lastly, they are able to maintain, before withdrawing, a reassuring and discrete presence in order to accompany the last steps of recovery. In that respect, thinking that it is possible to resolve crises without putting "boots on the ground" is sheer utopianism. The successive and unavoidable steps between the intervention, stabilization, then normalization phases cannot be taken without the land forces. The Libyan example convinces us of this reality. The absence of international troops on the ground—in response to a requirement made by the national Libyan Transitional Council—was harmful to the stabilization process and the process of securing territory by the authorities. We know that the porosity of the borders and the dissemination of armament stockpiles resulting from it feed regional instability.

I think that the Malian crisis, owing both to its sudden and brutal aspect, is a good example of the future challenges that will be met in the field of collective security. At the same time, the analysis of the response given on the spot through a military intervention opens some avenues for reflections and some perspectives which I think are worth sharing with you. The military intervention perfectly integrated into a global strategy conceived very early and quickly implemented by the international community through the resolutions of the United Nations, the initiatives of the European Union and the Economic Community of West African States (ECOWAS). Resorting to the Armed Forces thus seems to have created the prerequisite and indispensable conditions for the renewal of dialogue and restoration of a constitutional state.

The Mali Crisis—My View as Chief of the French Army

I thus want to share with you my view on this operation as Chief of the Army. Though the mission has not ended yet and our troops are still engaged, it is in my opinion already possible to draw some key lessons and to identify the factors which made this operation possible.

No military intervention should be triggered without the support of the international community. The resolutions adopted by the United Nations Security Council as of the summer of 2012 regarding the Malian crisis have laid the foundations for the legitimacy of an international reaction. The enforcement by France of the provisions of the United Nations Charter, which holds that it is possible to give a military response to a country asking for help and acting in self-defense, has ensured the lawfulness of its intervention. Lastly, the immediate announcement by the French authorities of its military objectives made it possible to clearly define the end-state and the limits of this action. The wide international consensus, built around a shared understanding of the situation and a common vision regarding the assets is one of the key elements of the rapidity of the intervention.

This rapidity is of paramount importance for two reasons. First, it grants credibility to the states which decide to intervene. Indeed, the international public opinion, the belligerents, the opponents and the partners can measure the level of collective political determination by the reactivity of the engagement. But the speed of reaction is above all key to the efficiency of the intervention. Without its dazzling speed, the French response, which was ordered and triggered in the hours immediately following the Jihadist attack, might have produced its effects too late. The reactivity of the engagement is based on several factors I am now going to address.

- First, it is vital to have a short military-political decision-making loop in order to decide quickly, as well as a reactive operational and strategic command system, able to have the political will enforced and executed quickly on the ground. In the case of Mali, five hours elapsed between the presidential decision to block the movement of the extremist groups and the first strikes on the ground. The high stakes and complexity of the situation required the ability to control the operation as soon as it was triggered. The command assets in France and in Africa immediately permitted us to ensure this control through a precise follow-up of the situation. Since the beginning of the operation, the Commander-in-Chief of the Armed forces, the Minister of Defense and the Chief of Defense have been and are still informed in real-time of the ground developments.
- Secondly, it is indispensable to own the assets to intervene rapidly. The French Armed Forces have in this case two major assets. In the areas of priority interest for France, prepositioned forces are stationed in several military bases throughout Africa and in the Arab-Persian Gulf. They comprise sufficient joint capabilities to deploy a first emergency intervention echelon and to provide the adapted logistic and command structures. It is mainly from two of them, located in Chad and the Ivory Coast, that the first French units converged toward Mali on January 11, 2013 in order to block the terrorist offensive and secure French and foreign nationals. Then, the French Armed Forces have a joint immediate reaction force. It is an emergency echelon, deployable within seven days and comprising special forces, a Land task force and a Naval task force constituted around a command and projection ship, an air detachment, and the

associated command and control assets. On January 13, 2013 the first ground units of this reaction force complemented the initial set up composed of the prepositioned forces. All these assets made it possible, within 12 days, to deploy 2,600 French military troops in Mali. There were more than 4,000 troops at the peak of the operation.

- Lastly, the deployment required numerous logistic transportation assets such that they quickly exceeded the sole capabilities of the French forces. Without the air support provided extremely quickly by 11 friendly countries, not only would the deployment have been less quick, but the continuation of military operations would not have been possible under the same conditions. Without a doubt, their contributions illustrate the state of mind in which this intervention has been positively perceived by the international community and how much easier it has been to lead the intervention thanks to that.

The violation of the sovereignty of Mali by AQIM and its Jihadist allies necessitated an immediate reaction to put an end to it. The restoration of the Malian territorial integrity required, in a second phase, to repel the attackers in order to reconquer the North of Mali. It is a critical phase from a military point of view since, at that time, the deployed force no longer enjoyed the surprise effect induced by its unexpected intervention. Moreover, it was facing an enemy who knew the terrain and had decided to entrench in its own safe heavens to fight at all costs. The development of this "reconquest" phase went well for several reasons.

The French armed forces are permanently engaged in large numbers of theatres of operations characterized by the variety of the environments and the diversity of frameworks of engagement. The brutal events in the Sahel that triggered the intervention there demonstrate this clearly. Indeed, Mali has shown to be exceptional in every respect since it has nothing in common with other areas of engagement. It imposed very difficult conditions of engagement on our deployed forces, because of the hemmed-in position of the country, the distances, the extreme weather conditions, the peculiarities of the terrain and, lastly, the fierce determination of the adversary.

The uncertainty weighing on the places of possible engagement shows imperatively that the forces must be versatile. De facto, this operation has shown the relevance of the capability choices made by France to maintain its capabilities in the field of intelligence and special forces in particular. The will to keep the entire spectrum of joint capabilities and to preserve an appropriate balance between light, medium and heavy forces, reinforces the versatility of our defense tool which is thus able to commit to all types of operations, ranging from normalization operations to the most violent coercion operations on nearly all types of terrains. Operation Serval has highlighted the relevance of these choices, especially the one consisting of keeping an airborne component. This set of capabilities ensures that France has a certain level of autonomy of decision regarding the design and conduct of operations. The liberation of the towns of Timbuktu, Gao and Tessalit was obtained through a combined action including armored assets on the ground and airborne operations under air cover.

The toughness of the confrontations, especially in the North and East of Mali, has underscored the remarkable capacity of the soldiers to endure extreme conditions and to bear heavy psychological shocks. This capability, which is obviously one of the keys to the success of this "reconquest" phase, invites us not to discount the efforts our countries have dedicated to the training of their forces. Like the capabilities, the versatility of which I was praising, the intervention in Mali shows to what extent the soldier must also be versatile to be able, in the few months between two operations, to switch from a patrol in a stabilized environment to a high intensity combat against an entrenched enemy.

The engaged forces have also made the most of the experience they had acquired over the last years in Afghanistan and in Libya. Air combat, based on the combined employment of fighters and support helicopters, confirmed the advantage it provided to the troops on the ground. The firing assets of the 3rd dimension (artillery guns, fighters and attack helicopters) have shown their complementarity: they obviously are a factor of superiority over the adversary and therefore contribute to reinforcing the protection of the troops. More generally, the lessons learned in the fields of combined arms and joint co-ordination have clearly been keys to success.

The toughness of the engagements increases the level of requirement in terms of equipment. Strongly exposed, conducting combat among the population, the combatants need to have well-adapted equipment in terms of protection, information sharing and exploitation, mobility, weapon effect accuracy. The economic factor in armament programs is worth taking into account.

The violence of combat conducted in the Sahel, sometimes hand-to-hand, raises an essential question. It pertains to the resilience of our western societies and to the level of political determination they are able to show to commit to the lives of their soldiers. This question has been answered through the immediate involvement of the African countries following the French intervention. Thus, on January 23, 2013, 1,000 soldiers from Togo, Benin, Nigeria and Senegal were deployed in Mali, and three months later, nine African contributing countries provided more than 6,000 soldiers to the African-led

International Support Mission for Mali (MISMA). These contingents enabled the forces in combat to focus their efforts on the North, thus accelerating the reconquest. Their action made it possible to prepare the favorable conditions for taking into account the mandate by the MISMA; this mandate is aimed at stabilizing the situation and contributing to the restoration of authority of the Malian state over all the country.

The simultaneous international efforts under the aegis of the United Nations, the European Union, as well as the Economic Community of West African States permits us to foresee the future with reasonable optimism. The rapid implementation of strategies to restore peace in Mali is remarkable.

As a complement to the action carried out by U.N. troops, the mission led by the European Union aimed at training the Malian Armed Forces contributes to restoring the military capabilities of the Malian state in order to enable it to ensure its own defense as well as the integrity of its territory.

After six months of military operations, security is largely ensured and conditions favorable to dialogue have been set up, thus enabling diplomacy to fully resume. From this viewpoint, the signature, under the aegis of ECOWAS, of an agreement before the presidential election and the discussions on peace in Mali represents a major progress because it is the prelude to the return of democracy in the country.

Concluding Remarks—The Need to Preserve Vital Military Capabilities

The defense of global security requires, among others, intervention assets able to respond to the nature of crises. When no other way brings solutions, the use of force imposes itself as the last argument to restore the international order. Our determination to defend freedom and the law commits our credibility and shows how attached we are to our values. For this reason, it is of paramount importance that we preserve sufficient intervention capabilities, in priority on the ground, in order to be able to intervene together when the situation requires it, always abiding by international law, since we know that justice without force is powerless. Maintaining these military capabilities has a cost. Negligence in this field has a price: that of global security.

Chapter 6

Providing Regional Security—Georgia's Role

His Excellency Irakli Alasania
Minister of Defense of Georgia

Aspirations for NATO and the EU

I would like to touch upon the main points of our theme, "Peace and Security—The Challenges Ahead" and also talk about where Georgia stands in providing regional security. First, I will start with Georgia's wider participation in providing security to the North Atlantic sphere. Georgia is an aspiring state to join NATO, a partner to NATO, and we are fully engaged to be not only consumers of the security NATO provides but also participants and providers of security as well. Our country has been a partner in Afghanistan and we beefed up our operations last year with an additional battalion. As the recent ministerial meeting in Brussels mentioned, Georgia will remain committed to the security of Afghanistan after 2014. We will keep our troops there although the nature and the structure of the operation will change. I will be honest with you: we are not there just to look good in your eyes and get political favors. We are there because we believe in what we are doing. We are there because we do share the values that NATO represents. For decades, Georgia has aspired to be part of the European family and we are now closer to materializing this aspiration. This is why we are honored to be part of that endeavor.

At the same time, Georgia is not solely oriented to be providers of security within NATO. We also want to be partners in the European Union security dimension and this is why, a couple of months ago, the Georgian government voiced its political decision that our country was ready to be part of European operations, whether in Mali or in other areas. We feel a sense of obligation to the European Union because the EU leadership was very instrumental in ending the brief war with Russia and it was also the first one to provide the European Union Monitoring Mission, which is the only international eyes and deterrent in the region.

Strategic Partnerships with Azerbaijan and Turkey

With regard to the Black Sea regional security, we have a strategic partnership with our allies, Azerbaijan and Turkey. The three of us are working jointly in many areas. One, which is very important for the European energy security, concerns transportation and the "Southern Corridor." Together, we are working to provide an alternative route to our NATO allies in the reverse transit from Afghanistan and we are jointly building the railroad that will come through the East, through Azerbaijan, Georgia and Turkey, to Europe. This project is one of our priorities and I believe it will be instrumental for NATO.

We are also working very hard to improve regional cooperation among states such as Azerbaijan and Armenia. We are blessed with very good relationships with both countries. As you know, they are not getting along. We believe that Georgia can use its convening power to help Azerbaijan and Armenia develop relationships on various levels, not directly related to security of course, but the economy is a possible area. We are also cooperating militarily with both countries. So we are promoting this kind of Caucasian regional cooperation with both states.

Toward a New Relationship with Russia

The new Georgian government, of which I am a member since October of last year, is also changing its approach to Russia. For the past twenty years, the Russia-Georgia relationship has been very unfortunate. There have been a lot of misunderstandings, misinterpretations of each other's intentions, and many missed opportunities. I do not think that we can blame these on one side only. There is a general understanding that we have clearly misunderstood each other for years.

Today, our approach is more pragmatic. We do not expect that anything will change anytime soon, whether it is Russia's approach to Georgia's territorial integrity or our aspiration to join the European club. But we think that we can improve things bilaterally at the people-to-people level in areas like trade and economy. We have over one million Georgians living in Russia and their fate is something that we worry about as well. So, we recently launched negotiations with Russia. The Prime Minister has appointed a special representative for trade with Russia and this initiative is moving forward. There are lots of skeptics but we believe that we will open up the Russian market to Georgian businesses, to Georgian agriculture, to Georgian wine. At the very least, it will give Georgia the space to develop itself, to develop its institutions and its economy.

No less important, it will give Georgia the space to deal with Abkhazia and Ossetia, which are currently under the occupation of Russian forces. We have declared openly and clearly that there is no military solution to the conflict in Abkhazia and Tskhinvali region. This is part of our military strategy and part of our diplomacy. Having said that, we want to reintroduce ourselves to Abkhazia and Ossetia in a different way by applying new instruments, which again are the economy, infrastructure, and trade. This policy of our new State Minister for Reintegration is very wise and, I think, very instrumental to stabilizing the region.

We are also looking forward to the Olympics that will take place next winter in Sochi and have indicated that, even though Russia is occupying 20% of our land, we wish to cooperate on counter-terrorism because successful Olympics will create success for the whole region and we are all interested in that. I think that it is in Russia's best interest to deal with Georgia maturely but an earlier panel today mentioned that sometimes Russia does not reciprocate. For example, we recently witnessed the construction of fences in the occupied territories, which had the effect of devastating the local population. We do not need additional fences in Georgia; we need more cooperation. This is why our approach to this situation was very mature. We did not engage in a lot of rhetoric and we asked the European Union Monitoring Mission to help us defuse the conflict.

At the same time, it is very important for the international community, especially NATO, to realize that, although we have a pragmatic approach to Russia, we still need to make sure that Russia understands that they cannot get away with the new status quo they created after the war with Georgia in 2008. We keep asking the international community to apply pressure on Russia to implement the agreement to withdraw from the Georgian territory that they signed with the European Union and Georgia. We are grateful to all of you and your nations for supporting the territorial integrity of Georgia with its internationally recognized borders and we view the accession process that we have started with NATO as another opportunity to show that Georgia is reforming and politically maturing. This is why I think that we deserve adequate instruments to enhance our cooperation with the North Atlantic Council and we must bear in mind that no one, not even Russia nor any other state, can block us on our way.

Progress toward NATO Membership

We are looking forward to hosting the North Atlantic Council meeting in a few days in Georgia. This is another opportunity for us to talk about the reforms that we are doing in the areas of defense, security, and in the judiciary. It is also another opportunity to demonstrate that our political cohabitation with the party that stayed in power for nine years and conceded the election last year is working out. Together, we adopted in Parliament the resolution that supports Georgia's integration into NATO. We jointly appointed the Joint Chief of Staff of the Armed forces. The President, who is from the opposition but still in power, had to negotiate with us over this. We successfully appointed a new Chairman of the Joint Chiefs. We are working very closely with the national security team of the president on military-related issues. We just completed the strategic defense review, which will be the guiding principle and policy for the Georgian armed forces to transform, and we have a very ambitious plan to go fully professional in 2017. We are enhancing our rapid reaction capabilities and our special operations forces as well. All of this is happening in Georgia and I believe that the next presidential election in October will be another way for us to demonstrate that we deserve to be closer to NATO and the European family.

I also think that NATO will acknowledge this by next year's Summit. We are not talking about the kind of instrument that NATO will provide for us: it is up to NATO.

We have to perform but we believe that the risks are too high if the countries that are performing are not given a chance to be more closely associated with NATO. We will keep our commitment to the Euro-Atlantic community and to security in Afghanistan. Although we had a lot of casualties recently, the stamina and fortitude of our troops will continue to be very high and I do hope that European countries and the Euro-Atlantic community will benefit fully if those aspirant countries—some of them are together with me today—are given a chance to be closely integrated into the North Atlantic Community.

Chapter 7

A View from the Western Balkans

His Excellency Igor Lukšić
Deputy Prime Minister and Minister of Foreign Affairs of Montenegro

Global security is in our common interest no matter where we are, what resources we have, or the size of our country. Today, security—and the need for partnerships to preserve it—is globalized, just as the threats are. Terrorism in all its forms is recognized as a plague of the 21st century and it can find fertile ground as easily in developed countries as in undeveloped ones. Energy security plays an increasing role in economic and political stability. Organized crime and corruption eat away at both weak and strong states. The continuous struggle for peace and stability worldwide—be it in Afghanistan, Iraq, or Syria—is troubling to all. In addition, the economic crisis directly affects countries whatever their size.

Cyber Terrorism and Asymmetric Threats

Perhaps the best example to illustrate the ever-growing contemporary nature of the threats is cyber terrorism. This form of terrorism particularly demands joint actions and shared expertise. I will remind you of two examples—in 2003, malware was able to halt the U.S. energy system and leave 50 million people without electrical energy; in 2010, the Stuxnet program caused many problems in systems that are controlling oil pipelines. These threats underline the magnitude of the problems and the need to be alert to security demands. However, security needs investments. In the current situation, it is not easy to justify investment in invisible, abstract, or far away threats when people fear losing their jobs. We therefore have to share the burden of providing security. The challenges we are facing are asymmetric, and none of us has the individual capacity to respond. That is why integration and the pooling of resources around common goals are a must. We have to think globally and to cooperate, first within our regions and then beyond Montenegro.

Partnerships and Regional Cooperation in the Western Balkans

Partnerships in the Western Balkans are at the top of Montenegro's foreign policy agenda. We particularly value regional cooperation. To this end, we have recently initiated a new mechanism of cooperation with the overarching goal of accelerating the region's European integration through cooperation in areas of common interest, such as infrastructure, the rule of law, and finance. This initiative is compatible with the policies of the Southeast European Cooperation Process (SEECP) and the Regional Cooperation Council (RCC) 2020 Strategy and it carefully avoids overlapping with existing regional mechanisms. Regional cooperation is directly linked to the process of integration: if we can be good partners to each other, we can be credible partners to the EU and NATO. We believe that this is the only way to bring about lasting security, stability, and development to this part of Europe. And thus we simultaneously give our own unique contribution to regional, European, and global security. No contribution is irrelevant in this day and age, even if it is limited in capacity.

Progress toward Accession to the EU and NATO. As an EU and NATO candidate country, Montenegro is making fast progress. From the time when Montenegro launched accession negotiations in June of last year, our country has employed all its capacities to adequately prepare for this task. This is particularly challenging for a small administration. Our efforts were successful, as we have already opened and temporarily closed two chapters that are dealing with science and culture. Montenegro is the first country in this process to apply the new approach of tackling the most challenging areas first. We are therefore going to open negotiations on chapters with the rule of law. The preparation of Action Plans to this effect is in progress, and we expect to start negotiating in the course of this year. These chapters will be the first ones to open and the last ones to close, but we believe that this is the best way to be absolutely ready for membership and also to avoid bringing in problems when we become part of the EU family.

Directly linked to and practically inseparable from the process of our European integration is our path towards NATO membership. We see these processes as two sides of the same coin, one bringing long-term prosperity and the other guaranteeing security. We are focusing on implementing reforms in key areas—the rule of law, defense, security, the intelligence sector, and strengthening public support for NATO membership. Montenegro is fully committed to fulfilling its tasks. Although we are not focused on dates but on criteria, that does not mean that we are not setting deadlines for ourselves to conduct reforms. When we are done, we expect the Alliance to give us a chance to prove that we are ready, not as a favor but on the basis of results. And we expect the Allies to place the enlargement issue, not just more pressing problems of the moment, on the agenda. The enlargement to the Western Balkans is in the best interest of the Alliance.

If we look at the region, there are good reasons to promote the open door policy for countries wishing to become part of the Euro-Atlantic structures. The membership of Croatia and Albania has had a positive effect on security in the Balkans. Montenegro's future membership will strengthen that effect and keep the "open door policy" alive. While countries are judged individually since each one has its unique challenges and problems, their success is good for everyone.

Global Peace Missions and Operations. We understand the importance of sharing responsibility and resources when it comes to global peace missions and operations. We have been present in Afghanistan in ISAF since 2010. The seventh contingent of our army, with 27 soldiers, was deployed at Camp Marmal in Mazar-e Sharif. Their tasks are now more complex, and we have changed our national caveats to allow a stronger engagement of our forces. Our efforts will continue in line with the principles "together in, together out." We are willing to be present in Afghanistan beyond 2014, and we were recognized as a potential operating partner for the post 2014 NATO-led Mission Resolute Support for a three year period after 2014. We believe we have proved to be a trusted partner of the Alliance in facing global security challenges, even though we are not a member yet. Montenegro also participates in missions of the EU and the U.N. in Somalia, Liberia, and Cyprus. Recently, Montenegro promptly reacted to crises and donated much needed equipment to the armed forces of Mali.

Smart Defence. Modern security threats and their changing nature require all of us to be creative in order to find the best solutions. The Western Balkans also has a role in this. The concept of Smart Defence prompts us to think of how to get maximum results with minimum financial efforts. Countries of the region contribute to this by joint actions in peace operations or in creating a joint regional air surveillance system in the framework of the U.S.-Adriatic Charter.

The Situation in the Western Balkans. Since our regional colleagues are here, let me say how we view the situation in the region. The times when the region was a source of instability are behind us. The image of the region has changed for the better. The EU and NATO enlargement and the perspective of membership have had a transformative power. Montenegro strongly believes that the Balkans is now part of the solution and not part of the problem. That does not mean that there are no more lingering problems: they are a burden for the future of individual countries and for the region as a whole and we all need to make an extra effort to resolve them with the assistance of the international community. After all the events of the past couple of decades, the region shares the same integration goals. We need to make use of this so that no one in ten or twenty years evokes nationalism, extremism, history, and or other strong emotions to cause instability again.

Serbia-Kosovo and Skopje-Athens. Let me also stress that we welcome the agreement that has been made between Serbia and Kosovo, and we believe that it will lead to increased practical cooperation and the inclusion of Kosovo in regional initiatives. We hope that Skopje and Athens will soon find a final solution to the name issue and we are confident that the negotiations will lead to a mutually acceptable solution in due time. We also hope that Bosnia and Herzegovina can overcome political complexities, which are an obstacle to its functionality and are slowing down its journey to Europe and NATO. Here, I would like to congratulate our neighbor Croatia on joining the EU after becoming a NATO member, which is the best example of how commitments to reforms lead to success and recognition by partners. The progress of each country of the region reflects positively on all of us and gives us new impetus for reforms.

Concluding Remarks

I wish to emphasize that as long as the Balkan region is not a part of the EU and NATO community, there will be a cloud over it. Europe can only be truly ''whole, free and at peace" after the final integration of all the Western Balkan countries. We understand that global challenges and threats to security as well as the economic crisis itself seem like the most important issues to deal with, both nationally and internationally. In comparison, Balkan issues seem small and inconsequential, but we only need to look back twenty years to see where Balkan problems can lead if they are allowed to fester. We must not forget that the Balkans is not a done deal, but rather a work in progress. We need one big final push to finish the job started after the conflicts. That is first NATO and then, slowly, full EU integration. This is not to say that the lion's share of this task is not our responsibility. On the contrary, we need to continue reforms and adopt standards and values in our everyday life, not just on paper. But our citizens also must feel that, once we have done our job, we will be wanted as equal members of the democratic European and Euro-Atlantic family. Integration is a two-way street. And so is security.

Chapter 8

Bosnia and Herzegovina's Path to Euro-Atlantic Integration In the Context of Global Security

His Excellency Zekerijah Osmić
Minister of Defense of Bosnia and Herzegovina

On behalf of the Ministry of Defense of Bosnia and Herzegovina, let me express my sincere gratitude for the opportunity to present our vision of Bosnia and Herzegovina's progress, experience, and future challenges on its path towards integration into NATO and the European Union in the context of security in our region and beyond.

The new forms of direct security threats such as terrorism, proliferation and use of weapons of mass destruction, human trafficking, narcotics, and cyber crimes, etc. marked the emergence of a period of mutual relations among countries, both globally and regionally. No country, no matter how strong, is capable of dealing on its own with the new asymmetric threats. This is especially true for small countries, which are certainly not in a position to meet these challenges. For this reason, they are trying to find solutions and security through wider regional and global initiatives.

Just as for defense and security, integration is also necessary and equally important for our economy, science and education, environmental protection, and in all other areas of social life. In this context, Bosnia and Herzegovina faces two distinct and complex challenges:

- First, in parallel with the process of accession into regional and European security structures, Bosnia and Herzegovina needs to deal with the post-war reconstruction of our society. This reconstruction is needed not only materially, but it also requires a process of democratization, the establishment of a modern state, and the building of trust among our citizens. This is an extremely complex process.
- Secondly, Bosnia and Herzegovina must keep track of current security concepts, which now include global changes in security and politics and in other areas such as economics, democratization and internationalization.

EURO-ATLANTIC INTEGRATION

For Bosnia and Herzegovina, membership in the Euro-Atlantic structures is an important strategic foreign policy goal. In this regard, our country has initiated a series of reforms aimed at meeting the prerequisites for membership in NATO and the European Union. These reforms are directed a the defense sector and at all other segments of Bosnia and Herzegovina's society such as economics, legal system, safety etc. In joining NATO and the European Union, Bosnia and Herzegovina sees political advantages, security advantages, and economic benefits.

Political Advantages

- Bosnia and Herzegovina will become a full member of the large family of European states;
- It will also become a visible political entity with a role in decision making processes at this level and an opportunity to promote its own interests and attitudes;
- It will increase the international reputation of our country.

Security Advantages

- As a security organization, NATO has the primary task of ensuring the territorial integrity and sovereignty of its member states with regard to almost all threats, a role which is without precedent in history;

- NATO is compatible with (and not duplicative of) the security systems of the U.N., the EU, and the OSCE;
- No member of the Alliance has been in an armed conflict with other members;
- The process of NATO and European integration encourages and promotes the internal stability of the new member states, and thus of the national security system as a whole.

Economic Benefits

- With membership in NATO, the EU, and other associated initiatives and forms of partnership cooperation, Bosnia and Herzegovina will become a member of a group of countries that holds more than two-thirds of the world's GDP;
- Membership in NATO and the EU will encourage an increase in foreign investment;
- A united Europe will become a large market for goods and products from Bosnia and Herzegovina;
- Costs of national security will be reduced.

Political Delays and Practical Difficulties

At the same time, there have been and still are political delays and practical difficulties in fulfilling the obligations and commitments arising from the integration process. What are they? In our opinion, the key difficulties are:

1. Subjective—the need to change the habits and mindsets of the people;
2. Objective—our country is working toward NATO and EU integration in several areas that require radical and comprehensive reform. Yet, it is important to consider that any reform process, no matter what it is, always brings resistance from traditional entities and is always is followed by political calculations;
3. Inconsistent or unclear standards and criteria given as preconditions and requirements. It is no secret that, especially for membership in the EU, Bosnia and Herzegovina has been given preconditions that were not placed upon new members acceding to the EU in earlier cycles of expansion.
4. The reform process requires adequate human and material resources to carry out these processes. We are close to the standards in terms of human resources.
5. However, material resources are not actually available. We have to do a lot more in that direction, perhaps by prioritizing projects that, in the long run, will not only increase national security but also attract foreign investment.

CONCLUSIONS

It is often said that Bosnia and Herzegovina does not have any alternative to accession to the Euro-Atlantic and European integration. In my opinion, there is always an alternative. Yet, would these alternatives be acceptable and could they be substantially better than the existing ones?

Bosnia and Herzegovina's NATO and EU integration and our country's views on NATO and the EU should be seen as a continuous process. It is a practical follow-on to the provisions begun by the Dayton Peace Accords in the 1990s, continued by the accession of our country to NATO's "Partnership for Peace" in 2006, and then, most recently, by the conclusion of the Stabilization and Association Agreement with the EU in 2008.

Moreover, the current geopolitical situation in the Western Balkans is favorable to the further enlargement of NATO and the EU in this area. Bosnia and Herzegovina sees the recent Croatian accession to the EU as a success and a possible source of inspiration for the region as a whole. Together with this encouragement, the agreement between Belgrade and Pristina on issues is another positive step that can and should relax relations throughout the region.

Bosnia and Herzegovina also contributes to global security by participating in peacekeeping missions, including both the U.N. mission in Congo and the ISAF mission in Afghanistan. Our country has become an active provider of services in the system of collective security.

Although it is still in its early stages, the NATO and EU integration process strongly supports and encourages the process of internal stabilization and democratization of Bosnia and Herzegovina.

Chapter 9

Peace and Security—the Challenges Ahead and Common Regional Responses

His Excellency Talat Xhaferi
Minister of Defense of Macedonia

A Rapidly Changing World Requires New Approaches

I would like to make a few comments from the viewpoint of the Republic of Macedonia. We began the new century with the understanding that the world is changing rapidly. We are indeed able to address some of these changes but many require a joint and coordinated approach. Today, new political, economic, security, cultural or religious developments are leading to a global civilization that is more connected, informed, transparent and accessible for an ever-increasing number of citizens.

The factors that caused this process to unfold are quite diverse. At one stage, connections were made through vast military conquests. At another stage, it was treaties. Later on, it was industrialization. Today, it is the interconnectivity of the modern world. In that context, the advances of science, technology, culture and rational discourse play a crucial role. In practice, the beginning of the 21st century has heralded a new paradigm which has brought new challenges to global security as well.

Terrorism, ethnic and religious conflicts, regional conflicts, drug trafficking and organized crime, weapons of mass destruction, financial and economic crises, poverty, environmental disasters as well as cyber attacks are real problems in this new era of globalization. In the new interconnected and interdependent world, problems are becoming universal. Hence, they represent a threat to international security. On the other hand, the advent of the Internet-based social networks or the so-called new forms of democracy have closed the gap, enabling people through the world to jointly organize, with fast communication. This provides them with opportunities to share views and ideas and take joint actions swiftly with online political activism.

The impact of these changes could be seen during the so-called Arab Spring. What previous generations could not even have dreamt of can be done today in minutes. This leads to the question as to how the international community can react in a timely fashion to these great changes and prepare for the advent of new security challenges.

I firmly believe that the new challenges should be addressed jointly and determinately. There is an apparent need to find ways of establishing and maintaining new defense connections and cooperation. Multidimensional political, expert, and academic knowledge and experience are needed. Moreover, I am convinced that domestic support for international engagements is one of the key issues, even though globalization is removing the difference between foreign and domestic policy.

The involvement in Iraq and the 2008 Iraqi Freedom coalition, NATO operations in Afghanistan, NATO's support in Libya, and the role that the EU member states have been playing in Southeast Europe show that taking joint action is the right way.

Instability in Southeast Europe Could Trigger Spiraling Regional Conflicts

Concerning security in Southeast Europe, history teaches us that regional instability has the potential to trigger a spiral of regional conflicts. It is probable that instability in many regions in the world will not disappear quickly. On this occasion, I would like to briefly remind you of the instability in the Balkans in the past two decades. The military conflicts in the Balkans caused many casualties and much suffering and destruction, including ecological, economic and political damage. The conflicts in our region have cost us two decades in our overall development. The conflict resolution in the Balkans called for a joint response by NATO, the EU, the United Nations and the entire international community.

The Southeast European countries are facing similar security challenges to those faced by other countries from the Euro-Atlantic region. These common challenges and problems require joint solutions and only by working together can we contribute effectively to peace, security and stability in the region, Europe and beyond. From a Balkan perspective, strong regional and bilateral cooperation are the best mechanisms for responding to the common challenges and contributing to global peace and security.

All Countries in the Region Should Be Integrated into NATO and the EU

Over the past decade, substantial progress has been made in the security sector and the overall development of all countries from the Western Balkans, as well as in the fulfillment of the vision for a united and free Europe. Albania and Croatia have become NATO members and we are expecting that the same will happen with Macedonia, Montenegro and Bosnia and Herzegovina as soon as possible. Today, each country from the Western Balkans has reached the stage where the EU integration process is irreversible. We are happy that the Republic of Croatia will become the 28th EU member in a week and that all other Western Balkan countries stand on the same European course. Montenegro has started the accession negotiations with the EU. Albania, Bosnia and Herzegovina and Serbia have made progress towards the EU. Kosovo is working hard to achieve a visa free regime with the EU and is taking steps in the direction of the agreement of stabilization and association with the EU. Macedonia is a candidate country and has waited for seven years to start the accession negotiations with the EU after several recommendations from the European Commission. However, NATO and the EU have not finished their job in our region and their contribution to regional security is still necessary.

NATO and EU enlargement are the right contributions to peace, security and prosperity in the Western Balkans, the European continent and the world. It is the answer to the legitimate request of the peoples from the Western Balkans to be integrated in a united Europe. NATO and the EU have both invested very much in the Western Balkans. Now, it is time to harvest the results. Europe cannot be free without a secure and stable Southeast Europe, and Europe cannot be united without the integration of all countries from the Western Balkans.

Regional cooperation is an essential contribution to regional security development, a precondition for progress of all Western Balkan countries towards NATO and EU membership, and it makes all countries contributors to Euro-Atlantic security and stability. Being aware of it, the Western Balkan countries are active participants in a number of regional initiatives and seek joint regional responses to the common challenges. At the end of last month in Albania, we discussed the perspective of the Western Balkan countries on Adriatic and Ionian security challenges in the framework of the Adriatic-Ioanian initiative. This month in Macedonia, in the framework of the United States-Adriatic Charter, first the defense ministers, and then the foreign ministers, discussed ways for contributing jointly to global peace and security. All these regional forums came to the same conclusion that together, if we join forces, we can do more for all countries, for Europe and the world.

Significant and tangible results have been achieved in the regional defense cooperation starting with the joint training of joint military units up to the joint participation in the ISAF operations in Afghanistan. In this context, the establishment and maintenance of the multinational Southeastern Europe Brigade SEEBRIG is a significant project. Close and fruitful regional cooperation within the United States Adriatic Charter proved to be a very successful example of joint regional response to the common challenges. The collaboration developed gradually through joint projects enabling joint contributions to the NATO mission in Afghanistan, first with the A3 medical team, followed by the A5, plus the military police school in Kabul. At the same time, this enabled the creation of a win-win situation for all A5 countries. The contribution of the A5 countries in Afghanistan today reaffirms our common will and ability to jointly address the common challenges. The Republic of Macedonia has confirmed its commitment to participate in the new NATO mission, Resolute Support, in 2014 and welcomes the initiative of the Republic of Croatia to reactivate the military police school in Afghanistan. We also support the proposals for a possible joint contribution force, protection and joint advisory teams in several specific areas.

The Republic of Macedonia is committed to participating in NATO-led missions, in missions of all the international organizations. At the moment, the Republic of Macedonia participates in the ISAF mission in Afghanistan, and the EU Althea mission in Bosnia and Herzegovina.

Chapter 10

Defense and Foreign Ministers of the Balkans and Black Sea Region: Panel Discussion

Ambassador Michel Foucher
Director of Studies and Research, Institut des hautes études de défense nationale (IHEDN)

It used to be common understanding that the Balkans were producing more history than they were able to absorb. I never forgot that when I served as the special envoy of the French government in the region some years ago and later on to the Caucasus. My impression today is quite different. It is that history is much more under control, at least if I refer to the biographies of each of our speakers. With their permission, I will not read their biographies but I invite the audience to have a look at them. They are quite interesting.

The Deputy Prime Minister of Montenegro made a reference to recent progress between Kosovo and Serbia. If we come back to the wider Black Sea region, you are four countries with four so-called frozen conflicts, from Moldova to, let's say, Western Azerbaijan, and the oldest one between Armenia and Azerbaijan is already twenty-four years old. Everyone knows the technical geographic border issues and diplomatic solutions that are required, but it seems impossible for political leaders to sell that to their political friends and foes and to their public opinion. How do you explain this impossibility to get out of four frozen conflicts in the region? Can we live many more years with these so-called frozen conflicts?

Georgian Minister Irakli Alasania

The nature of each of these conflicts is different but their common cause comes from the Soviet policy of "rule and divide," which was enacted by the Soviet leadership and unfortunately continues under the current Russian leadership. So I do not see a breakthrough in these conflicts for the coming years, because there is no political will on the side of the main player which is the Russian Federation. At the same time, things are changing in Russia as well and we are hopeful that in the next decade, things will change concerning this policy.

This is not the only reason. There are also internal reasons. For twenty years, Georgia has had the wrong policies towards Abkhazians and Ossetians, namely keeping them in isolation. We thought that, by isolating them, we would deprive them of international legitimacy and that later on, we would reintegrate them back, which is wrong. This is why we completely changed our policy toward these two regions. We want them to experience democracy, how things are working in Europe, and we are opening them up toward Europe so that they feel that, together with the Georgians, they will be better off if they are part of Europe instead of staying under Russian occupation. So there is a lot of blame to go around for these past twenty-five years but I believe that the only way to move forward is to state that there is no military solution and put an emphasis instead on infrastructure, economic and trade projects.

Azerbaijan's Ambassador Khazar Ibrahim

The question you asked of how long we should wait is actually critical, and it should also be addressed to the international community—How long should the international community wait?—In fact, all the recent polls and surveys I have seen show that the younger generation is less and less inclined toward a peaceful resolution and this is dangerous. My generation still has contacts, we still talk to each other, but the younger generation does not have people-to-people contacts. So it is important for the international community to put tangible proposals on the table and push for a practical resolution.

Estonian Minister Jaak Aaviksoo

I think there is a pretty broad consensus against the use of force in solving these conflicts. On the other hand, I do not believe that patience alone can make things happen. Two trends are important for solving problems: the first one, demography, is a slow process but, in the long run, it will determine what will happen. The second one is the economy—Who is doing better and who is doing worse? Our experience on the Baltic coast shows that if you cooperate in the region economically, politically, and on all levels, you can more than triple your impact. So can you comment a little bit on these trends—How is the economic cooperation going and what are the demographic trends for the future?

Montenegrin Deputy Prime Minister Igor Lukšić

One thing is certain: the overall economic crisis has left a lot of scars. The economic enthusiasm that existed several years ago when economies were growing was killed by the economic crisis. All the Western Balkan countries are suffering from recessional stagnation with a lot of structural problems, and the restructuring of economies imposes different challenges ahead that are not easy to resolve. This is what we have gone through in Montenegro but our experience is quite similar to the experience of Croatia, Serbia, Bosnia and Herzegovina, Albania, and Macedonia.

In addition, when you look at some indicators such as public debt, most countries in our region have already reached a level of debt that prevents them from borrowing for useful purposes such as infrastructure. This is one reason why, in addition to existing regional initiatives, we have initiated new mechanisms of cooperation. Since it will take some years for the countries in our region to get into the EU, we need to focus on different mechanisms of cooperation in order to speak with one voice when we have immediate common interests. This goes hand in hand with economic improvement, with the development of the infrastructure and new jobs to be created. These new mechanisms of cooperation are also intended to reduce business costs and the costs for people in the region to move from one place to another. Finally, we need to weed out corruption, organized crime, and make progress in the development of our institutions. All this will hopefully convince investors from other parts of the world that our countries are good business destinations.

Another factor is demography. Populations in our countries are getting older according to a pattern that is more or less similar to the one in all of Europe. At the same time, I am convinced that the Western Balkan region is one of the regions in Europe that should have the biggest potential for growth. With integration in the EU becoming closer, the challenge will be to find a way to convince people with talent and skill to stay in our region, which will generate growth, instead of going abroad. This may be the integration paradox. We have seen a lot of brain drain in the 90s, we saw that process stop in the early 2000s, and then the current economic crisis is opening up different perspectives for the people. So, from that point of view, the demographic challenge is a big challenge. There is also internal migration within our countries and we see it in Montenegro, where it is strong and not easy to tackle. I recently visited the Baltic countries and was told that from the moment of their accession to the EU, the population in some of the Baltic countries has kept falling. This could serve as an example to us because, from a sustainability point of view, this is an important point.

Georgian Minister Irakli Alasania

I will add quickly that, in addition to the conflicts, Georgia and Azerbaijan are pretty much the same. We have a large part of our population that was ethnically cleansed as a result of the conflicts and we are trying to reconnect this population into society, but this is a heavy burden for our economy. In general, however, the Georgian economy, which is still a little bit slow, has been picking up after the elections. We have pumped a lot of money in the agriculture, which helps the people in rural areas. I was in Azerbaijan a week ago and it is a miracle to see how much development there has been in Baku and Azerbaijan. So this gives me hope that there is enough potential for economic growth in our region for these conflict areas to actually be part of it and benefit from the economy and from democracy.

Chapter 11

Views from the Visegrád Region—Poland, the Czech Republic and Hungary

Ambassador István Kovács
Hungarian Ambassador to NATO

Today I have the pleasure to chair this panel consisting of the representatives of Poland, the Czech Republic and Hungary. One might ask why these countries are on this panel together today, what bonds them together. Let me just state a few facts to kick off the discussion.

All three were part of the Warsaw Pact at one time. All three had the immense courage of trying to leave this political-military system bestowed on them that they had never freely chosen: Hungary with the revolution of 1956; Prague with the Spring of 1968; and Poland with Solidarnosc in 1980-1981.

Soon after 1989-1990, all three expressed their readiness to be part of the EU—then the European Community—and NATO. All three were always part of Europe but, after 1990, they could freely ask to be integrated into the Euro-Atlantic structures. In all three countries, the citizens indicated that they uphold the commonly shared values of NATO and the EU: at a referendum in Hungary on NATO membership for example, 84% voted with a yes. All three took the necessary steps to meet the challenges to be accepted as members of NATO and the EU; and during the past 14 years of their NATO membership, all three proved that they are not in for a free ride to enjoy the benefit of collective defense but are actively committed to contributing to the security of the Alliance—ISAF and KFOR to name just two operations.

And to finish, all three recognized at an early stage the merits of Smart Defence and Pooling and Sharing within the Visegrád Four regional cooperation. This also extends to security and defense cooperation but still holds room for improvement. On 1 July of this year, Poland is handing over a successful chair to Hungary in the V4 and we will do our best to move defense and military cooperation ahead.

With this introduction, let me give the floor to our distinguished speakers.

Chapter 12

Polish Security and Defence Policy: the Story of Success

Minister Bogusław Winid
Undersecretary of State, Ministry of Foreign Affairs of Poland

Following a nearly six-year occupation during World War II, Poland experienced 45 years of limited sovereignty during the Cold War until the collapse of the Soviet Union. Finally, at the end of the 20th century, Poland returned to the family of independent nations and became a full, reliable, and active member of the West. Today, membership in NATO and the European Union, together with the strong alliance with the United States and good relations with our neighbours constitute the cornerstones of our security policy. Poland is a credible ally, a constructive partner, and a security provider. The main foundations of the current Polish foreign policy were laid down during Poland's democratic transformation. This process started almost a quarter of century ago in 1989 with the Round Table talks that brought together the representatives of both the Communist regime and the democratic opposition. The talks paved the way for the first partly democratic elections in the Eastern Bloc held on 4 June 1989 and decisively won by the Solidarity movement (Solidarność). Its consequences were indeed symbolic: the first democratic government on our side of the Iron Curtain was created as early as September 1989, even before the Berlin Wall collapsed. Lech Wałęsa, the legendary leader of Solidarity, was elected President of Poland in November 1990. The new political elites of independent Poland formulated a new strategic goal for our foreign and security policy, namely the return to the West, which meant the full integration into the European and Euro-Atlantic structures of NATO and the European Community. The transformation in Poland had an enormous impact in our region, leading eventually to the formal dissolution of the Warsaw Pact in July 1991. The process of recovering independence was symbolically finished by the peaceful withdrawal of the Russian Army from Poland's territory in 1993.

Membership in NATO: Poland's View on the Alliance

Poland became a member of the North Atlantic Alliance in 1999. NATO, as the political and civil Alliance of Western Europe and America, standing shoulder to shoulder in defence of common values, had always been a reference point for the Poles. To be a member of NATO was a seemingly impossible dream. After 1989, this dream became the target of almost all political powers in Poland and all consecutive governments. During the next decade we worked hard to split from our Communist past not only by declarations, but above all by improving our governance and modernising our country. Joining NATO 14 years ago was a landmark development in the history of Poland that marked the real sign of the demise of the old bloc system. Our membership in the EU, achieved in 2004 thanks to a nationwide effort, cemented for good our place in the West.

As Minister Radosław Sikorski said in 2009 on the tenth anniversary of Poland's accession to NATO: "Our accession to NATO is one of the most important political events in our modern history. For Poland, the year 1999 was a critical milestone in building our citizens' security awareness and their trust in the state. Our accession came along with the tenth anniversary of the Autumn of 1989, which transformed the socio-political system of Poland, and shook, puzzled and eventually rebalanced the whole European continent and the then world order. As such, joining NATO was a confirmation that the way chosen ten years earlier, in 1989, was the right one as far as our security and defence policy was concerned."

Poland is now a fourteen-year-old NATO member. During this period we smoothly grew into the Alliance's political and military structures, procedures, habits and culture of debate. Each year of Polish membership in NATO was a test of our credibility and effectiveness in the joint fight against common threats and challenges. We intensively modernised our military capabilities. From the first days of accession, Poland has participated in NATO missions. We have proved to be a serious and responsible ally. We do not consume security, we actively participate in providing security in Europe and beyond its borders wherever and whenever the Alliance deems it necessary.

We see the Alliance as an appropriate mix of the old and new missions and capabilities. A continuing readiness and preparedness to perform collective defence functions needs to be accompanied by an ability and capability for effective reaction in the face of new threats. For us the fundamentals of Euro-Atlantic security are: unity, allied solidarity, and a strong transatlantic link, all of that based on reliable political mechanisms and constantly updated defence capabilities.

As Minister Radosław Sikorski said at the 2008 Munich Conference on Security Policy: "Poland views NATO traditionally. We joined the Alliance in 1999 convinced that it would offer us security through collective defence, which for us is the essence of NATO. Allied consultations, defence planning and a broad range of relations with NATO partners are our indispensable collective procedures. Although NATO has undergone transformation in reaction to ethnic wars, terrorism and a nexus of asymmetrical threats, we still need the sound basis of collective defence."

Strengthening the Transatlantic Link: Polish-American Security Relations

Poland has been a strong supporter of strengthening the transatlantic alliance and maintaining the United States' engagement on the Old Continent. Cooperation in the security and defence domain, which constitutes one of the key dimensions of the Polish-American relationship, contributes to this end. Over the past two decades, Poland and the United States developed an extensive bilateral framework for cooperation—the current security policy cooperation is based on the 2008 Declaration on Strategic Cooperation. Both our countries intensively consult within the Strategic Dialogue, Strategic Cooperation Consultative Group and High-Level Defence Group. Polish and American troops have been standing shoulder-to-shoulder in defence of the common values of freedom and democracy—our longstanding military cooperation in Afghanistan serves as the best example. Based on agreements from 2008 and 2010 Poland will host the American missile defence site in the framework of the European Phased Adaptive Approach. This particular project, however, has a wider impact as the Redzikowo site will be part of the NATO Ballistic Missile Defence (NATO BMD) and therefore will contribute to the security of the Alliance. The recent example of strengthening our bilateral security ties with the U.S. is the so-called Aviation Detachment inaugurated in November 2012 in Łask, Poland. This initiative, being a first permanent deployment of American troops on the Polish soil, provides for joint trainings of Polish and American air forces.

Poland in the European Union: Enhancing Common Security and Defence Policy

Since the accession to the European Union, Poland has been engaged in the security and defence dimension of the European Integration. While cherishing the transatlantic alliance, we believe that Europe itself should and can do more. Our position in European defence was built over the last years on the following key foundations: the increase in defence spending and modernisation of our forces, the achievements of the Polish Presidency of the Council in the EU in 2011 and our active engagement in meetings and initiatives within the Visegrád 4, Weimar Triangle, and Weimar plus. In Poland's view, the Common Security and Defence Policy (CSDP) should be seen as a prospective project and we are ready to continue to play an active role in promoting stronger integration between Member States in the field of security and defence.

One of the concrete examples of our work during the EU Presidency was that we were able to bridge the gap between Member States to achieve compromise over the Conclusions adopted on 1 December 2011. Even though the establishment of a standing civil-military planning and conduct capacity (EU OHQ) from a political perspective proved to be too ambitious, we managed to gather the majority of the Member States to discuss an idea that had been taboo for years. The decision on the activation of the Operations Centre in January 2012 opens the way to fully use its potential to support a civil-military approach to CSDP in the spirit of the comprehensive approach. The implementation of the tasking from the December 2011 Council conclusions concerning the need to further develop planning capabilities will be of the highest importance in reducing the response time when a crisis occurs.

The aims of our EU Presidency, i.e. improving the decision-making process and increasing CSDP operational effectiveness, have never been more pertinent than today. We need a more robust and more effective CSDP that can respond to the challenges in its immediate environment. But we also need an EU that could relieve NATO wherever it could do the job better or when there is no pressing need to use the heavy military machinery of the Alliance. In order for this to happen, there are two significant challenges: firstly, we have to ensure that European nations provide and sustain their capabilities to act and secondly, we need some institutional fixes to ensure that CSDP can really deliver.

Current processes concerning the revision of crisis management procedures, the review of the European External Action Service, the debate on enhancing flexibility and usability of the EU Battle Groups and, most importantly, the preparations for the European Council on defence in December of this year should add elements for an answer to the above-mentioned needs and challenges. Poland is ready to and will contribute to this process.

Engagement Out of Area: Polish Participation in International Operations

With its long-standing tradition of participation in U.N. peacekeeping missions dating back to the early 1950s, Poland naturally joined the NATO stabilisation activities in different regions of the world. At the time of our accession to NATO, Poland already had 500 soldiers committed to the Stabilisation Force (SFOR) in Bosnia and Herzegovina. In June 1999, 850 additional troops were sent to the KFOR mission in Kosovo.

Since then, Poland has always been among the significant troop providers to stabilisation operations conducted under the NATO command, within the EU framework, or within the coalitions of the willing. At its peak in 2004-2005, more than three thousand five hundred troops were permanently deployed to operations in Afghanistan, Iraq and the Balkans. Poland also contributed to African EU missions with more than 500 troops. In 2008-2009, Polish forces (400 soldiers) were involved in EUFOR Chad, in 2006 our contingent was present in EUFOR Congo (130 soldiers). Our contingent in Chad was the second largest force, after the French, in the theatre. This has been a significant effort for a country like Poland. Currently, Poland participates in 2 out of 3 NATO operations (ISAF, KFOR) and in 7 out of 16 EU missions/operations (EUMM Georgia, EULEX Kosovo, EUFOR Althea, EUPOL Afghanistan, EUTM Mali, ATALANTA, EUBAM Moldova). In terms of personnel in EU civilian operations, Poland is the second largest provider with 203 experts deployed.

ISAF has been so far the most demanding operation both in terms of human and financial resources. Many countries have had quite substantial forces on the ground. Poland, currently the fifth largest contributor to the operation, had 2600 troops at the peak period, mostly located in the Ghazni province, considered one of the most difficult provinces.

With the end of the ISAF mission in 2014, the Balkans will most probably remain our main area of commitment. The EU should strive to gradually assume the prime responsibility for security, stability and long-term development in the Balkans, including Kosovo. I hope that the European Council in December will give decisive guidelines to this effect. Poland stands ready to shoulder this responsibility side-by-side with our EU partners.

Multilateral Diplomacy: Poland in WMD Disarmament and Non-proliferation

Poland is traditionally very active in supporting efforts aiming at global disarmament and non-proliferation of nuclear weapons. Poland is a member of all existing control regimes dealing with nuclear materials, e.g. the Nuclear Suppliers Group, Wassenaar Agreement, the Australia Group and the Global Initiative to Combat Nuclear Terrorism. In 2010 we joined an Australian-Japanese project, which has since then evolved into the Non-Proliferation and Disarmament Initiative. NPDI is a cross-regional initiative of ten states striving for universal implementation of the final document and Action Plan of the 2010 NPT Review Conference. Our particular objective encompasses increasing transparency of nuclear arsenals, revitalisation of the Conference on Disarmament, promotion of ratification of the Comprehensive Test Ban Treaty (CTBT) and universalisation of the IAEA's Additional Protocol on Safeguards. On various fora, including NATO and the NPT, we have undertaken steps to initialize dialogue on tactical (non-strategic) nuclear weapons that have not yet been covered by any arms control agreement. Just recently, in February 2013, the Polish Institute of International Affairs, Norwegian Institute for Defence Studies and Carnegie Endowment for International Peace hosted the Warsaw Workshop: Prospects for Information Sharing and Confidence Building on Non-Strategic Weapons in Europe.

Poland is also actively involved in international efforts to promote the effective prohibition of chemical and biological weapons. Every year, as a sole sponsor, we introduce the Resolution of the U.N. General Assembly on the Implementation of the Chemical Weapons Convention. In April 2013 a representative of Poland chaired the Third Review Conference of the CWC. Poland was also a Vice-chair of Biological Weapons Convention meetings in 2012. This active and continued engagement is a concrete input Poland has made throughout many years to support these non-proliferation regimes.

We are also engaged in international efforts to improve counter proliferation capabilities. Poland hosted in Warsaw on May 27-28 the High-Level Political Meeting of the Proliferation Security Initiative (PSI), an event marking the tenth anniversary of the creation of the PSI. The meeting made it possible to lay out the next steps that the attending states intend to take both individually and together with other PSI partners to improve common counter proliferation capabilities.

The Regional Dimension: the Example of the Visegrád Group

Our security policy is deeply rooted in the region. The flourishing cooperation within the Visegrád Group (V4) bears testimony to this end. Our nearly concluded presidency in the V4 (lasting from July 2012 until June 2013), while continuing work already started by previous chairmanships, has succeeded in launching new dimensions of cooperation: the so-called cross-format cooperation. In that spirit, the Visegrád meetings with our Weimar, Nordic, and Baltic partners are creating opportunities to develop activities in different constellations, with diverse intensity and dynamics. We believe that initiatives like Pooling and Sharing and Smart Defence have a better chance to succeed when developed and implemented first by partners in the neighbourhood. It is worth mentioning some V4 and V4+ initiatives that have been expanded lately: a CBRN battalion within NATO's Smart Defence initiative, cooperation within the Multinational Corps Northeast, Baltic Air Policing Mission, and NATO Joint Force Training Centre in Bydgoszcz. An example of developing V4 cooperation was signing the Letter of Intent concerning creation by 2016 of the V4 Battle Group within the framework of the EU.

Credibility: Modernisation of the Polish Armed Forces

Poland spends 1.95% of its GDP on defence. The figure is fixed and therefore guarantees a stable level of the defence budget. Given that the Polish economy is successfully coping with the crisis, this means that spending is rising steadily. At the time when most NATO military budgets are under severe strain, Poland is undertaking a thorough modernisation of its Armed Forces. In April of this year, Polish President Bronisław Komorowski said during the signing ceremony for the Financing and modernisation of the Polish Armed Forces act "Poland will be more secure and more credible as an ally and a key country in our part of Europe, able to defend its own territory and able to help others."

In the nearest future Poland is going to develop state-of-the-art capabilities, thus increasing the combat potential of its Armed Forces for realisation of national and allied commitments according to Art. 5 of the Washington Treaty. At the end of 2012, the Ministry of National Defence accepted the Technical Modernisation Plan and the Program of Development of the Polish Armed Forces for years 2013-2022, launching a new era of modernisation of the Polish army. In his annual speech in Sejm (the lower house of the Parliament) Minister Radosław Sikorski said: "History teaches us that Poland must look to itself to look after its security—also in the military sense—and that this security largely depends on our own defence potential." Our objective at the same time is to be more credible as an ally.

In the present decade, Poland is planning to spend almost 140 bln PLN (33 billion euros) on modernisation. The priority will be given to command, reconnaissance, and action support capabilities. We will also strengthen other capabilities, such as mobility, survival ability and protection of forces as well as the ability to support non-military systems in crisis situations. The list of future defence spending includes 13 main programmes, among which are: air defence system, helicopters, UAVs, command-and-control capabilities, and modernisation of the Navy.

Our own national efforts fit into the broader NATO/European context. Some good examples are: air and missile defence (AMD) and helicopters. Firstly, Poland plans to significantly upgrade its AMD system by 2022, and acquire, inter alia, 6 batteries of the medium-range air defence system with lower-tier missile defence capabilities (codename Wisła). These new capabilities, together with the American missile defence base on the Polish soil in Redzikowo, will contribute to the security of the entire Alliance as parts of the NATO BMD system.

Secondly, the process of purchasing 70 helicopters has already started. In particular, the Ministry of National Defence plans to buy 48 multirole transport helicopters for the land forces, 6 anti-submarine warfare (ASW) and 6 maritime search and rescue (SAR) helicopters for the navy, and 10 search and rescue examples for the air force. This purchase will strengthen mobility and action support capabilities and is important for potential future engagements in international operations.

This major technical upgrade will have to be implemented in cooperation with foreign partners. What should be underlined is that Poland wants new technologies to be transferred to our defence industry companies. We are not interested in simply assembling parts of the armament. Independence of our defence production and technological strengthening of our companies are an integral part of the Polish security capabilities. Our aim is to make Polish defence industry a strong partner in the European construction process.

The fulfillment of the modernisation plan will let us exchange a big part of currently used, obsolete, military armament. Nowadays modern equipment constitutes 22% of the totality. We hope that this number will grow in 2022 to 65%. This ambitious goal of the Polish Government is treated as necessary investment in our national security, as well as in the security of our allies and NATO capabilities.

Poland's philosophy for our Armed Forces was described by Prime Minister Donald Tusk: "Our efforts are to offer Polish citizens a safe haven, i.e. life in a country that is protected by brave, highly skilled soldiers with state-of-the-art equipment."As a reliable ally, Poland spares no effort to advance the security of the Euro-Atlantic area.

We are a credible NATO and EU member, which not only enjoys the security benefits deriving from the membership, but also is willing and able to contribute.

Chapter 13

Deterrence and Stability in the 21st Century

First Deputy Minister Daniel Kostoval
Ministry of Defense of the Czech Republic

Regarding Deterrence

I would like to share with you a Czech perspective regarding deterrence and strategy stability in the 21st century. The notion of deterrence is necessarily linked to the nature of the security environment. If somebody must be prevented from acting against security and defense interests, there is a need for deterrence. Unfortunately, assessments of the security environment now and in the future—up to 2030 for example—demonstrate a strong need for a functioning deterrence system.

Having said that, it is only natural that deterrence is a co-pillar of NATO's collective defense and the Czech Republic supports it strongly. Global power is shifting towards an increasingly aggressive multi-polarity. Actors are becoming more heterogenous. There is increasing access to technology, proliferation of weapons of mass destruction (including nuclear weapons), resource scarcity, centralization of global processes, faster speeds of communication, pressures on traditional states (with fractured identities and broken states), and free riders on multilateral institutions and international law.

This short list of important trends—which is by no means complete—shows the need to define and plan deterrence and defense in the context of a highly fluid, complex, and unpredictable security environment. Deterrence for the 21st century thus must be broader than simply relying on strategic nuclear weapons. It must be an aggregate concept: a mix of policies, postures, procedures and capabilities. Those capabilities should be military, politico-military, and also civilian. To put it simply, a functioning system of deterrence depends on credibility. In other words, we as the Atlantic Alliance, must demonstrate two things: first, we must demonstrate the political will and determination to employ the concept in extremis. Second, we must be seen as actors who possess real and deployable military capabilities. These capabilities must include nuclear armament, both strategic and sub-strategic, as well as conventional state-of-the-art capacities.

Regarding Nuclear Capabilities

As to the nuclear dimension of deterrence, I would like to point out that this element is smaller than ever before. Yet, it is still indispensable. Sub-strategic nuclear weapons give us additional flexibility. At this moment, it is important to point out that NATO's deterrence is based on a flexible response strategy. Our aim must be to have at hand as many tools as possible in order to have as much flexibility as possible. I would like to draw your attention to two new elements that we should consider as already belonging to our flexible response strategy.

A Flexible Response Strategy

The first element is missile defense. Despite our efforts to make non-proliferation commitments a reality, the proliferation of weapons of mass destruction and missile technology continues. Missile defense will reduce the relevance of nuclear weapons and will help give us a wider range of options when under threat or even attack.

The second element is cyber capability. For the first time, a NATO defense ministerial meeting has been dedicated to cyber defense. There is an emerging consensus that cyber space—just like land, sea, and air—is another space that must be included in Article 5 operations or scenarios. It is important to include cyber capabilities in our concept of deterrence based on a flexible response strategy for the following reason: we are in a multipolar world, so we cannot rely on symmetrical approaches as we did during the Cold War. In addition, our strategy needs to include a very strong political-diplomatic track. This track must focus on non-proliferation policy, arms control, and disarmament. But, at the same time, I would like to emphasize the need for a focus on the ability of the Euro-Atlantic community to enforce the rules of international law. I am convinced we are not doing enough in this regard, and it is especially in this politico-diplomatic dimension that we can demonstrate our political will.

Advancing our security and defense interests. As to our European ability to advance our security and defense interests, I would like to make a final appeal. For deterrence to be effective, it must be credible. Yet, we Europeans are doing exactly the opposite in the defense area: we have been making ourselves constantly less and less credible. As a cause, I could easily focus on our lamentable defense spending. In my view, however, defense spending is a real problem but not a crucial one. Our true problems are (a) the lack of the political will to act and (b) the way our defense budgets are allocated when we view them through the lens of deployability. A typical example is the implementation of the battle group concept in the European Union. Because there is no political will, battlegroups exist mainly on paper and, as a direct consequence, they are not deployable. At the same time, we actually have enough military units to make two battlegroups that actually would be deployable—which corresponds to the current level of ambition of the European Union.

As for the Czech Republic, it is vitally important for us to be able to rely on collective defense and crisis management capabilities in the Euro-Atlantic area. At the present time, we are doing our best to contribute adequately. Although the Czech Republic is not spending 2% of its GDP on defense right now, the defense budget was stabilized for the next few years with the intention of slowly increasing it in the years that follow. We continue to have the same political-military goals as before the economic crisis and part of the solution to this budget crisis is international cooperation. In this context, I would like to mention that we are with the other three Visegrád countries in putting together the EU-Visegrád battlegroup, which will be in standby mode and really deployable in the first half of 2016. Moreover, we want to ensure that this battlegroup is deployable, including an airlift component.

Chapter 14

Doing More with Less—the Management of Defense under Austerity

State Secretary Tamás Vargha
Parliamentary State Secretary, Ministry of Defence of Hungary

Recovering from Historical Setbacks in the Defense Budget

It is an honour to be invited to this distinguished workshop and I appreciate the opportunity to brief you on the effects of austerity on the management of defence, with a special focus on our experience in Hungary. Our defence budget—like that of other Allies—has suffered a significant setback in recent years as a result of the long-lasting financial storm of the European sovereign debt crisis and the enduring financial austerity that it has produced. This has been coupled with the constant lack of financial resources, which the Hungarian Defence Forces (HDF) has experienced for years, nearly bringing the whole defence sector to the edge of bankruptcy.

The Hungarian Government and the current leadership of the MoD began its work three years ago with a new approach towards defence. Despite the roughly 29% decrease in our defence expenditures since 2008, we were able to maintain the same number of troops abroad (1,000 personnel) as in 2008, which is one of the highest ratios in NATO compared to the number of deployable troops. In this respect, let me just highlight our participation in the ISAF mission in Afghanistan. In early summer 2010, our contribution was around 350 troops, in spring 2013 (before the withdrawal from our PRT) it was around 550 troops, and at present it is 432 troops. Besides participating in missions in most areas, we maintained the level of exercises, we even increased flying hours, and we not only prevented the HDF from losing more capabilities but also gained new ones.

Our commitment to capability development is supported by the fact that, under the present cycle of NATO's Defence Planning Process, Hungary accepted every capability target allocated to us, which has never happened during the entire period of our membership in the Alliance.

The development of the voluntary reserve system also contributed to the increase of the military capabilities of the Hungarian Defence Forces. It provides a framework for the training of our fellow countrymen who wish to take an active role in the defence of the homeland, permitting their employment in peacetime under a special legal provision. In 2010, we had only 17 personnel in our reserve forces, but now we have 4,700 troops available for homeland security, operational contributions, and disaster relief tasks. Our goal is to increase their numbers to 8,000 by the end of next year. The importance of their service to the country was demonstrated during the recent heavy floods of the river Danube, when more than 1,500 reservists helped on the dams to hold back the water.

How the Hungarian Defense Ministry is Coping with Austerity

Since the title of my presentation is "Doing More with Less," let me shed some light on how we tried to cope with austerity in order to preserve our capabilities and our contributions to missions in times of economic hardship.

First of all, we had to cut fat, which was the prerequisite for increasing efficiency. We had to look for areas where we could streamline the structure and minimise costs. The guiding principle was to not touch military personnel serving as troops, so we downsized the bureaucracy—but in a very different way from the proportional reductions that occurred during the massive cutbacks of our military personnel over the last 20 years. This reduction of the "overhead" by around 1,200 personnel resulted in a huge decrease in administrative costs.

The reform of the pension system (no early retirement) and a total freeze of wages (in some cases wages were actually decreased) were the most painful measures.

We have reorganised the MoD, along with the structure of the General Staff, reduced the number of defence agencies and institutions as well as merged the military intelligence service and the military counter-intelligence service. We have reviewed previously outsourced tasks and services as well; just to give you an example, we made considerable savings by replacing the private security companies that previously guarded our military facilities with reserves.

We reviewed our procurement contracts; most importantly, we renegotiated the leasing contract for our Gripen fighters with Sweden in order to prolong the leasing period until 2026 with considerably more advantageous conditions. By decommissioning the costly MIG-29s, we were able to concentrate our recourses exclusively on our new Gripens.

In order to unify the budgetary resources allocated to the training and education of future state employees, we merged three separate institutions to establish the National University of Public Service on 1 January 2012. This elite institution is responsible for the high-level training of military and police officers as well as specialists of state administration. In parallel, we reinforced the military character of the national officer training.

The grave financial situation triggered the need to generate as much income as possible. We therefore sold defence land and buildings that were no longer used by the armed forces, and we liquidated excess stocks and equipment. The income realised in this way is being used for capability development.

Harsh Economic Conditions Require Multilateral Cooperation

We believe that the harsh economic situation requires increased multinational cooperation. This does not necessarily lead to savings, but it does lead to delivering capabilities more effectively. For this reason we are committed to NATO's Smart Defence and Connected Forces Initiative as well as to the EU's Pooling and Sharing initiative.

Beyond the cooperation within NATO and EU frameworks, we attach special importance to regional cooperation as well. The geographical proximity, common challenges, similar problems and similar force structures can provide a solid basis for cooperation. Addressing these challenges effectively requires a coordinated approach. There are a number of considerable examples of regional cooperation, like NORDEFCO, the BENELUX cooperation, or the Visegrád cooperation (V4) where we assume the rotating presidency next week. Our cooperation within the Visegrád Group and within a wider Central European circle provides an excellent foundation on which we can build cooperation in capability development. Among others, the initiative of the V4-based regional CBRN battalion and the V4 EUBG are good examples. These will also serve as a driver for common training and education and as a firm basis for facilitating the implementation of the Connected Forces Initiative.

We should not forget, however, that multinational or regional cooperation is not a "panacea," but just part of the solution; ultimately we must spend more on defence. All the measures mentioned above are useless unless we can provide adequate resources as well as a reliable forecast of the resources that will be available in the future. I cannot agree more with NATO Secretary General Anders Fogh Rasmussen who, in preparation for the Defence Ministerial Meeting earlier this month, said that we must hold the line on defence spending during the years of economic austerity. And we must politically commit ourselves, even now, to increasing spending in the future once financial conditions make it possible.

This is exactly the approach that we are taking: for the first time ever, the Hungarian Government has passed a resolution declaring a firm resource commitment for the coming planning period. This resolution stops the decrease in Hungary's defence spending and promises that, for the next three years, defence spending in nominal terms will not fall under the level of spending in 2012. The Resolution also guarantees an annual increment of 0.1% of the GDP beginning in 2016, achieving a roughly 1.4% GDP share for defence expenditures by 2022 as a result. While this still does not meet the 2% goal of the Alliance, our spending will converge to the average of the European Allies. Counting on the guaranteed financial increment, we plan to spend 2.7 billion euro for capability development; if used rationally and in accordance with our priorities, this will sufficiently meet the requirements stemming from our level of ambition.

Conclusion

To summarize, I think we have made considerable achievements, despite the budgetary setback. We have maintained our commitments in operations, our level of ambition is unchanged and I firmly believe that appropriate resources will be on hand beginning in 2016 in order to effectively enhance the capabilities of the Hungarian Defence Forces. In the meantime we are actively seeking new and innovative ways for multinational and regional cooperation.

Chapter 15

Transatlantic Security's New Normal: the Dilemma of Getting Smart, Connected and Comprehensive, or Going Home

Ambassador Lawrence Butler,
Civilian Deputy to the Commander and Foreign Policy Advisor,
U.S. European Command, Stuttgart, Germany

Good morning and my compliments to Dr. Roger Weissinger-Baylon and thanks to the French Ministry of Defense, NDU and NATO for the opportunity to challenge you today. This is a fitting and magnificent setting to tackle key issues facing us and I am honored to be invited to participate.

Dealing with the New Normal—and the Risk of Stove-Piped, Dumber, And Disconnected Forces

Here is my objective today: transatlantic defense and the defense of the transatlantic space are two different things. The former was the entrenched defense bureaucracy paired with the defense industrial establishment; the latter is our new normal. How we achieve this is what keeps me up at night.

Indulge me while I point out what my position is—a civilian who is one of the two deputy commanders of the American Combatant Command, or COCOM, responsible for Europe, the U.S. European Command, or EUCOM. I work at the intersection of defense, diplomacy and development, often called the Comprehensive Approach. Three of the six geographically aligned U.S. Combatant Commands that are primarily engaged in full spectrum security cooperation and building partner capacity have civilian deputies commanders. This is a new development representing an important evolution in how the United States addresses security challenges in the 21st century.

Europe is a mature region for America and therefore unique, which argues for a different type of COCOM. EUCOM in 2013 might well be a hybrid functional/geographic combatant command. It is functional because in normal times our role is to organize, train, and equip Allies and Partners for combat in NATO-led operations and in coalitions of the willing. ISAF is an excellent example. The increasing convergence of our bilateral security cooperation programs, NATO's capability targets, and our Foreign Military Sales program is indicative of the "functional" aspect of our COCOM. Israel, the Baltics, the Balkans, Eastern Med/Levant, and the Black Sea/Caucasus region serve as ample evidence of the challenges to deliver on our geographic responsibilities.

This is as hard as it sounds, and I need your attention to the possibility that instead of smart defense, connected forces and comprehensive approaches to complex stability operations, driven by declining budgets and tunnel vision, the transatlantic security relationship could devolve into stove-piped and dumber defense that is disconnected, along with the disappearance of U.S. forces in Europe. The consequence would be disjointed, fragmented responses to conflict and post-conflict situations. And we, Europe and America, could be equally at fault for allowing this to happen.

America and Europe are fundamentally committed to freedom. We are each other's best allies and friends. We are about liberal democracies, human rights, free press, and market-driven economies. And together we have demonstrated the will to defend it. Nothing in the past 65 years of NATO has changed that fundamental compact, even as the threat of a Soviet invasion has evaporated.

The security challenges confronting the Transatlantic Alliance are more diverse and demanding than during the Cold War and will only get harder and more complex. Afghanistan, the intervention in Libya, Mali and the Benghazi attack last September all required not just capabilities but more importantly, a true, flexible and nuanced comprehensive approach that in future operations may prove valuable, efficient, and cost effective in addressing security challenges.

Fifty-seven years ago, my Army officer father moved his family to the Fulda Gap and, as an armored infantry company commander, was prepared to risk his life to protect Europeans. I knew firsthand the tension of the imminent threat of war in those days when Europe was undergoing a political and economic renaissance, protected by a NATO/American shield. The sense of shared purpose of the Cold War has given way to an understanding that, while Russian tanks are no longer going to blast their way into Europe's democracies and an American brigade in Berlin is not longer the tripwire for a world war, old and new threats to our shared security exist from a number of sources. This has led to the evolution of the meaning of transatlantic defense.

Therefore, I was dismayed at opinions published in recent days. Spiegel asked whether there is still a shared vision, as evidenced by President Kennedy's Berlin speech. This was followed by sharp criticism from a German TV outlet, "Care packages and the airlift were yesterday," and then it cited fracking as one of today's most thorny issues with America—really?—concluding with "welcome to Germany, President Obama."

This neatly captures the reality that time and circumstances have moved on, and with it the perception of what threatens our democracies and prosperity.

European security is not permanently secure. No one's is. Take a look at your neighborhood. Events in Syria and the broader Levant, the Balkans, or North Africa—or home grown religious extremism—can and do impact the welfare of your citizens. And you can be attacked by someone sitting in the comfort of his own home, via cyber.

With our huge economic interdependence in mind, America's security depends on Europe's, and vice versa. Our futures are tightly intertwined by the millions of jobs we share, by our cultural and academic and tourist exchanges, and fundamentally by our shared values and experiences. NATO lets our business people, the creators of jobs and wealth, focus on those core tasks. America's commitment to NATO is the cornerstone of this. Will it continue to be so?

Criticism and questioning of America has a transatlantic counterpart. This came with a recent piece in Foreign Policy magazine, arguing that all U.S. troops in Europe should come home now, that it is time for you Europeans to shoulder all of your defense burden:

> "NATO has become politically unmanageable, militarily dysfunctional, and now risks strategic irrelevance…EUCOM has become largely a supporting command; it once had a major role in Persian Gulf security and broader contingencies like Afghanistan, but CENTCOM now has the lead for operations in the Gulf and South Asia. It has pre-deployed assets in the Gulf that no longer make European deployments essential…The bulk of U.S. land forces in Europe would be decommissioned, brought home, or allocated to other theaters. Meanwhile, the United States should rotationally exercise with its European allies, but primarily on its own territory."

Last week, a failed amendment to a defense budget bill in Washington singled out a U.S. brigade to be brought home from Germany. Upcoming decisions to reduce the size of the U.S. Army will only increase political pressure to bring troops, and the jobs they create, home.

In the age of sequestration and economic distress, the latent pressure for America to completely pull its forces from Europe becomes more real, active, and attractive. And we, Europeans and Americans, have to work harder and smarter to make the case for why this would be the worst thing we could do.

Smarter and More Comprehensive Defense

Since T-72s are not poised to roll across the German plains and my father's soldiers are not dug in to thwart that, what are the security challenges that make the U.S. presence in Europe and NATO not only relevant, but vital to protecting our shared democracies and prosperity? And in a sustained era of declining defense expenditures, how do we efficiently and effectively provide for that? There is an umbrella concept that captures this: globalization and convergence.

Former SACEUR Jim Stavridis recently revealed that what worries him is the convergence of criminal networks with terrorism, citing narco-terrorism and cybercrime as examples because we are so ill-equipped to respond. His answer is not less military, but different capabilities—special forces, cyber capabilities, and remotely piloted vehicles. Many of these challenges straddle the border between law enforcement and military operations, which present challenges to Americans and Europeans. The proximity of the Levant, with the Syrian civil war and its nearly 100,000 victims and lots and lots of chemical weapons, ought to keep European leaders up at night. Instability in the Maghreb leads to terrorism and mass migration. All these demand smarter, more comprehensive defense, not less.

Let me add to this the potential demands on our defense forces posed by: the new doctrine of responsibility to protect and mass atrocity response; man-made and natural disasters; contradictory legal bases; evolving international law; complex and dense IGO and NGO networks; and last and not least, budgets.

The Comprehensive Approach and EUCOM

My personal experience with the comprehensive approach in the Balkans, where the military, governments, intergovernmental organizations and civil society joined forces to end conflict and promote stability, and also with the mixed civilian-military Provincial Reconstruction Teams of both Iraq and Afghanistan, have demonstrated the value and necessity of bringing military and civilians into a common enterprise. I know how easily those lessons can be forgotten. In Macedonia, I teamed with a French EU special representative, a Dutch NATO civilian representative, a Canadian OSCE head, and a German NATO general (who was replaced by an EU general) to help the country implement a peace agreement. That is what right looks like.

I can ask an infantryman to promote good governance and development during a military operation, and he will do his best to deliver, but he will not be as effective as a civilian counterpart trained in these fields. And conversely, we do not want our diplomats and development officers carrying guns.

But long before we get into an actual operation, isn't it better to prime the pump for the so-called comprehensive approach, just as our militaries train together in peacetime both as a deterrent to conflict, but also to be more effective in actual operations?

United States European Command has about 100,000 uniformed military and civilians serving in Europe. At EUCOM we have embedded representatives of a dozen civilian agencies that deal with everything from development to energy. These men and women are full partners with their defense counterparts in supporting more effective security activities that have obvious civilian implications, always in concert with American Embassies in the 51 countries we cover.

When a logistics, disaster or humanitarian response activity is involved, they link us to the lead offices responding to help our partners and help us be more efficient with our resources. We often are the only ones who can get to a disaster, but we need the partners to handle the civil response.

We are developing relationships not just with other countries, but with organizations such as NATO, the EU and the OSCE.

At their EU Mission in Brussels, France is in the early development phase of a decision support platform for the collective use in planning and executing comprehensive action. If achieved, this would be a best practice worthy of emulation.

Across town in Brussels, NATO's Civil Emergency Planning can be a positive way to highlight progress in aspirant nations; by Pooling and Sharing our resources, we can leverage HADR exercises—key to being ready for real emergencies—whether by linking the Euro-Atlantic Disaster Response Coordination Center (EADRCC) at NATO to our own State National Guard Partnership Programs, or with the EU. This may not sound like a military mission, but in one Caucasus country, an Army National Guard unit has linked one of its State universities to work with host nation authorities to promote agricultural development, which contributes to social stability and lowers the risk of conflict. The EU also has similar goals for that country. Image linking those two efforts?

Individual nations are making internal progress on developing Comprehensive Approach tools; however, the collective awareness and development of those national advances is still problematic and we are open to ideas on how to address this gap. When countries are so preoccupied with domestic issues, it can be hard to concentrate on new, external initiatives. Nonetheless, we should not be daunted by the bureaucratic challenges. In particular, we need to break down barriers both in Washington and in Europe that are making it difficult to work with the EU, which has both the mandate and the resources to partner with.

Six Conclusions

- We are each other's proven partners; when things go wrong, who can the Americans or Europeans look to for help?
- NATO is a proven, expeditionary partner in a challenging world. Campaigns like ISAF or in Libya are not viable when we go it alone. They require transatlantic cooperation and solidarity.
- Speaking to American audiences, a strong U.S. presence in Europe and unflinching leadership of and commitment to NATO frankly may be the key reason why NATO allies and partners risk precious blood and national treasure to be with us in Afghanistan. Because we are still here, Europeans are "there" (Afghanistan).
- Fourth, Europe sits next to three of the four major global flash points: the Levant, the Maghreb, and Eurasia—it is the crossroads and heartland of the world.
- In this connection, Europe provides proven, ready, well-postured bases from which to support operations vital to our collective security. Whether the U.S. provides aerial refueling support for operations in Mali—flying from an American

base in Europe—or whether it responds to crises around the Mediterranean or the Middle East, we can rely on billions of dollars worth of security-related infrastructure; walking away from this would be irresponsible.

- And, finally, we have to do all of this smarter, not just with connected forces and Pooling and Sharing of vital enablers and joint exercises, but by cementing the hard-won lessons of bringing stability to conflict and post-conflict situations. This is NATO's Comprehensive Approach and EUCOM's emphasis on inter-agency, whole of government and whole of society solutions to problems that cannot be solved with the application of military power alone.

The security challenges confronting both sides of the Atlantic are more diverse—and more demanding—than they were a decade ago. The intervention in Libya, the crisis in Mali and the terrorist attack in Algeria are clearly interlinked and require a more comprehensive approach. In such a context, the integration of new 3Ds of security—development, diplomacy, and defense—may prove to be valuable in addressing security challenges more effectively.

Chapter 16

NATO Operations in Afghanistan

General Hans-Lothar Domröse
Commander Allied Joint Force Command Brunssum

The Broader International Context of the ISAF Mission

Today, I will talk about NATO's current and future operation in Afghanistan. I will deliberately stay clear of describing the latest developments in the diplomatic arena, for example the possible talks with the Taliban. NATO's position on that is that reconciliation will ultimately have to be reached through an Afghan-led mechanism. Meanwhile we need to support all efforts to facilitate the process.

As you know, ISAF is the largest military operation in modern history, with currently 50 troop-contributing nations. In a wider sense, the International Community—including dozens of donor nations such as Japan and Russia—is also heavily involved in the development of Afghanistan. In sum, it is a massive civil-military comprehensive effort of the International Community which reflects the collective desire to create stability in the region for the benefit of all, but especially for the Afghan people. As we engage in this huge effort with blood and money, we remind ourselves of the fact that our security in the West is a function of stability in Afghanistan and I commend the men and women of the International Community, be they military or civilian, who are dedicated to this task. They make the world a safer place.

As Commander of Allied Joint Force Command Brunssum, which is one of NATO's two operational joint headquarters residing under the Supreme Allied Commander Europe, I am the responsible "out of theatre" Commander for NATO's engagement in Afghanistan. The International effort in Afghanistan is of course not an isolated operation as that nation is located in the middle of an important geostrategic area where opposing regional and global interests converge. Some of the relevant nations, as you know, are nuclear powers. Some harbor enemies of the Afghan state and of our forces.

Contributions of India, Russia, and China. Afghanistan borders on Iran and Pakistan, and in both nations large numbers of Afghans still reside as a result of earlier conflict—a burden for all concerned. India, Russia and China are major powers in the region. All three nations are active in the development of Afghanistan in different ways. Many initiatives exist that enhance regional cooperation.

We note with appreciation that Russia continues to support ISAF and the NATO efforts to build the Afghan National Security Forces (ANSF). I especially mention the Russian support of the Afghan Air Force through training of Air Force technicians and delivery of spare parts to help the Air Force to operate its helicopter fleet.

Another vital role played by Moscow is assisting NATO in the reverse movement of ISAF troops by air and land including through the so-called Northern Distribution Network that uses the railway system through the Afghan neighbors and Russia right up to the ports of our Allies on the Baltic Sea. My political masters in NATO will be looking for the continued support from Moscow for ISAF and as we transform into the new NATO mission in Afghanistan on January 1, 2015.

Implications of the U.N. Mandate. As we discuss the international context of the ISAF operation, we must remind ourselves of the origin of the mission. ISAF was created by the International Community in 2001 based upon U.N. Security Council Resolution 1386. That document is a useful read. In 2003, at the request of the U.N., NATO took over command of the ISAF mission, especially with the intent to provide continuity for the peacekeeping effort. And so it still is. I am sometimes greeted by surprise when I repeat that NATO, until the end of 2014, is executing a mission in Afghanistan at the behest of the U.N. It also places the mission in its correct legal context. Two very fundamental pillars of the mission ensue from the U.N. mandate:

- Pillar One: Afghanistan is—and has always been—a sovereign nation. ISAF has no authority over Afghan institutions.
- Pillar Two: ISAF is in Afghanistan to assist the Afghan government.

It is important to note these points, as they also have determined the progress of our mission. ISAF is of a fundamentally different nature from SFOR and KFOR. In the latter two missions, the International Community was in control. In Afghanistan, it is the government of Afghanistan led by President Karzai that is in charge. We also need to note that ISAF works alongside and in cooperation with the American coalition of Operation Enduring Freedom (OEF), which has been legally endorsed several times by the United Nations since its start in 2001.

Linking the International Community and the Afghan Government—The "Bonn Process." Over the last twelve years, the engagement of the International Community in Afghanistan has transformed not only as a result of the security situation but also of many conferences and agreements. Sometimes called the "Bonn-Process," this sequence of international conferences includes the meeting in Tokyo in Summer 2012 where a crucial document, the Mutual Accountability Framework, was approved. In it, the International Community made an enduring commitment to the Afghan people while at the same time agreeing with the Afghan government to make efforts and funding dependent on the performance of the Afghan government institutions. This link between the International Community and the Afghan government is crucial as NATO moves into its new mission. At the same time a failure to enact the work planned under the Mutual Accountability Framework could have severe effects for the population of Afghanistan, and ultimately affect a proper establishment of human rights and the rule of law.

While underlining the absolute need for synergy between the military operations conducted by the Afghan National Security Forces and ISAF on the one hand, and the development efforts of the Afghan government and International Community on the other, let me return to the military mission. As per its mandate, the purpose of NATO's operations in Afghanistan has been from the beginning to extend the authority of the Afghan central government and to create an environment conducive to the functioning of democratic institutions and the establishment of the rule of law. On 18 June, we reached an important new stage as tranche 5 of our transition plan was announced. This entails that Afghan Forces are now fully in the lead on security operations in the country. They will also be responsible for providing security for presidential elections next year leading to a democratic handover of legitimate power. ISAF will support the Afghan National Security Forces in an advisory and in-extremis capacity.

As we scale down ISAF operations according to plan, NATO's main effort will remain the building of sustainable Afghan national security forces led by legitimate Afghan security institutions. The ANSF development continues to focus on enhancing the capability and professionalism of the Afghan National Army (ANA) as a national fighting force and the Afghan National Police (ANP) as the Afghan law enforcement body. Meanwhile, the ANSF continues to improve in capacity and operational effectiveness, already leading the majority of all conventional operations.

The ANSF has achieved more than 95% of its end-strength objective of 352,000. The focus of force development will shift from quantity and growth to quality and sustainability. On 18 June, with the announcement of tranche 5, the gradual transition of lead responsibility for security from NATO troops to the Afghan National Army and Police was fully implemented. However, despite its continued improvement, the ANSF continues to struggle in terms of sustainment, attrition, leadership, and enabler capabilities.

Mission Handover to "Resolute Support" in 2014

Overall in Afghanistan we see signs of progress and achievements in many fields, in education, trade, health, roads, electricity, and telecommunications. Many Afghans are gaining access to electricity for the first time in decades: there are more children in school than ever in Afghanistan's recent history, and 8,000 km of roads were constructed, connecting the people, producers and markets. Altogether, this justifies a cautious optimism. To maintain and secure these achievements, NATO decided in Chicago in May 2012 to stay committed beyond 2014. This will be done through a completely new mission, with a significantly changed character: it will be a non-combat, train, advise, and assist mission.

The handover to the new mission, called "Resolute Support," will take place by the end of 2014. Provided with a force of approximately 10,000 (+), the intent is to follow a hub and spoke model, with the capital Kabul as the hub and northern, southern, eastern and western spokes. According to mission progress, we envision to reduce our engagement to the hub within approximately two years. All this planning is still depending on the commitment of the Troop Contributing Nations to Resolute Support, not least that of the U.S. It is also vital that the new mission be underpinned by the necessary instruments of public international law, such as an invitation by the Afghan government or a Status of Forces Agreement between NATO and Kabul.

The Need for Continued Support from the International Community

At least as important will be that the other agencies of the International Community continue to work with the Afghan government on development. In that context, many non-security tasks that are currently conducted by default by ISAF will have to be taken over by the Afghan government or by International Organizations or NGOs. I encourage you all to help work towards this transition and call upon the creativity of donor nations to step into the breach.

Limited institutional capacity remains one of the greatest impediments to long-term stability and sustainable security in Afghanistan. As I described, the Tokyo Mutual Accountability Framework continues to be the principal mechanism by which the International Community links financial support to improved governance. In the future, sustainable security and stability in Afghanistan will depend on the continuing support of the International Community and the confidence of the government and population in the International Community's commitment. This support will have to comprise funding, i.e., for the ANSF (in need of $4.1 billion per year until 2017 with $3.5 billion in pledges already available), for the presidential elections and within the Tokyo Mutual Accountability Framework ($16 billion for development until 2015).

Additionally, we need the provision of military personnel and capabilities to implement Resolute Support, as discussed earlier. As this mission is focused on training of and advice to the Afghan Security Institutions, adequate numbers of advisers will have to be found, including for the MoD and MoI security ministries. Efficient coordination with other agencies remains essential.

The common goal of the Afghan Government and the International Community is a secure, just, stable, and prosperous Afghanistan, based on a functional democracy, a professional and efficient civil service, common access to justice, and the rule of law. NATO's follow-on engagement will enable the Afghan Government to preserve stability and the Afghan Security Institutions to protect the populace/people. Increased stability in Afghanistan will create trust and confidence with all neighbors, strengthen mutual interdependencies in the region via economic exchange, and foster a modest level of well-being.

I had the privilege of gaining personal experience in Afghanistan while serving in different military positions and I am convinced that, when united with other agencies of the International Community, we are in the position to safeguard progress, support elections, economic development and the reconciliation process. We will thus also demonstrate NATO's relevance to global security, maintain our reputation in the world and, at the same time, prove our ability and will to respond to global challenges.

Chapter 17

Afghanistan and NATO: Ten Years of Cooperation

Ambassador Dr. Assad Omer
Ambassador of Afghanistan to France

Our achievements since 2001, after the fall of the Taliban, represents nothing less than a historic transformation, especially if we take into account the historical context of physical, social, cultural destruction and suffering that the past conflicts have imposed on the Afghan population for more than three decades. It has now been more than a decade since Afghanistan has begun a new era of respect for democratic values and human rights. Indeed, since the Bonn Agreement in 2001, the presidential and parliamentary elections were held twice. Moreover, freedom of expression is guaranteed.

Our Achievements

Afghanistan has achieved tangible results in all areas. Let me give some examples:

- The primary objective of both Afghanistan and our international partners is education. Currently, nearly 9 million children attend school. This represents 70 percent more children enrolled than in 2001, and 40 per cent of these children are girls. Within the coming three years, all children of school age will be in school. This year, institutions of higher education received more than 90,000 students. Both are a record in our history.
- The place of women in society has improved, Afghanistan ranks 22th worldwide in the participation of women in state bodies when just 12 years ago, there were none.
- The reconstruction of roads and airports has also made remarkable progress. It is perfectly possible to reach large and medium cities by road or air. Links with the outside world are greatly facilitated. Between Europe and Afghanistan, dozens of flights per week provide the opportunity for Afghans and foreigners to travel.
- Telecommunications is also an area where there have been dramatic developments. In 2001, some fixed telephone lines were still working, but calling abroad was nearly impossible. The infrastructure was completely destroyed or severely degraded. Today, 20 million Afghans have access to mobile phones. Five telecom companies are operating in Afghanistan. More than 80 percent of Afghanistan is covered by phone services and the Internet is available in all major cities.

At the same time, we are approaching an important event that is worth mentioning: the April 2014 presidential election. President Karzai completed his second and final term. The Afghan government is doing everything necessary to ensure free, fair and credible elections, where all eligible Afghan citizens can vote. The success of these elections will strengthen the roots of the young Afghan democracy and grow the historic achievements of the last decade.

Afghan Security Forces

Currently, the Afghan security forces have reached 352,000 people. In this area, Afghanistan has made significant progress, which allows us to bring the transition process of security responsibility from NATO to Afghan forces in its final phase. This is a clear demonstration of the strategy and success of the transition process set up with our partners that will end at the end of next year.

Afghan security institutions are more aggressive and more capable than they have been over the last ten years, taking a more active part in the responsibility for security in Afghanistan. Actually, it was on 18 June of last year that President Hamid Karzai announced the transfer of the national security responsibility from NATO to the Afghan authorities. The transition was announced at a ceremony during which NATO forces, in the presence of Secretary General Rasmussen. handed over control for the last 95 districts. Consequently, Afghan security forces have taken control of all security operations. It has been a long way to reach this stage since 2001 and it will remain as a testament to our strong partnership with the international community.

Along with all these developments I have just described, the Afghan government is pursuing a comprehensive effort to find a political solution to end the violence. It is now apparent that the vast majority of the Afghan people strongly supports the political solution.

What we need now is real and honest support from external stakeholders, in particular, the countries of the region. We hope that this will illustrate practical support in the weeks and months to come in the interest of peace and security in the region.

The Economy

We are determined to maximize the potential of our natural resources to strengthen our economy. In addition, we have given priority to foreign investment and building adequate infrastructure. These efforts will enable us to play a key role in developing and strengthening our regional economic cooperation, resuming our historical role as a crossroads between Central Asia, South Asia, the Middle East and the rest of the world.

In this context, we appreciate the commitment of substantial assistance from the international community at the Tokyo Conference to fill the budget deficit in the Afghan national budget beyond 2015. This would give us the opportunity to increase our national income by furthering the development of the Afghan economy and attract investment in our key sectors such as mining, agriculture, transport and transit.

The Immediate Challenges

The greatest challenges to peace and stability in Afghanistan are terrorism, extremism and illegal drug trade, at regional and international levels. Our common threats require cooperative solutions. We work with countries in the region and have concluded strategic agreements with other partners for a comprehensive response to these threats.

We know that the fundamental interests of the region (security, stability and prosperity) are organically linked to each other. Stability and prosperity will come to the region with a solemn sense of shared responsibility, sincere and pragmatic. It is very important to build the confidence necessary to provide such economic cooperation between the countries of the region.

In addition, we will keep the momentum going and implement infrastructure projects for energy as well as roads and railways interconnections.

Afghan and French Cooperation

These many accomplishments would have been impossible without the partnership between our government and international partners including France. The Afghan people are deeply grateful for the continued support and assistance provided by France. This long-term cooperation has brought tangible changes in the lives of Afghans, including capacity building of an Afghan army and police, the health sector, agriculture and justice.

The 90-year relationship between Afghanistan and France can only look ahead to the future. The two countries have signed a Treaty of Friendship and Cooperation in 2012 for twenty years.

Concluding Remarks

In concluding my remarks, I would like to say that as we are approaching the drawdown of international forces at the end of the transition in 2014, Afghans are looking at the post-2014 era with hope and confidence. We are making every effort and taking all opportunities to increase security, stability and prosperity not only for our people but also for the benefit of the region and the world as whole.

Chapter 18

Syria, Iraq and the Middle East

Dr. Stefanie Babst
Head, Strategic Analysis Capability of the NATO Secretary General and
Chairman of the NATO Military Committee

The wind of change that swept through the Arab world in the Spring of 2011 unleashed a new optimism. The uprisings in Tunisia, Egypt, Libya, Yemen and elsewhere in the Arab world seemed to reaffirm the long-held belief that democracy and freedom can also prevail in this part of the world. With the fall of long-standing dictators and the spread of mobilized public opinion, the prospects for a fresh start seemed to be within reach; and parallels were quickly drawn to the transformative events in 1989, which led to the collapse of Communist regimes in Central and Eastern Europe and the dissolution of the Soviet Union.

The Arab Spring: Premature Optimism

Our understanding of the nature of the Arab Spring was premature, and the drawing of historic parallels wrong. In Eastern Europe a large majority of people and political elites shared more or less the same vision for their future: they aspired to democracy, the rule of law, pluralism and market economies. They sought to join the European Union and NATO.

Yet in the Arab countries a joint, majority-based vision of how societies, governments and regional relations should look in the future remains elusive. Instead, the past two years have witnessed the emergence of new political forces, including but not limited to Islamists, a growing sectarian divide and power struggles between former and new political forces that, altogether, have led to heightened violence and regional instability.

Indeed, the Arab Awakening has many different faces: some countries have witnessed regime change (Egypt, Libya, Tunisia and Yemen), others are undertaking modest political reforms from within (Jordan, Oman and Morocco), while in Bahrain, Saudi-Arabia and other Gulf countries, demands for political change are met with a stern government crackdown.

The situation in Syria stands out in many ways. What started with peaceful public protests has turned into an extremely bloody regional proxy war that has produced tens of thousands of casualties and hundreds of thousands of refugees. To date, there is no clear resolution in sight but it is obvious that the conflict has profoundly destabilizing consequences that we can see on a daily basis for all of Syria's neighbours.

Setting the Scene: Six Points

Before we enter the discussion about Syria, Iraq, and what more we should expect from a second or third wave of the Arab Spring, let me make a few points to set the scene for our discussion together:

- *The old order in the Arab world is vanishing and will continue to vanish.* Regardless of how specific cases unfold in the future, one underlying reality seems clear: the apparent stability of dictatorships in the Arab region that has guided policy for decades has proven to be an illusion. The Arab Awakening has turned the "old order" upside-down. The 21st century communication technologies will continue to empower popular activism and challenge old and new governments to initiate genuine political and economic reform. Even Arab states that have resisted mass protests are experiencing a dramatic change in the nature and extent of public engagement with politics, from rolling weekly protests in Jordan to the rapid emergence of political arguments on Twitter in Saudi-Arabia.
- *The success or failure of the Arab Awakening will be measured by how successful the new or/and old elites can master the immense economic and governance challenges.* With the exception of the petro-rich Gulf states, the Arab region is in appalling economic shape: GDPs across the Levant are among the lowest in the world, growth rates are meagre, income

inequality is high, as is unemployment—ranging between 18% and 30% in Egypt, Tunisia, Jordan and Morocco. All Arab countries need to retool and modernize their economies. They need to create jobs, improve education, re-engineer public services, review their trade policies and overhaul financial structures and tax systems. Given that 60% of the population in the region is under the age of 25, the creation of jobs is one of the most pressing tasks. Estimates range between 52 and 80 million jobs that need to be created by 2020 in the region to keep pace with new entrants. At the same time, Arab governments will have to meet significant governance challenges—and I would just like to underline two: they must find new forms of power-sharing arrangements, encapsulating as many ethno-religious, secular and political groups as possible, and they must reform the security apparatuses, bringing them under civilian control and oversight. But it is clear that most of the Arab countries still have a long way to go on these two fronts.

- *The outcome of the war in Syria will define the future of the entire Levant region for many years to come.* In terms of strategic effects, regional implications and human suffering, the Syrian war has already outweighed the implications of regime change in Iraq that took place ten years ago. It remains conceivable that Assad's regime will continue to barely survive, severely weakened but still supported by Russia, Iran and Hezbollah. It is also possible that the armed opposition, with more assertive support from the West, will defeat Assad's forces but the results of such a victory are hard to predict. Perhaps a rebel victory would pave the way for a more inclusive state but there is also a strong likelihood that it could lead to a failed state with battling warlords harbouring Al-Qaeda extremists. Alternatively, the current stalemate may well persist for some time, deepening the sectarian rift and escalating what is de facto a regional proxy conflict with the Assad regime, Iran, Hezbollah and Russia on one side, and Qatar, Saudi-Arabia, Hamas as well as some Western countries on the other side. Under the most plausible scenarios, Syria will be a gaping security and political hole in the heart of the Levant for years to come, unable to establish state authority over its territory and population and with profound consequences on Lebanon, Jordan, Iraq as well as possibly Israel.
- *Iran will remain a key player in the region—as it will continue to pursue its nuclear and hegemonic aspirations. In the absence of a diplomatic resolution on Tehran's nuclear programme, capitals in the Levant, Iraq and the Gulf region will continue to fear a nuclear-armed Iran.* In particular, Saudi-Arabia might even seek its own nuclear deterrent that could lead to a volatile arms race in the region. Yet, there are at least two decisive factors that will determine Iran's future role in the region: first, the fall of Assad's regime and second, how newly elected President Rouhani will shape Iran's foreign policies. Indeed, the fall of the Assad regime would be a big blow for Tehran as it would lose its only Arab-state ally and an essential conduit for supporting Hezbollah in Lebanon. The old "axis of resistance" would break apart—which might lead Tehran to increase its political pressure on Iraq. As far as Rouhani is concerned, it is still too early to make serious predictions but there are a few reasons to be slightly optimistic. Rouhani likes to portray himself as a moderate, yet I do not think he is. We should not forget that he was one of the driving forces behind the crackdown of the 2009 revolution. Perhaps he is more of a pragmatic Iranian leader—if such a political label is helpful at all—who enjoys the blessing of the Supreme Leader and is well connected to all political camps and the security apparatus. Seemingly he is also more open to the International Community's concerns about the nuclear programme. We will have to see how Iran's relations with Washington and the regional players evolve in the future—but it is clear to me that a comprehensive effort to overcome instability in the region cannot be successful without Tehran.
- *While Arab-Israeli tensions are no longer the central driver of events in the Middle East, the failure to reach an Israeli-Palestinian peace accord continues to pose a fundamental challenge to both Israel's security and regional stability.* In the absence of a two-state solution, the geographic reality of Israeli settlements and continued occupation of the West Bank will inevitably collide with the demographic reality of an expanding Palestinian population. This, in turn, will make it difficult for Israel to maintain its identity as a Jewish state. I am not sure if more recent statements by some of Israel's top policy-makers help ease the frustration about the current impasse. Just a few days ago Deputy Defence Minister Danon and Minister for Economy Bennett (Jewish Home Party) both publicly said that the peace process is dead and there would be no room for a Palestinian state. Prime Minister Netanyahu merely dismissed these statements that seem to increasingly reflect mainstream thinking in Israel's political spectrum. Meanwhile, Palestinian leaders remain deeply divided between the Fatah-led leadership in the West Bank and Hamas in the Gaza Strip. If the current Israeli-Palestinian impasse prevails and the Syrian war produces more spillover effects, we should not exclude a third Intifada or "Palestinian Spring."
- *This is my final point. The defining feature of the current strategic landscape will be uncertainty.* Uncertainty about which next regimes may fall, and which parties may rise to take their places; uncertainty about the ability of the new governments in Egypt, Libya and Yemen to tackle the political and economic challenges; and uncertainty about the willingness and capacity of newly empowered Islamist parties like the Muslim Brotherhood to engage with Europe and the United

States. There are many more wild cards in the MENA region; and many potential tipping points that could provide further dynamics to the Arab Awakening. The large demonstration in Cairo planned for 30 June [2013] may well be one of them.

We Need a Long-Term Strategy to Engage the Arab World

However, this should not prevent us from developing our own strategy for how to respond to all these trends and contradictions. It is true that, in the first place, the Arab Spring is owned by the Arab people as well as other ethnic and religious groups that are part of the social fabric of the countries. But neither Europe nor North America have the luxury to ignore what takes place in our immediate neighbourhood—what is likely to preoccupy us for many more years to come—and what has a number of grave security implications for us.

I think we all agree—more or less—on the political diagnosis of the current state of play in the Arab world. We also agree that we have made mistakes in the past, and did not anticipate people's thinking in the Arab world. And if we are honest with ourselves, we should also admit that Europe and North America have largely been running behind events going from one crisis to another. With a view to the Syrian crisis, we are already very late—perhaps even too late.

What we lack is a realistic, comprehensive and long-term strategy that spells out how we see the MENA region evolving in the coming years: which strategic objectives we want to pursue in the region; how we can assist the transformation processes in the countries respectively; what we will not be able to do; and how we can enhance our own resilience capacities against future turbulences and shockwaves that will undoubtedly occur in the future.

As NATO Deputy Secretary General Ambassador Alexander Vershbow said earlier, NATO, for example, has a lot of experience and expertise in the field of capacity-building and security sector reform. What we are about to do in support of Libya, we could also offer to others if they wish.

We could start crafting a long-term transatlantic strategy by having a critical look at our partnership toolbox (Mediterranean Dialogue and Istanbul Cooperation Initiative) and discussing whether we must overhaul and adapt it to the new realities in the Arab World. Simply sticking to what we have offered to some of the Arab countries ten years ago or distancing ourselves from the developments on the ground, will not do the trick. We must engage the Arab world—proactively and with open eyes—all across the Maghreb, the Levant and the Gulf region—because it is in our genuine interest.

Chapter 19

Security in the Middle East: a View from Baghdad

Ambassador Fareed Yasseen
Ambassador of Iraq to France

I will try to give you the perspective from Baghdad. It is an interesting one because if you look at all the countries in the Middle East—and I say this with not only sadness but also some pride—we have had both the worst and richest history of the past 20-30 years. This is because the power structure in Iraq that we have inherited was not in equilibrium with a natural power structure that you would expect given its population and its neighborhood. This resulted in a series of wars, both external and internal. A lot of people argue, wrongly I think, that Iraq is on the verge of dividing because we have finally accorded autonomy to the Kurdish region. But in fact, we do not have a guerilla war going on in Kurdistan as we did in the 1960s; Arabic is being taught again in Kurdish schools; and the north of Iraq is not as it was in the 1990s.

A Brief History of Iraq

So, I will now go over the recent history of Iraq, give a little deeper description of the current situation, and see what lessons we can draw for countries of the Arab Spring. I would like to say that I am a little cautious about names like "Spring." Arab countries are characterized by having very short springs followed by very hot summers. We are in the summer right now. I am also cautious about names like Awakening and Resurgence: my country was destroyed by the Ba'ath Party, and Ba'ath in Arabic means resurgence or awakening.

I will talk about Iraq after 2003. Regime change happened. For this I am grateful to Vice Admiral Mark Fox and many of his colleagues. It is something that should have happened earlier, in 1991. We would have avoided many of the worst passages of time that we have had to go through such as an embargo that destroyed the middle class; being cut out of the information revolution; or the pauperization of the middle class. And many things that seemed so difficult to accomplish in Iraq are in fact the result of the weakening of the institutions of the state that have resulted from the embargo. But regime change took place and, very quickly, we developed a sort of conflictual relationship with the United States because—I think that was the cardinal mistake that was done—we were put under the status of occupation. It would have been a lot better had the United States and the International Community agreed to take an acceptable representative group of Iraqi politicians as happened in France for example after World War II and said: okay, you are in charge, you have authority, we will support you on condition that within one year, you hold elections. I think that would have facilitated a lot of things.

Nonetheless, this is what happened and the November 15 agreements were signed by a group of Iraqi politicians, the Iraqi Governing Council at the time, and the United States. The elements of this agreement were later enshrined in Security Council Resolution 1546, which set up an agenda for the development of a Constitution and for a series of elections. I am really happy to say that we are still on track. Looking at history and at the Arab Spring, I see elements that give me a sense of déjà vu. For example, if you look at what happened in Libya in 2011, it is what should have happened in Iraq in 1991. There was a U.N. Security Council resolution, Resolution 688, that called for the imposition of a no-fly zone in the north; it was enacted and it saved a lot of people but, sadly, it allowed the regime to stay in place. If you look at what happened in Tunisia, they quickly developed an electoral process and set up a constitutional committee that, down to the names of the institutions themselves and the types of memberships, recalled what happened in 2005 when we had our first referendum on the Constitution and our first elections.

Lessons Drawn from Iraq's Experience

One lesson that I draw from this for the countries of the Arab Spring is the paramount importance of the constitutional process. It has to be representative, and I have heard Iraqi politicians who were involved in the Iraqi constitutional process criticize the process that took place in Egypt for example. The constitutional process needs to be inclusive. In Iraq it was. In fact, efforts were made to make it inclusive. In the first elections, we had a boycott of the Sunni population and because of the quirks of the electoral system, we had very few Sunni Arab members of Parliament. So the constitutional committee itself broadened its membership and included distinguished representatives of that community to participate in the drafting of the Constitution. This is one lesson, one thing we did well.

One thing we did not do well is that we worked on an agenda that was very quickly put together. I think that the constitutional process needs to mature on its own time frame. Unfortunately, we had to obey a time frame that had more to do with the American elections than with the needs of Iraq. So a constitutional process has to take the time it takes.

The second feature that was really important for us was the electoral system. Here, I cannot point the finger at the Americans. I think the electoral team that was sent by the United Nations committed the mistake. The electoral system is really key. The team that came was mostly composed of Latin Americans who had carried out elections in South Africa very successfully; so they took the same model and applied it to Iraq. There were two main features: direct representation and a very large electoral district. The objective was to try to pick up a vote that would be "a mile wide and an inch deep." In other words, people who did not have local concentrations would still be able to contribute to the elections in aggregate. Unfortunately, because the electoral slates were national, most Iraqi voters did not know who they were voting for. And so the identity reflex took over. They voted for people whose names they recognized, not necessarily people whose reputations they knew, but people who were of their own tribe. That enshrined identity voting.

Then we had the boycott of the Sunni community, which was a really bad problem because we ended up having a skewed representation. It was eventually corrected in the follow-up elections but what I mean is that, in countries like Egypt, which have a very important minority like the Copts, one has to make sure that the electoral system that is chosen is as representative as possible.

The other lesson that I would draw is to avoid underestimating the legacy of dictatorship. Italians and Spaniards that are present at this workshop sympathize with us because they still have laws that go back to the time of Franco or of Mussolini. Ten years later, we are still working with rules and regulations that go back to Saddam and came from a framework of top down Socialism that is not very conducive to set up and run a very lively economy that can provide jobs. So do not underestimate the difficulties.

Nonetheless, it is important to keep at it and focus on the most important element which is elections. We have had a series of elections on schedule with slight variations because of the security situation and we look forward to the elections that will take place in March or April [2014]. Let me add that after the past elections, we broke the record of the Netherlands as the country with the longest government formation process and more recently, our own record was broken by the Belgians. So when the politics of Iraq get compared to the politics of Belgium and the Netherlands for a country that was occupied barely ten years ago by Saddam Hussein, I have to feel optimistic.

The Crisis in Syria

As to Syria, the Iraqi leadership is indebted to the Syrians, not to Bashar al-Assad but to his father, because Syria and Iran were the only places where they could seek refuge. Very early on in 2011, the Iraqi leadership urged the Syrian leadership to open up. President Talabani sent a very compelling letter to Bashar al-Assad to set up a national unity government. Senior officials met with him repeatedly about that idea. Unfortunately he chose not do that. We took a wrong turn somewhere and the protests quickly morphed into armed conflict. As a result, we had a short period of relative calm in certain areas because the mid-level operatives of Al-Qaeda in parts of Iraq who were Syrian—who had in fact come from Syria—went back there. And I must say that before 2011, Syria was the main gateway for foreign fighters and suicide bombers into Iraq and one of its main sources. But now, we are concerned about the growing influence of Jihadists, particularly Al-Qaeda, in Syria. The official position of the Iraqi government is in support of the Geneva documents. We were present there as part of the Arab League and as a signatory member. We would seek a negotiated settlement for Syria and we believe that force of arms would only create problems, as they have. Since 2003, we have had about 120,000 civilian victims but barely two years of the Syrian crisis are going to create just as many. So it really is something that needs to be stopped.

We view the development in Syria through the perspective of what we went through. A main concern of the Iraqi government that is shared by many Iraqis is what would happen to a shrine in Damascus that has great importance for the Shia in Iraq and for the Shia generally, when they remember that the terrible two years we had in 2006 and 2007 were ignited by the destruction of such a shrine.

Chapter 20

The Middle East: a Military Perspective

Vice Admiral Mark I. Fox
Deputy Commander, United States Central Command

The Four "Wars" in the Middle East: Afghanistan, Iran, Syria, Counter-Terrorism

Many of my thoughts have already been spoken. But I would like to touch on the Middle East from a military perspective. There are four wars currently going on in the Middle East. The Afghanistan war has already been addressed. After December 2014, there will be a transition and a change in the way we view what is going on in Afghanistan. Another war is Iran against the world with all of the sanctions and the continuing concern about the Iranian nuclear program. I agree that perhaps the new Iranian President may be pragmatic, but I do not think he is a moderate. As Secretary Gates used to say, he has been looking for 30 years for the great Iranian moderate and has not found him yet.

Syria was described as a gaping hole in security. I use the bleeding ulcer example. There continues to be a great deal of activity and discussion within the United States about what must be done to stop the killing. Already, 93,000 people have died. From a military perspective, it is really difficult to come up with a logical application of military force that makes the situation better. I would second the comments for the need for a Western and—in my case a United States— strategy of how we want to engage. The real issue is whether we should engage or whether we should try to contain. By doing nothing we are kind of falling into the "contain or at least hope it does not spill over" camp; but it is not a well articulated strategy.

The fourth war is counterterrorism. It is a transnational problem with Al Qaeda. Al Nusra is a significant threat; in fact, that has been a detriment to the willingness of the U.S. to arm the Syrian opposition. I was in the State Department last week: there are 1,262 identified groups in opposition to Assad. Once you take Al Nusra away, there are 1,261 and that does not necessarily mean that they have got all the groups that are in opposition to the Assad regime. There is Al Shabaab in the Horn of Africa; Yemen. The counter terror war is a continuing focus.

Three Broad Confrontations: Arab-Israeli, Sunni-Shia, Arab-Persian

In addition to the four wars I just described, there are three broad confrontations. The Arab-Israeli issue has been discussed as well as the need for a Middle East peace. Quite frankly, there are many hopes that have been dashed against those cliffs but that is something that must be addressed. I just do not see any way around it. And within the region, there are the ethno-sectarian, the Sunni-Shia, and the Arab-Persian with many variations on the source of confrontations. Then finally there is the India-Pakistan confrontation which shapes a great deal of the thinking that goes on in Pakistan and affects us in Afghanistan. These are all very interrelated.

Sea Lines of Communication, the Straits of Hormuz, and Bahrain

From the maritime point of view, I was always concerned about the sea lines of communication and the places where people can choke off the cardiovascular system. I described the Suez canal, the Strait of Bab-el-Mandab, the Straits of Hormuz. Every single day, 365 days a year, there are between 15 and 20 million barrels of oil going through the Straits of Hormuz. And so we the U.S. and we the Western community must look at the region in the context of the energy that is now coming out. One of the rare sources of new oil in the region comes from the new levels in Iraq. I would have visits when I was in command of the 5th fleet. People would come through essentially saying, you are making decisions based on strategic interests rather than interests based on human rights. From a Western perspective, we have to embrace both, quite frankly. There are strategic interests. My advice always was the Hippocratic oath. First, do no harm. I can find ways to create harm by doing a lot of things in particular. For example, if you could reroll the tape on the big angst-filled moments in that region, the Sunni Arab leaders were infuriated with the United States, with our lack of support for Mubarak after just a few weeks of unrest. And the feelings were essentially, “So that is how you treat a friend of 30 plus years. You just ditch him. You throw him under the bus.” There was a lot of vitriolic attitude towards us. And we in the West have always wanted the Gulf Cooperation Council, the GCC, to function as a quasi-Arab NATO, as a collective security organization and yet we never dreamed that it would be the perception of our lack of support for Mubarak that would create the appetite for the GCC to actually do something together for the first time. They sent troops across the causeway into Bahrain in March of 2011.

Finally, we must be engaged and present to influence the situation in the Middle East...”virtual presence” is actual absence. We can surge troops and equipment, but we can’t surge trust.

With that, I will conclude my remarks. I am not optimistic.

Chapter 21

The Spanish Security Position toward the Mediterranean

Ambassador Alejandro Alvargonzález San Martín
Secretary General, Spanish Ministry of Defense

Introduction

I am grateful for the opportunity to bring before such a distinguished audience an overview of the Spanish security position towards the Mediterranean, specifically towards the Maghreb: the West of the Arab world. I am particularly pleased to be here with you today to address the issue from the perspective of the "National Security Strategy: A shared Project," approved less than a month ago by the Prime Minister. This important document defines the global and all-encompassing reference framework in the security field, and guides the State's comprehensive action when tackling current challenges across different policy areas.

Let's recall that Spain's geostrategic location, as part of Europe, open to the Atlantic and a bridge to Africa, has traditionally marked the four vectors of Spanish foreign policy: the European Union, the United States, Latin America and the Maghreb, or rather, the Mediterranean as a whole. Currently, two years after the outset of the Arab revolts, Spain is still firmly committed to promoting security, development, human rights and democracy in North Africa and adjacent areas, as we shall see.

Security as the Foundation for Development and Progress in a Free Society

Allow me to begin by highlighting the first sentence of the Spanish National Security Strategy: "Security is the essential foundation for the development and progress of a free society." This statement is also valid for all countries of the Mediterranean Shore. Undoubtedly, in the light of Arab revolts, concern over Mediterranean stability has increased and continues to define the security agendas of Spain and other countries of the International Community, apart from the activities of the international organizations to which we belong and others of regional nature.

In the particular case of Spain, I must emphasize that the new National Security Strategy takes into account the change processes underway in its southern shore, and considers that indeed, all transitions are complex and entail opportunities as well as risks. What is clear is that there are not two equal transition processes and that these cannot be rushed. And here, I remember my own experience: while I was stationed in Egypt, I used to hear time and time again the words "Shuaia, Shuaia," slowly, slowly…

In this sense, Spain has an important role to play, due to its experience of democratic transition and the positive image it has in the countries of the region. And I would note two important characteristics of our transition to democracy which need to be highlighted:

- Reaching national reconciliation is essential for any change of political regime to prosper.
- The order of the factors cannot be reversed. First, there needs to be freedom to reach democracy, and not the other way around.

In this context, synchronicity must be found between Mediterranean societies and public powers, since the exclusion of social groups or the use of violence for achieving political gains, breeds further instability and could have very negative consequences on the countries of the Southern Shore and on security throughout the region.

The Mediterranean: the Challenges of a Highly Heterogeneous Region

The Mediterranean is not a unitary whole since, from socio-economic, demographic, and cultural perspectives, there is more heterogeneity than would normally be assumed. Although Mediterranean countries share similarities, each one is quite different due to its past, to the way time has carved its political feeling, to the strengths and weaknesses of its population and to its political class. In short, if I may use such an expression, each one has its political cosmo-vision or "worldview."

It is true that until very recently, the West watched the region with a certain degree of condescension, convinced that it was the way towards an ordered transition to democracy. I myself lived those interpretations in Egypt in the nineties, where the cult to the Rais' personality, to Mubarak, was a constant as well as a stabilizing element in a world already filled with problems. For some, the great failure of European policies was to back the maintenance of an existing system without seeing the elements of change that triggered the uprisings.

As Ms. Catherine Ashton pointed out in her recent visit to Madrid on June 13, "Europe will be judged by its own effectiveness on its neighborhood," thus it must redouble its commitment so that the security and prosperity of our neighbours also benefits the security and prosperity of our own citizens.

In the immediate future, security and prosperity will face major challenges and uncertainties that will affect us as our neighbours move toward establishing true States governed by law, economic and social development, control over migratory flows and fight against terrorism, drug-trafficking, and other illicit international trafficking.

Within this context of political change, we can distinguish three types of transition models in Arab countries: the reformist Algerian-Moroccan model, the revolutionary Tunisian-Egyptian-Libyan model and the regressive one of Syria. Allow me to focus on the first, noting that our neighbourhood with Morocco and territorial proximity with Algeria—and also with Mauritania—make their economic development and their political stability decisive factors for our national security.

Morocco is slowly following a reform process initiated by King Mohamed VI in the summer of 2011, whose most tangible example has been the amendment to the Constitution in order to promote a democratic transition.

In the particular case of Spain, the physical border we share with the autonomous cities of Ceuta and Melilla is also present in the economic domain due to a difference in income per capita of 1 to 13. If we add to this the Salafism influencing the Maghreb, the risk is clear, since it could permeate an individual case which could affect us.

This fact, the threat of Islamist fanatism, has created a ground where cooperation seems crucial in another unresolved conflict: the Sahara issue, which continues to condition Moroccan-Algerian relations. If the solution to the Maghreb problems involves an understanding between Algeria-Morocco, the solution to the problem involves the Western Sahara.

Algeria is in the middle of a process for the succession of President Buteflika, whose candidacy to the 2014 elections is uncertain. It is also determined to address the problems of terrorism and organized crime on its territory, hardening its southern border with Mali while the interior is relatively calm. For Spain, the major risk comes from our energy dependence. For example, what happened in In Amenas resulted in a 6% reduction of Algerian gas for several weeks.

Mauritania, for its part, had some success facing the protests that appeared a the beginning of 2011, although we should carefully monitor the consequences of the military intervention in neighbouring Mali. In our opinion, Mauritania's stability is key to avoiding the massive migratory flow towards the Canary Islands and to ensure the personal safety of Spanish citizens living there.

Finally, I would like to point out our grave concern about the precariousness of West Africa's governing systems, which could lead to the emergence of groups that engage in piracy, as happened in the Gulf of Guinea, and pose a threat to the safety of maritime traffic between the Canary Islands and Cape Verde to Europe. This is also one of the challenges we face in the Horn of Africa, where Spain participates in EU and NATO-led missions. Our country has just taken on the command of the Standing NATO Maritime Group (SNMG-2).

Spanish Response: the Role of the Maghreb in Our Foreign and Defense Policy

Spain considers it fundamental to address the region's challenges from what we call "reinforced multilateralism," as it is clear that the variety and nature of the new challenges are such that they cannot be tackled in isolation. In this sense, we have to assume a comprehensive approach to security where the efforts of dialogue and multilateral cooperation are further reinforced through bilateral relations and cooperation with other intergovernmental or even non-State actors, thus creating a climate of trust and transparency between our nations.

Spain is very well positioned on this issue, and I will now mention several action frameworks in which we operate:

- *The promotion of bilateral relations with our most immediate neighbors.* Within the framework of the Defense Diplomacy Plan (visits, joint committees…), we must promote bilateral relations with our most immediate neighbors. In particular, we support the effort of the United States Africa Command (U.S. AFRICOM) to favor interoperability with the Armed Forces of African countries.
- *The consolidation of the Defense 5+5 Initiative.* The Defense 5+5 Initiative, which celebrated its tenth anniversary last May, has an informal and flexible nature which allows it to reach an important practical and operational orientation in three specific areas: maritime surveillance, civilian protection and air security, through conducting annual multinational exercises.
- *The promotion of NATO's Mediterranean Dialogue.* Since it came into existence in 1994 thanks to a Spanish initiative, we strive to deepen political and practical cooperation in both its civilian and military dimensions with partners, through the development of education, training and operational activities.
- *The reactivation of the EU's Union for the Mediterranean.* Since it captured the acquis of the Barcelona Process in 2008, we have continued to actively work on its development. It is true that, as an ambitious project where we find Israel with all Arab countries, making progress in the development of its objectives is not an easy task. However, the arrival of a new Secretary General, Moroccan Ambassador Fatala Sijillmasi and the new role that the European Commission would like to play in Euro-Maghreb cooperation have given cause for renewed optimism.
- *The United Nations.* As for the United Nations, Spain has been carrying out several initiatives in the last few months to encourage mediation in the Mediterranean, closely cooperating with the Department of Political Affairs in order to establish synergies between States and civil society in the mediation processes. On 8 and 9 July, a third Seminar will be held in Rabat, Morocco.

But we must be realistic. This has been recently indicated by our Foreign Affairs and Cooperation Minister when he referred to the fact that the Middle East Peace Process (MEPP) continues "to pollute" cooperation initiatives. Therefore, we must strive to enhance greater inter-Maghreb relations so that the risks and threats affecting us (terrorism, transnational crime, and especially the rise of radical Islamism…) do not swing toward the establishment of fundamentalist regimes in the long term, which would pose the greatest risk to our national security.

In short, bilateral cooperation, international cooperation and South to South cooperation are key to avoiding the hybridization among terrorist and criminal organizations that undermines security. This could extend the action of hybrid terrorist-criminal organizations beyond national borders, and thus affect our own security.

Conclusions

As I mentioned at the beginning, Spain's geographical location makes us the Southern border of Europe and the Western border with Islam—a border that is not only religious and cultural, bur also economic and social.

As stated in the National Defense Directive 1/2012, our location gives us "the responsibility to ensure the consolidation of a safe environment, particularly in the Mediterranean" as a necessary condition for guaranteeing international peace and security, as well as our own, in the face of risks and threats—shared or not—coming from the Maghreb, a sensitive, fragile and always surprising region.

Chapter 22

Panel Discussion: Security in the Mediterranean and The Middle East

Ambassador Alejandro Alvargonzáles San Martín (Spain), Ambassador Fareed Yasseen (Iraq), Vice Admiral Mark I. Fox (U.S.), Vice Admiral Robert Davidson (Canada)

Ambassador Alvargonzáles: We have been supporting dictators. This is absolutely real. I was posted in Cairo from 1991 to 1994. And our hypocrisy was that we did not speak about dictators, we spoke about transitions to democracy, the Arab way to democracy; because they had an imbalanced society, we should teach them to balance it. This was happening in Egypt. I saw it. This was happening elsewhere too. Others took advantage of that. Because what I saw in Cairo is that while we were supporting dictators, others were filling the void. Now we had reasons to support dictators—very cynical but very realistic reasons. We had the Cold War and the idea of stability was always in the forefront. But while we were doing that, and the state was functioning under the schema of a dictatorship, others were doing their job. I am talking about the Muslim Brotherhood and even the Salafists who were very close to their people. I remember that the Muslim Brotherhood were the first ones to mobilize during the earthquake in Cairo; In the south, the Salafists were the ones who helped the poorest people; who had hospitals for poor people; who had teachers in the madrasas, etc. So when democracy came, who won the votes? Not the ones who carried out the revolution but the ones who had been there for so many years doing their job and being very close to the people that they were helping. They won the elections—I am not talking so much now of the Muslim Brotherhood but of the Salafists—even though they do not believe that the democratic regime is a legitimate regime or is a regime that is able to compromise with their final objectives. When I talked about the comprehensive approach, I talked about the armed forces, training police, training the armed forces. I also advocated training judges and investing in education which I think is very important. I did it on purpose because in the European Union we tend to speak of global approaches and the first thing we do in this global approach is to cut out a piece, which is the armed forces and focus exclusively on other things. The armed forces, education of the armed forces, assisting the armed forces is as important as the rest. If it is not global, it will not work.

Ambassador Fareed Yasseen: The Iraqi example shows that people take to elections. Any effort you undertake to strengthen the electoral process, to make it a constant of the political life of the country will be beneficial. In particular, I have seen this with institutions that were helping us carry out our elections like the National Endowment for Democracy; the National Democratic Union; and the EU's electoral programs which do have a real impact. I think these institutions should be strengthened. In fact that is one of the running comments I have with my French friends: they do not have anything equivalent to the National Endowment for Democracy. The British do, but the French do not. And it is worth noting that most of the people who initiated the Arab Spring learned the tricks of their trade—gathering people together, activism, and so on—working on projects that were fostered by these organizations, including Tawakkol Karman, the Yemeni woman who got the Nobel prize in 2011.

Vice Admiral Mark Fox: We in the West are guilty of mirror imaging. We have heard this discussion about the Arab Spring or the Arab Awakening and those are wistful, wishful kinds of concepts that the West would like to say occurred when the fear barrier in the unrest was broken for the first time. I think a lot of it was driven by social media, by factors that most of us certainly have not grown up understanding. Also, there are people who are not comfortable with the idea of our non-governmental organizations coming into their countries saying "here's how to have an election." And so there is this tension between bringing Western ideals and Western ideas into places. And I completely agree with your approach but the practical application is going to be the hard thing since there are many places today where Western non-governmental organizations that teach people about electoral processes are seen as undermining the authority of the government.

Vice Admiral Robert Davidson: All of us around this table drink the same Kool-Aid. We are the security community. In fact, you could say that we are part of the security faith group ready to sing the same song when it comes to what we want to accomplish. We approach a lot of what we do with—and here I will steal one of Admiral Fox's words—wishful optimism, a lot of wishful thinking. I am very pleased that he brought up the comment of the "do no harm." In fact, the one I was going to bring up was "do the least harm," because these are ethical problems and everything we do causes some harm. It is impossible to do no harm. It is a matter of what can we do that is the least harmful rather than what does not hurt. All of us Western nations are spending money that we do not have. Some of our economies are teetering on the verge of insolvency because of the amount of spending. How many of us would have envisaged sequestration that long ago? The comprehensive approach is expensive. We have talked about job creation; in fact, we have created 352,000 jobs in Afghanistan. And that has not solved the problem. We tend to take too optimistic an approach. Without understanding what the end state is or what we are trying to accomplish, it is very difficult to have a strategy. And yet we launch into these problems without knowing what our end state is going to be. So how can we have a comprehensive Middle East strategy when we do not know what the end state will be? Without an end state it is essentially a dream. I see parallels between counterterrorism thinking and counter-drug thinking. We have been doing counter-drugs now for decades and consistently failing, if I may say, because we have not eliminated the problem and drugs remain in all the streets. And why do we continually fail in the counter-drug strategy? It is because we attack the wrong end of the supply/demand chain. We attack the supply end and as long as there is a demand, anybody with an MBA understands, you cannot eliminate suppliers.

Chapter 23

Towards Effective Cyber Security—a New Strategy

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

This paper is a transition from the policy discussions we have been having to a technology-focused discourse: while there have been some underlying references to cyber security, I will make it the sole focus of my talk. To explain a bit about MITRE's activities, we work on the government side, looking at some of the most difficult problems that the government is facing. My efforts (along with Gary Gagnon, who is the vice president of MITRE in this area) are on cyber issues and national security. (There are other MITRE centers that work in homeland security, health, and the Federal Aviation Administration.)

A New Strategy: from Reactive to Agile Systems

In terms of our work for the government in this area, we are looking at different mechanisms for improving the cyber security methods that we use. We are at a point of transition from a reactive system to a proactive system. Up until now, we have attempted to secure operating systems and applications by trying to reduce the exposure (i.e. reducing the surface that could be attacked; reducing protocols and ports) as well as by engaging in faster scanning and patching. However, even if you are scanning and patching at the fastest rate possible—the business standard being the patching of 90% of assets within 72 hours—you are still exposed 65% of the time. So if you are in a reactive "how fast can I apply patches to my system" mode, you can never close the window of exposure.

The game of soccer provides a good analogy: until now, we have had our goalie turned backwards so that he is facing the net, trying to see where some of the shots pass through holes in the net and then patching them. However, we should be doing the reverse. The goalie isn't looking for holes in the net, he is trying to understand the net in detail in order to better defend it. Also, we want the goalie and the other defenders to communicate to prevent shots from happening in the first place or to block them before they reach the goalie. We may even want to have another goalie join us. In this way, we can use what we might call "indicator analysis" to identify where the threats are coming from.

This more proactive approach can be thought of as agile or active cyber defense. In other words, it involves achieving greater threat awareness and sharing the tactics, techniques, and procedures that are being used with others in your field or sector. In this way, you can be better informed about the nature of threats facing your specific business or government enterprise. The set of individuals who seek to penetrate systems has certain tactics that are repeatable. It is thus possible to identify these patterns by gaining more awareness and facts about the nature of that threat and thereby strengthening your information security.

The Advanced Persistent Threat Is No Longer a "Hacker"

In addition, over the last decade or so we have really stopped using the term "hacker" to describe the Advanced Persistent Threat. In the past, a hacker was someone who penetrated a network for entertainment or for bragging rights. However, hacking is no longer an entertainment activity. It is now an industry focused on gaining information or financial access to systems. Furthermore, it has become a way of life for a number of individuals who now work an eight hour day and are given a task list of sites to attack. Hacking has been transformed into a set of repeatable processes using a number of standard techniques.

There Is a Co-evolution of Resiliency as Defenders Act and Learn from the Actions of the Adversary

There has also been a co-evolution in the resiliency of systems, i.e. the ability of a network to absorb an attack and keep operating instead of shutting down. The reason I call it a co-evolution is that both sides are informing each other: the threat is learning about the procedures we are using to keep the system running. In exchange, we are learning more about the threat's actions.

We Cannot Keep the Adversary Out

In doing this, it is important to recognize that it is impossible to guard against all network intrusions. There is no perfect defense. You have to assume that your networks will be penetrated and that you will be able to identify where the adversaries or the threats are within the layers of your system. Rather than trying to create an unbreachable Maginot Line, instead you need to look at a threat-based cyber defense focused on mitigation as well as detection and response—and the sharing of threat indicators.

So rather than just having your small enterprise defending your computer network, that enterprise shares information with other like entities or regional entities and gains further information. This is what we might call "crowdsourcing" of what we are seeing within our sector, either of the economy or the country. This can be done either regionally or by functional divisions of businesses.

Identify and Pre-approve Response Actions

It is also important to implement within your network response capabilities with pre-approved actions so that you are not stunned and unsure of what to do. Instead, you have pre-scripted or pre-approved the sort of measures that will be taken to keep the system operating and move from one level of defense to the next. To give an example, we used to place the emphasis on user convenience. During times of duress, the priority is no longer user convenience. We will require more authentication to join the system when you are not at work. You might have to go through a couple extra steps. They would be fairly straightforward things, but with an emphasis on information integrity rather than user convenience.

Employ a Covert Red Team

Further, I think it will be necessary to take a hard look at the system, instead of just "blaming the CIO" for any problems. Instead there must be an elevated level of responsibility. In the case of the military command, there needs to be responsibility for the way systems are secured. Also, the work force culture is important, especially how the work force is informed about appropriate ways to do their work, so they will not just automatically click on a link for a website without considering possible consequences. In board of directors parlance, a Red Team of outside auditors is needed to look at your system. That would be a red team that looks at the way your networks are being operated and how your PII (Personally Identifiable Information) or your intellectual property is protected. Now the Red Team does not just look at your network connections or the physical configurations of network activity. They look at you as an entity, a facility, and a work force to see where the gaps are—including the way you vetted people to become system administrators and whether they are actually following the system administrator procedures of having two people approved to witness certain backup activities. It is work, it is dreary work, but it has to be assured in order to be secure.

I believe that further authentication and transaction controls will emerge as one of the more important aspects of the way forward: a system where we are secure based not only on the user credentials of those who are coming into the network, but also based on the devices. This is particularly important with mobility and the way we have moved toward a more cloud-based mobile computing environment. Greater authentication will be required in order to have the privilege to be a part of the system.

We have talked about the CERT concept that would absorb information, digest it, then send it back out. What I am now talking about is more of an agile, nodal network—not hierarchical but nodal—that informs different members of the system or the coalition about what is going on with regard to vulnerabilities or intrusive attempts. This approach has been resisted in the past, because we started out by using an internet security awareness coalition, and that meant reporting your vulnerabilities to us. It was a disincentive to have to report vulnerabilities and we have legislation in our country that makes it particularly onerous if you have to acknowledge publicly that you have had a vulnerability in your system. It is called the Sarbanes-Oxley Act.

Instead, we need a simple means of sharing indicators and information about the ways in which systems are being intruded and that should be done with a standard format. In Europe, there is some interest in using some of these formats that have been developed in order to facilitate quick sharing of information among enterprises, either business, government, or military. These standard data formats are machine format messages. They are not something written out in long text messages about an incident. Analysts who are in this space are competitive about who can get the information first by looking at the indicator, digesting it, and then advising about what they are going to do about it. In this way, they are sharing the tactics that have been used to deal with network intrusions. And they are building a wealth of knowledge across the enterprise.

Essential Attributes of Effective Cyber Programs for the Present and Future

The effectiveness of cyber programs, now and in the future, depends on (a) having an understanding of the network and its critical components as well as (b) having a development team working with operators—a Cyber Indicator Analysis Program:

- *Knowing the Network and Its Critical Components.* I will just give a short list of the central attributes of effective cyber security programs today. The first is knowing the network and its critical components. That means mapping your mission in a military context. It means mapping all network components including linkages and communications networks. The mapping must not just be inside the building, but it must also include how you are connected to the world and all the way out. In this way, you can find vulnerabilities in a single point, failure points, that you had not been aware of. Moreover, it is really necessary to map things in order to permit quick recovery, and soft degradation (whatever that means). You need to know how to be resilient after physical events such as cable cuts or when someone takes out your network accidentally. Once you have mapped your network, you know what is most important to you so that you can work through different scenarios and pre-scripted actions to protect vital information.

- *Development Team Working with Operators—the Cyber Indicator Analysis Program.* It is also important to have a development team working on these concepts to talk to what I would call the operator, so that that person's priorities are relevant to the way the system risk management is configured. Over the last few years, we have taken risk management in the cyber field and elevated it to the national level. However, it really needs to be down at a commander level, so that the commander can decide whether or not he is willing to take the risk in a certain area regarding network connectivity. In other words, it should be something that can be judged at a more tactical level, not something that is taken to a national level.

Cyber awareness that transcends across the culture of the organization is as important as building your defense in depth and red team analysis. For the future, the key is going to be investment in network capacity, instead of IT efficiency. This will mean building out enough capacity to be resilient and to have a failover option, not just minimal investment. Software development that provides better security within software will also be important, as well as systems engineering that is not just systems engineering for IT efficiency but engineering that will provide resiliency and strong networks.

Chapter 24

Dealing with Chaos, Risk, and the Cyber Threat

His Excellency Jaak Aaviksoo
Estonian Minister of Education and Research, Former Minister of Defense

Before speaking about cyber, I would like to say a few words about our debates so far. As I was walking around in this wonderful building of the Invalides and looking at the portraits, I was thinking, what is different about these men—Louis XIV or Napoléon III (as there are few women in the portraits). There is one common denominator for all of them: they were men who made things happen. Why do I think this is important? It is important because we have been discussing global security and I have heard several people saying that it is unstable, it is unpredictable, we have to monitor what is going to happen. I think I am correct in saying that we are men and women who talk about things happening rather than being like those in these paintings who made things happen.

Dealing with Chaos, Risk, and Maintaining the Status Quo

Chaos is about non-linear dynamics and, as a physicist, I know that there is always an equation of motion with many constraints. Some of those constraints are critical. If you can tune the constraint, chaos appears and disappears and the constraints are then irrelevant. Generalizing this to society or on a global scale, there are always interests that are able to tune critical constraints and there are other constraints that are irrelevant. I think it makes sense to think about it.

What we are witnessing in this world today is a very, very, big change concerning first and foremost Europe but also the Transatlantic Alliance. Our people, our societies have gradually given up the ability to take, manage, and digest risks. This inability to take risks on different levels, and in different countries, is a strategic disadvantage over those who are able to take risks, who are thirsty, who want to achieve, be successful, and pay a price if they fail. This is a problem that we have to address somehow.

As democratic societies, we always have to take into account what people think of us. People think of us in terms of what they think is good for them. And what is good for them is maintaining the status quo because there is a general feeling that the good old days were better than the future. This is not a very good feeling. However things are, I think that we should give up referring to austerity measures, economic crises, and other similar terms. These terms are convenient because we can postpone answering serious questions. I would rather believe that this is the new normal and that the stability we expect to come back one day and sustain growth will never take place. The world is different.

In the case of defense and security, the question is not about austerity or economic crises, the question is whether we want to spend on security or not. I believe that we do not want to spend on security. If we ask people in the street whether they favor increasing defense spending or decreasing it, their answers will be much more pragmatic: they are concerned about education, social security, and things like that, and they have a different perception of threats, different from what we were discussing here today. They do not feel that Syria is a grave problem because it is a distant thing and the countries they live in are so big, with such glorious histories that they allow them to run away from these problems and avoid them. But what they cannot avoid is that their salary is not really going to grow in the forthcoming years, which is a serious problem because they will need a new car next year. So we have problems with the threat perception in our societies and unless we solve this political problem, I hardly believe that we can make things happen in the strategic sense.

Now, what is happening is a redistribution of global wealth. And some, the majority, aspire for their fair share whereas many are trying to maintain what they have got. I believe that the people out here in Paris or anywhere in Europe and North America would blame their governments more for the loss of their social security than for the consequences of these international threats. This is a problem.

Dealing with the Cyber Threat

Now, I will get to cyber. The fact that there is so much talk about cyber threats is nothing new. Most of the threats were imagined, at the very least imaginable and there is a tendency to mystify cyber. That is the psychological reason why there is a lot of hype around cyber threats and cyber defense. On the other hand, of course, some of the threats are also real. So, there is a lot of cyber frenzy and noise but there are serious threats too. Let's take for example the case of these famous Nigerian emails that offer one million dollars. Probably 99.99 percent of people think that it is crazy, and they are not taken in. But the scam does work with a probability of perhaps one per million. With the billions of people all around the world, if you can fish ten of them and each of them gives you a few thousands dollars, that is pretty good income compared to the average income in those countries. So these threats are real.

In the broader sense, there are two kinds of people in cyber space. There are those who explore the possibility of cyber for their own fun or for curiosity or for other reasons. Yet, increasingly more of the things happening in cyber space are interest driven. People simply want to make money, and at the end of the day, all these borders are blurred. You start with curiosity and you may end up in hacking, or in espionage, or in cyber defense depending on circumstances. It depends on who pays more. Maybe it is not that cynical in real life but it is very close to that.

I want to make four points concerning cyber and the conceptual innovations that cyber reality has brought to our lives:

- First, on the political level, lines of division are blurred. For example, the division between internal and external security is blurred. How we organize our governments poses a very serious challenge because we are not very good at communicating between the Ministries of Interior and Ministries of Defense. The bad guys are much better. There is also blurring between the public and private spheres. Where do government services end? We know the bad guys are much more ingenious: they employ people from the private sector to carry out tasks that are either sponsored or at least tolerated by national governments. Criminal activities are also a grey area. At what point does something become criminal? So much activity is taking place in the grey zone. Shall we legislate in this grey area? Shall we police it? This raises a number of serious questions. I think we have to organize our defenses and security measures correspondingly, and we are not good at that, or at least not good enough.
- My second point is about openness. Nice guys are no longer compartmentalized like in a classical physical space. There are no safe havens. Everything can happen and happens almost automatically everywhere. So I think we have to rearrange our thinking about these threats correspondingly.
- The third point is about networking and hierarchy. We try to respond to a network threat in a network way but what we usually end up with is not a a functional network, a big hierarchy, but rather a bundling together of small hierarchies. This is not a functional and mature response. It must be truly functional like the workings of U.N. networks and the human brain. It is conceptually different. It is not technically different.
- My last point is about confidence. In the physical space, there are two components to confidence. First, there is identification. We know whom we are talking to. That is easy because we know people in most cases. There is no problem of identification or attribution but there is still a problem of trust. Do we trust that man? We usually want to meet him in person, to look into his eyes and understand whether or not he can be trusted. In cyber space it is worse. We do not have the identification first step, and we clearly have to do more to have a safer cyber space concerning identification via technologies as well as legal structures.

There is also a great challenge on the political level: how do we proceed? Do we extend the status quo of security to cyber defense or, on a lower scale, do we try to introduce some sort of arms control regime? There are different countries, different states that have different views for understandable reasons.

I would like to add the moral dimension. If somebody kills or robs someone, he is considered a criminal. But if somebody gets away with one million dollars stolen in cyber space, he is considered a hero and the one who lost the money is an incapable foolish institution, be it a bank or a ministry or a company. This moral problem is very hard to fight.

Last but not least, there is an increasing number of people who believe that the cyber space will remain an important domain of human activity.

Chapter 25

Orange and Cyber Security

Mr. Francis Bruckmann
Orange–Deputy Group Chief Security Officer

Orange is one of the world's leading electronic communications operators. Both as a domestic operator in more than 30 countries—mainly in Europe, the Middle East and Africa (providing Internet, broadband, landline & mobile phone lines, ADSL television, and satellite broadcasting)—and as a provider of communication services to companies around the world in more than 170 countries, Orange must protect its own infrastructure and guarantee the services it provides its clients.

The group's role as communications operator places it at the heart of major developments that are blurring technological borders as we knew them: between landline, mobile and Internet networks; between laptops, office computers, and mobile phones which can serve as computers; between personal and work telephones, etc.

Modern society can no longer function without digital technology. Orange operates a vital infrastructure, providing the backbone to the economic fabric in the countries where it operates this infrastructure and delivers its services to its 230 million clients or other providers using vital infrastructure (energy, transport, banking, commerce, etc.).

The Vulnerabilities of Digital Technology

These changes and the increase in interoperability provide fine opportunities for attacks that hackers have begun to take advantage of, as with the arrival of each new technology. Cyber security has become a major challenge for today's society, which is constantly connected to the Internet.

These attacks are rapidly increasing in number and strength: some of them, which affect the group directly, double every quarter, and are occurring more regularly owing to the powerful tools that have become more commonplace on the Internet. A look at daily news reports shows the increasing scope of cyber attacks due to attackers' boundless imagination in achieving their aims. Examples include:

- Denial of service (DOS) attacks that render a network or a web service unavailable (i.e. an electronic commerce website), as well as factory control rooms, or even a country's Internet network.
- Modification of data: client data, bank details, company web pages, or product prices displayed electronically in shops.
- Theft of confidential data, clients' personal data and bank details, industrial espionage, strategic company documents, operator traffic or the content of electronic communications.

Parallel markets are developing and offering their own services: usurping identities to steal goods, data and services or to carry out reprehensible actions, purchasing undisclosed vulnerabilities in software allowing attacks that are almost impossible to counter, and providing services to perform these attacks.

All of these are risks to the group's infrastructure, customer services, business, and brand image. They are also risks to the data of clients and employees alike, although it is protected by an increasing number of national and international laws and regulations that impact almost the entire operator information system.

The Security of Information Technology

Security has an increasingly important role to play and it relies on the involvement of everyone. It also requires all users to be aware of the risks involved in this kind of technology. Cyber security covers the more traditional notion of security of information systems. It also refers to the security of industrial systems, software embedded into equipment, and machine to machine applications.

And the risks related to the interconnection of Orange's various information systems concern the company both on an internal level and with regards to the networks used by the general public or institutional and private clients. The most frequent attacks—which are also increasing in number—are distributed denials of service (DDOS). These involve an attacker sending IP packets over networks including the Internet to a specific target from tens or hundreds of thousands of infected machines which form the attacker's network—a botnet. On average, the group suffers several significant attacks of this kind every day—in other words, attacks that require specific treatment of the traffic they generate—lasting an average of up to two hours, with a flow of up to several tens of Gb/s. The targets vary and sometimes appear to be of only secondary interest such as educational institutions or small companies. But usually the targets are large companies and administrations, including bank networks.

The most significant consequence for companies that do not have the necessary security services from their operator or who do not have the technical know-how internally or via a service provider occur when their own clients are unable to log on the company's website. This in turn causes customer dissatisfaction and loss of sales. Telecom operators can also be affected, but usually indirectly, particularly when the attacks target the interface between the mobile network and the Internet, causing disturbances for users.

PRISM and the SOC Concept

In light of these issues, Edward Snowden's revelations about PRISM look set to begin a virtuous circle of internal or external service implementation for security solutions. They show the lack of technical know-how in digital technology, both in terms of software, applications, products, and communication systems which all condition the everyday lives of our citizens and our institutions, and reveal major design flaws. Not a week goes by without some program or operating system undergoing a security update, following the discovery of a security flaw due to a software development error.

But how can we detect and counter cyber attacks as soon as they appear, or better still, when suspicious signals point to a future cyber attack? By using security operation centers (SOC), which first appeared around fifteen years ago. An SOC is an organized supervision centre able to detect attacks and cope with the current economic and business-intelligence cyber war. Orange has set up several SOCs around the world to meet its own needs and those of its corporate clients.

These centers form part of the overall security architecture, based on the latest dedicated equipment (Firewalls, IDS/IPS, UTM, etc) which can analyze the fastest flows in real time by using the Deep Packet Inspection (DPI) technique on the collection and synthesis of abnormal events, and their qualification by the appropriate teams. All of this is done 24 hours a day / 7 days a week / 365 days a year around the world.

Orange's SOCs make use of a range of skills: business risk analysis to identify the company's essential goods that need protection, collection of information needed for supervision, analysis of that information, and processing or activating plans of action.

This supervision is entirely different from traditional network or application supervision, which aims to ensure that the object under supervision remains operational. SOCs, on the other hand, are designed to detect attacks that will use the network as furtively as possible. During the attack or preparation phase, and if the attack is well done, all of the elements attacked will remain operational (unless of course the aim is to destroy them), and the operator will see no major change in how the systems operate.

A New Approach to Risk Assessment

Within companies, cyber security requires a new approach to risk assessment, which is the only way of determining the importance and impact of a threat. This has long been the priority of telecommunications companies, quite simply because it conditions how well their equipment operates and, by preventing cyber crime, their revenues. Cyber security has been a key priority at Orange for years.

Among other types of companies, however, the demand for the security solutions the group offers is often inadequate, given the risks that they face. They make decisions merely on financial grounds, and neglect the sophisticated services available from specialized companies that ought to be implemented.

The business world still needs to evolve in order to integrate these new concepts into digital technology. Yet, on these issues, telecoms operators including Orange are leading the way forward.

Chapter 26

Orange et la Cybersécurité

Monsieur Francis Bruckmann
Orange—Directeur Délégué, Direction de la Sécurité Groupe

Orange fait partie des plus grands opérateurs de communications électroniques. A la fois opérateur domestique dans plus de 30 pays, principalement en Europe, au Moyen Orient et en Afrique (activités internet, haut débit, téléphonie fixe et mobile, télévision par ADSL, diffusion par satellite) et fournisseur de services de communication aux entreprises partout dans le monde pour plus de 170 pays, il se doit de protéger ses propres infrastructures et garantir les services fournis à ses clients.

Notre métier d'opérateur de communications nous met ainsi au cœur de grandes mutations qui bouleversent complètement les frontières technologiques connues jusqu'à présent : entre les réseaux fixes, mobiles et internet ; entre les ordinateurs fixes et mobiles, et les téléphones devenus de vrais ordinateurs portables ; entre ces téléphones qui étaient soit personnels soit professionnels, etc.…

Nos sociétés modernes ne peuvent plus fonctionner sans numérique. Orange est donc un « opérateur d'infrastructure vitale », véritable colonne vertébrale du tissu économique des pays dans lesquels nous faisons fonctionner nos infrastructures et délivrons nos services, que ce soit à nos 230 millions de clients mais aussi à d'autres opérateurs d'infrastructure vitale (énergie, transport, banque, commerce, etc.…).

Vulnérabilités du monde numérique

Mais ces changements et l'interopérabilité apportée offrent aussi de formidables possibilités d'attaques que les hackers ont commencé à exploiter, ou se préparent à le faire, comme à l'arrivée de chaque nouvelle technologie. La cybersécurité est ainsi devenue un enjeu majeur pour nos sociétés « hyperconnectées » grâce à l'internet.

Ces attaques augmentent très rapidement en nombre et en puissance de frappe : certaines d'entre elles qui nous concernent directement doublent tous les trimestres, et elles se « démocratisent » par la banalisation d'outils puissants mis à disposition de tous sur internet. L'actualité nous montre chaque jour que le champ des cyber-attaques est de plus en plus vaste et résulte de l'imagination sans limite des attaquants pour arriver à leurs fins, comme par exemple :

- des attaques en déni de service (DOS) pour rendre indisponible un réseau, un service web (site de commerce électronique par exemple), mais aussi une salle de contrôle d'une usine, d'une centrale, voire le réseau Internet d'un pays…
- des modifications de données : données clients, données bancaires, pages web du portail d'une entreprise, prix des produits affichés électroniquement dans un magasin…
- des vols de données confidentielles, de données personnelles de clients, de leurs données bancaires, de secrets industriels, de documents stratégiques pour une entreprise, de données de trafic opérateur ou de contenus de communications électroniques…

Ainsi, des marchés parallèles s'organisent et se développent pour proposer leurs services : usurpation d'identités pour voler des biens, des données ou des services ou pour mener des actions répréhensibles, achat de vulnérabilités logicielles non dévoilées permettant des attaques quasiment impossibles à contrer, ou offres de services pour réaliser des attaques.

Ce sont autant de risques sur nos infrastructures, sur les services à nos clients, et donc pour notre business et notre image de marque. Mais aussi risques d'atteintes aux données de nos clients ou des collaborateurs de l'entreprise, couvertes par des lois et réglementations toujours plus nombreuses, nationales ou transnationales, qui impactent la quasi-totalité du système d'information des opérateurs.

Sécurité des technologies de l'information

La sécurité a donc un rôle de plus en plus important à jouer et s'appuie sur une implication de tous les acteurs, mais elle demande aussi une prise de conscience indispensable de tous les utilisateurs concernant les risques liés à ces technologies. Cette « cybersécurité » a ainsi englobé la notion plus traditionnelle de sécurité des systèmes d'information. Elle couvre non seulement cette dernière, mais également celle des systèmes industriels, les logiciels embarqués au sein de nos équipements, les applications du « Machine To Machine », etc..

Et les risques liés à l'interconnexion des systèmes d'information du groupe Orange le concernent aussi bien au niveau interne que pour les réseaux à l'usage du grand public ou des clients institutionnels ou privés. Les attaques les plus fréquentes et qui vont d'ailleurs croissantes sont celles relatives au déni de service distribué (DDOS—distributed denial of service). Il s'agit de l'envoi par un attaquant de paquets IP au travers des réseaux dont Internet en direction d'un objectif bien ciblé, à partir de dizaines voire de centaines de milliers de machines infectées et constituant le réseau d'attaque, un Botnet. En moyenne, nous subissons quelques attaques significatives de ce type par jour—c'est-à-dire qui nécessitent un traitement spécifique de leur trafic—avec une durée moyenne pouvant aller jusqu'à 2 heures, et avec un débit pouvant aller jusqu'à plusieurs dizaines de Gb/s. Les cibles sont variées : parfois elles semblent ne présenter qu'un intérêt ludique, comme des établissements d'enseignement ou certaines petites entreprises, mais plus souvent de grandes entreprises et des administrations (dont des réseaux bancaires) en constituent les cibles privilégiées.

La conséquence la plus importante pour les entreprises qui n'ont pas souscrit les prestations de « sécurisation » nécessaires auprès de leur opérateur ou qui ne disposent pas de compétences techniques suffisantes en interne ou via des prestataires, est l'impossibilité pour leurs propres clients de contacter le site de l'entreprise et donc de provoquer une insatisfaction des clients, et une perte de chiffre d'affaires. Un opérateur télécom peut également être impacté, mais le plus souvent de manière indirecte, notamment lorsque ces attaques visent l'interface entre le réseau mobile et l'Internet, provoquant des perturbations pour les usagers.

PRISM et le concept de SOC

A cet égard, les révélations par Edward Snowden de l'affaire PRISM devraient faire démarrer un cercle vertueux de mise en place de services internes ou externalisés de solutions de sécurité. Elles montrent l'absence avérée de maîtrise technique de l'univers numérique, qu'il s'agisse des logiciels, des applications, des produits, jusqu'aux systèmes de communication qui tous conditionnent aujourd'hui la vie quotidienne de nos concitoyens et de nos institutions, et qui font montre de défauts flagrants de conception. On peut en effet noter qu'il ne se passe pas une semaine sans que tel ou tel logiciel ou système d'exploitation ne fasse l'objet d'une mise à jour de sécurité, suite à la découverte d'une faille de sécurité due à une erreur de développement logiciel.

Mais comment détecter et contrer des cyber-attaques dès qu'elles apparaissent, ou mieux encore dès que des signaux suspects laissent présager une future cyber-attaque ? C'est via le concept de SOC, ou « Security Operation Center », apparu depuis environ une quinzaine d'années. Il s'agit d'un centre de supervision organisé pour avoir les capacités de détection d'attaques suffisantes et ainsi faire face au contexte actuel de vraie cyber-guerre économique et « business-intelligence ». Et pour ce faire, Orange en gère de nombreux au niveau mondial, pour ses propres besoins et pour ceux de ses clients entreprises.

Ils se fondent sur une architecture globale de sécurité, à base d'équipements dédiés (Firewalls, IDS/IPS, UTM,…). Les plus récents sont capables d'analyser en temps réel les flux les plus rapides (grâce à la technique de Deep Packet Inspection, DPI), sur la collecte et la synthèse des évènements anormaux, et leur qualification par des équipes appropriées, tout cela 24H sur 24 et 365 jours par an, sur un périmètre mondial.

Nos SOC font appel à de multiples compétences : analyse des risques métiers permettant d'identifier les biens essentiels de l'entreprise devant absolument être protégés, collecte des informations qui auront été identifiées comme nécessaires à cette supervision, analyse de ces informations, et enfin traitement ou activation des plans d'actions.

Il s'agit d'une supervision totalement différente de la supervision classique des réseaux ou des applications, qui vise à s'assurer que ce qui est supervisé est en état de fonctionnement. Le SOC, quant à lui, doit détecter des attaques qui vont utiliser les réseaux en étant les plus furtives possibles. Pendant l'attaque ou sa phase de préparation, et si l'attaque est bien faite, l'ensemble des éléments attaqués restent en état de fonctionnement (sauf bien évidemment si le but est de les détruire), et l'exploitant ne verra pas de changement majeur dans le fonctionnement des systèmes.

Une démarche nouvelle d'évaluation par les risques

Au sein des entreprises, il apparait ainsi que la cybersécurité doit mettre en œuvre une démarche nouvelle d'évaluation par les risques, seule apte à déterminer l'importance et les impacts de telle ou telle menace. C'est depuis longtemps une priorité des entreprises de télécommunications, tout simplement parce qu'elle conditionne le bon fonctionnement de nos équipements et au travers de la lutte contre la cybercriminalité, le niveau de leurs revenus. Il s'agit donc d'une question qui fait depuis des années l'objet d'une attention particulière.

En revanche, concernant les autres entreprises, force est de constater que l'appétit pour les solutions de sécurité que nous pouvons vendre n'est parfois pas à la hauteur des risques auxquels les entreprises doivent faire face. Les arbitrages sont souvent purement financiers, et se font au détriment des services sophistiqués que les entreprises spécialisées sont à même d'offrir et que le tissu industriel devrait mettre en œuvre.

Aussi, le monde des entreprises doit encore évoluer pour intégrer ces nouveaux concepts à la vie numérique, mais sur ces sujets les opérateurs de télécommunication, et Orange parmi eux, font office de pionniers.

Chapter 27

Cyber Security: the U.S.-China Relationship

Dr. Frederick Douzet
Castex Chair of Cyber Strategy, Institut des hautes études de défense nationale (IHEDN);
Professor, University of Paris 8

During this workshop we have been discussing the need to cooperate internationally and we have emphasized the fact that cooperation requires trust. In my remarks, I would like to discuss the relationship between the United States and China—a case where trust building is particularly difficult. In the past few months, the U.S. approach to cyber defense has been characterized by an escalation in means as well as in verbal exchanges with China. The Director of National Intelligence even told Congress that the cyber threat risk surpasses terrorism as the top national priority today.

There has been an obvious escalation marked by numerous leaks to the press, revelations, statements by experts and congressmen, and at the end of May, direct overt accusations by the Obama administration against China. Questions were raised about the existence of a Cyber War or perhaps a Cool War with China, which is what David Rothkopf argued in February in a Foreign Policy article. According to him, the Cold War era was followed by a time of Cool War, which is a little warmer than the Cold War and a little more techie. While the Cold War technology made war unthinkable, the Cool War technology makes it irresistible.

Is the U.S. in a Cool War with China?

So, my question is whether the U.S. seems to have chosen the path of the Cool War. There has been an escalation of cyber means in a context of sequester and a Pentagon budget that has decreased overall by almost $4 billion. In fact, the cyber security budget is probably the only one that has increased by $800 million. Recent statements have also shown a clear U.S. choice of an offensive rather than defensive political posture over cyber space, with the U.S. Cyber Command saying that their staff is scheduled to increase in the next few years from 900 members to almost 5,000 members. General Keith Alexander expressed the intention of turning it into an Internet age combat unit.

Now, we are at a stage where these declarations come on top of the development of experimental offensive weapons such as Stuxnet. Moreover, there have been revelations concerning the purchase of tools intended to fend off attacks against system flaws and vulnerabilities. Recently, the Guardian disclosed that President Obama had ordered a list of potential targets for cyber attack. The timing of this disclosure was interesting, because it was just at the very beginning of the California summit between President Obama and the President of China. Of course, Edward Snowden's revelations in the following days also shed additional light on the verbal escalation over cyber threats of the past few months.

There are multiple analogies between this verbal escalation and nuclear weapons. To give a few citations, I would mention Leon Panetta talking about a digital Pearl Harbor; John Kerry talking about foreign hackers being the 21st century nuclear weapons; and apocalyptic scenarios developed in books such as those by Richard Clarke. There are also mounting accusations targeting China, such as the Mandiant Report that was released just before one of the biggest conferences on cyber security in the U.S., and, last fall, Huawei and ZTE had to testify before the U.S. Senate about potential back doors in their equipment. Finally, there was a continuing resolution forbidding the government purchase of IT equipment produced by China.

I think that there are some domestic reasons for this kind of escalation: going back to the sequester, we talked yesterday about the game of chicken between Congress and the Administration which helps explain what defense budgets are for. There are also issues about passing legislation and perhaps being able to force some decisions through executive orders, or the influence of the cyber security industry since it is a flourishing market, too.

If we look at the broader geopolitical picture, there is clearly an increase in cyber attacks which is not likely to diminish. We have to assume that the networks are going to be penetrated in a context of rivalry between the two countries. In addition, the U.S. Administration has made strong statements about considering massive cyber attacks as acts of war. In February 2013, the conclusions of a secret report exposing the extended powers of the President of the United States to order a pre-emptive strike were leaked to the press.

The U.S. Cyber Strategy: Is It Viable?

So is this escalation really leading towards a Cool War or is this just political posture? If it is political posture, can it have serious consequences? Interestingly, the strategic debate is not completely closed in the United States and many questions and concerns have been raised. In March 2013, Martin Libicki urged Congress to tone down its cyber warfare rhetoric with a warning about the consequences of strong statements. He argued that such statements create a demand from the public and would compel the U.S. to act in case of major cyber attacks even if this were not the best course of action or even if it were not necessarily possible. Also, these statements engage the credibility of the United States in a sort of a deterrence strategy.

A problem with cyber attacks is that the successful response to the attack depends on knowing who is behind it and why, and responding can also include some risks. What if the enemy has not been identified or is wrongly identified? What if the enemy is identified but there is no strong proof about his identity or why the attack was perpetrated? Or what if the enemy is a non-state actor and then there is no capacity to destroy? The U.S. strategy also raises the question of the definition of an act of war in cyberspace. The Tallinn manual started the discussion on how to interpret international law for cyberspace and offers qualifications for the use of force or acts of aggression. However, the United States does not really distinguish between the two, which is interesting because it does push to frame cyber conflicts by reaffirming the applicability of international law but shows no clear consensus on the definition of an act of war or on where the threshold stands. This position seems to be against the logic of deterrence. Is the U.S. strategy to let the enemy know that there is a threshold with the hope that he will not try to find out about where the threshold lies? Is this a calculated ambiguity, where the U.S. is trying to keep the lid on deciding what qualifies as an act of war while, at the same time, retaining the ability to decide what an act of war is? This in turn would leave the possibility open for other nations to decide for themselves what the threshold is, with potential consequences.

Europe's Challenge, if It Wants an Independent Voice

To conclude, some tough questions remain to be addressed that are important for European countries if they want to have an independent voice concerning the cyber threat, cyber defense, or cyber war debates and also defend their democratic values. The public debate that started after the PRISM revelations raised two main issues: first, the balance or imbalance between security and civil liberties and second, the question of political oversight. These are core values for democracies and the consequences of cyber escalation are potentially huge, because we cannot be sure that the Cool War will remain so cool.

Chapter 28

Ready for a C5I Defence Command? Peacetime Challenges of Cyber Space and Cyber Intelligence

Mr. Marco Braccioli
Senior Vice President Area S.p.A.

Dealing with the Deep Web, Silk Road, and Bitcoin

What is the Deep Web? The deep web is a wonderful world, but it is a place where there is no law. In the Deep Web, aggressive governments are enrolling hackers whom they pay to attack their enemies—whomever they may be. This is where you can buy hours of attacks against a public site or an institution. The Deep Web is the vast part of the Internet that is not easily available to the usual search engines. Are readers of this chapter familiar with Silk Road? Silk Road is the equivalent of Amazon for weapons, of Amazon for illegal drugs, of Amazon for almost any illegal activity. It is even the Amazon for where Internet vulnerabilities are sold, and it is the Amazon for every kind of attack against organizations or infrastructures. Silk Road is the result of an emerging industry in this sector. Even if you are not familiar with Silk Road, you are probably familiar with Bitcoin, which is a form of money with legitimate uses that can also be used to pay for whatever you buy on Silk Road or elsewhere on the Deep Web. And this is not science fiction; it is reality.

It is partly to deal with the Deep Web and illegal activities facilitated by the Silk Road that the experience of our independent company supports three departments in Italy: the Departments of Justice, Interior, and Defense. We work on dual-use technology because the same technology that you would use to infiltrate a digital agent inside a group of criminals that are trafficking drugs is the same that you would use to deal with groups managing terrorist actions.

Challenges of Encryption, Cloud Services, Anonymizers, and Advanced Persistent Threats

On top of the challenges of the Deep Web and Silk Road, there are others such as encryption and Cloud services. Imagine this. We have citizens who are accessing data from within one country but these same data are actually stored in another country. This situation creates some strange problems, since a government may have to seek a search warrant in another country in order to obtain data concerning its own citizen. This is weird. To make matters worse, most of us have ten or twenty different accounts on the Internet ranging from online bank accounts to email to Facebook. So this means that we need strong instruments of correlation to understand what is happening on the Internet.

In addition, there are groups that are working using anonymizers, which attempt to hide their behavior on the Internet, and they are using this anonymity as a weapon against institutions. And then we arrive at the Advance Persistent Threats (APT), which are even more dangerous, especially in a military context, because everything under the sun becomes possible with APT. For example, the design specifications for an advanced military aircraft is stolen from the networks of one country and, just a few years later, a similar aircraft is produced and introduced to the Air Force of a country in another part of the world.

Cyber Security Is a Small Part of Information Warfare

Cyber security is just a small part of information warfare. Information warfare also includes intelligence, counter-intelligence, camouflage, disinformation, electronic warfare (including debilitation of communications, degradation of navigation support), psychological pressure, degradation of enemy information systems, and so on. So the cyber threats that are getting so much attention at the moment are just a drop in the bucket when you consider the full range of what we have to defend. This has strange consequences. In Italy, for example, our military forces are only allowed to defend, because—

without the common law that exists in Anglo-Saxon countries—we are not allowed to counter-attack, even kinetically.

Proposal for a C5I Cyber Command

As to intrusions, for example, the first intruders were smart people with quick fingers, but this situation has totally changed. Today, anyone can buy a cyber attack kit for 10,000 euros. For this reason, we can imagine creating a fifth domain—a C5I command. The mission is straightforward: the first priority is to defend the network and the second is to create a defendable one. Of course, we also have to ensure the mission command and, in particular, decide whether or not the critical infrastructure should be under military authority. Unless everything is under one command, there is no unity of command in case a decision has to be made. As another example, you could have a classified network up and running with a less secure transportation or navigation systems running underneath.

In conclusion, I would like to repeat a suggestion that I made earlier in this seminar, which is to emphasize the need for a cyber academy in every country of the Western Alliance. This is important because we need a new generation of cyber warriors that is both elite and trusted.

Chapter 29

Dealing with the Challenge of Cyber Security: The French Government's Approach

Mr. Patrick Pailloux
Director General, French National Agency for Information Systems Security (ANSSI)

I would like to discuss what France is doing in the cyber security area, the problems that we face at the moment, and our answers to these challenges. The subject of cyber security and how we can organize ourselves to respond to the threats is a sexy one because we are facing a lot of issues. I am in charge of coordinating the response to attacks or threats against national security targets in France. Given the number of attacks and espionage cases targeting our government and key parts of the French industry, the situation is really serious. So it is a hot topic for us and for our political decision makers. The very nature of cyberspace makes it impossible for any State in the world to succeed alone against these attacks. Just as is the case for aeronautics or space industries, strength comes from international cooperation. I notice that over twenty countries are represented at this workshop and that is a very good signal.

How France is Responding to the Threats—My Agency's Role (ANSSI)

Let me share what we are doing in France and the role of my agency. The National Agency of Information Systems Security (ANSSI) was created in July 2009 in the wake of the French White Paper on Defense and National Security. This White Paper is not the product of a think tank but the official presentation of the French defense and national security strategy as approved by the President. For the first time in France, the 2009 White Paper made the analysis that the risk of a major attack against a critical infrastructure was very probable in coming years and that we had to act on that issue. And in the way we always get ourselves organized in France, we decided to have a centralized system. We created an agency that is directly attached to the Prime Minister and has the global responsibility for answering the threats preventively, by helping the critical infrastructures that need to protect themselves, and also by being ready to react in case of a major attack.

Unfortunately, we discovered in 2010—earlier than expected—the first massive espionage cyber attack in France. It was a spying campaign that targeted our Ministry of Economy and Finance. This experience deeply changed the way we tackled the cyber threats. In 2010, we published the first national strategy for cyberspace and this strategy reaffirmed our main goals to:

- Strengthen France as a world power in cyber defense;
- Strengthen the IT system in companies that are vital for our economy and our nations;
- Help the information society to develop in a secure way and,
- Ensure the protection of all sovereign information so that the decisions and communications made by our authorities remain confidential when these authorities decide that it is necessary.

This orientation has been reaffirmed by decree in 2011 and by the French Council of Ministers' formal assignment for my agency to be in charge of our resilience against attacks. Today, we have reached new levels: on the logistical side, we have doubled the size of our staff and we have new offices. But our mission goes way beyond these facts and figures.

In its last version, the 2013 French White Paper on Defense and National Security stresses two elements:

- First, the importance of the cyber threats faced by our nation—the threat of a major disruptive cyber attack is considered to be the third highest threat on the national level;
- Second, the need for our nation to further develop our cyber defense capabilities. We must raise to an adequate level

the IT systems of companies that are vital for our economy and our nation. This was already stated less formally as a second strategic objective in our national cyber security strategy published in 2011.

National Priorities—Protecting the Critical Infrastructure, Identifying the Origin of Attacks, Developing Resilience, and Responding When Necessary

So let me summarize the key points regarding the French strategy. The first role of the government, and especially my agency, is to support the critical infrastructures. This includes developing awareness among our industrial and economic actors to make sure that they protect themselves adequately from attacks on their information systems—ranging from disruptive attacks on their critical systems to cyber espionage and thefts of their intellectual property.

The new French strategy also calls for a strategic stance in identifying the origin of attacks, organizing the resilience of the nation, and responding to attacks, which is a key role for my agency. The forthcoming Military Program Act, which will be a new law, will demonstrate our willingness to address cyber security matters at the right level. Resilience of critical infrastructure is a priority. It also means that France will put efforts into ensuring that it has the ability to autonomously produce essential security products and systems. It will also strengthen the human resources working on cyber defense through a unified chain of command.

Regulation of the Critical Infrastructures

The regulation of critical infrastructures that will result from the Military Program Act will be voted on before the end of this year in parliament. It will extend the government's capacity to control what is going on in critical infrastructures based on four themes:

- First, it will give the government the capacity to set up rules for operators. To give you an example of what we have in mind, we will have the authority to oblige nuclear operators to disconnect their electricity from the grid, or to prevent them from connecting their nuclear facilities to the Internet, that sort of thing. The situation in France is exactly the same as in other countries where there are no such rules at the moment. Companies have a lot of obligations regarding their physical security, fires, and other similar things, but they have no obligations regarding IT security. They can have very sensitive industrial systems connected to the Internet and that is totally allowed. So the first thing that we will change is to give the State the ability to set rules that operators will have to follow.
- The second idea in this project of law is to oblige operators to report to the government if they suffer an attack or an incident in their critical systems.
- The third idea is the authority to verify the security level of their systems. Verifying means doing audits, performed by the government itself, or by an accredited company.
- The last idea concerns times of crisis. It establishes a legal basis for the government to oblige operators to take some difficult actions. For example, in the physical world, when there is a fire somewhere, the government has the power to stop trains or close roads because it is dangerous for those who are in the train or drive their cars. So we must have the legal basis to close roads or stop trains. It is absolutely not the case today regarding the IT systems of critical infrastructure operators.

As you can see, it is a really ambitious law. The analysis that was conducted by our political leaders shows that we cannot continue to have critical infrastructures that are not under control and without verification, obligations, or security. The good will of operators is not sufficient to protect our nation against cyber attacks, especially against sabotage.

Of course, these new obligations on the private sector will require some other elements such as a set of new certified schemes for detection and mitigation of incidents. We need cyber companies in France that are able to help and manage cyber security, because most companies have absolutely no know-how, no ability to do so. We need to develop our cyber industry, an industry able to help all these companies, especially the critical ones, to secure their systems.

Although these new regulations only target critical infrastructure operators, i.e., about 100 French private companies, we look forward to their positive effects. In the case of the electrical company, for example, the regulations will target the big switching systems or the SCADA system, although they will not target the intranet or other similar things that are completely free. We also hope that these regulations will have a positive impact on small and medium size companies, which are completely out of the scope of these regulations.

The Importance of International Cooperation

As this workshop illustrates, European and international cooperation is vital. Why is this so? It is because most large companies are international. Therefore, it would probably be useless to set security obligations for a Franco-German-U.K.-U.S. company that would only be applicable in France. So we want all countries to increase the level of security of their critical infrastructure companies. This is one reason why France is in favor of a project supported by the European Commission that is called the NIS Directive Proposal. It proposes exactly what I have described to you, which is to create regulations regarding the cyber security of critical infrastructures operators.

In conclusion, let me stress again that, although states are responsible for their own national security, cyber security issues go far beyond national borders. At this workshop on global security, we are all aware that the security of information systems is a common international challenge and that cyber security can only be addressed with common and coordinated efforts. These efforts range from cyber crisis management to building awareness tools and from insuring the sustainability of cyber security industries to protecting critical infrastructures and other sectors.

Chapter 30

Cyber Security and the French Military Defense

Rear Admiral Arnaud Coustillière
Flag Officer Responsible for Cyber Defense, French Ministry of Defense

The Growing Cyber Threat

It is a great pleasure to be here at the 30th International Workshop on Global Security. I am the general officer in charge of cyber defense at the Ministry of Defense. The development of information systems represents a rich opportunity to enhance communication worldwide, but this improvement does not go without risks that need to be prevented.

The 2013 White Paper on Defense and National Security identifies the development of information systems as a major vulnerability and cyberattacks are seen as an important threat. These cyberattacks can take various forms: attempts to penetrate networks for purposes of espionage; remote takeover, paralysis and, in the near future, destruction of critical infrastructures or even weapons systems and strategic military capabilities.

Over the last few years, cyberattacks have been more and more sophisticated and are now targeting critical systems and aiming at their physical destruction. Today, every conflict has a global cybersecurity aspect: it can affect individuals as during the Arab Spring, major companies like the massive cyberattack against Aramco, or even the heart of a national sanctuary as it happened in Iran with Stuxnet.

Cyber is also an ideal weapon for non-state organizations, which can develop new capacities to confront States from abroad and with an ease they never had in the past. Jihadist groups are now all over the Internet for propaganda, including recruitment.We also see that hacktivists are structuring their action. Without clear borders, and dominated by the "fog" of a virtual world, cyberspace can be seen as a new field of opportunities for the attackers who benefit from anonymity and a lack of legal framework.

Cyber Defense—the French Defense Ministry's Response

Much effort is still needed to ensure the cyberdefense of our nation. A high level of political awareness is necessary to build a strong cyber community between several areas: military operations, Intelligence, governmental posture, and communication. All of them contribute to information superiority, which is the key element we must reach in order to guarantee our sovereignty and independence.

At stake for the French Ministry of Defense is the increasing level of cyber implications in recent military operations. This phenomenon started in Afghanistan and became increasingly important two years ago when we intervened in Libya and this year in Mali. Cyberattacks against the Internet websites of the Ministry of defense are now frequent. They are not very disruptive but show a tendency in cyberspace.

The Ministry of Defense has the responsibility to ensure the cyber defense of the French armed forces and has set up a chain of command in 2011 under the authority of the Chief of the Joint Staff. In this chain of command, I have been appointed to conduct the Defensive Cyber Operations of the MoD and to implement the cyberdefense posture within the whole ministry of defense as well as the armed forces.

Because coordination and an exhaustive knowledge of cyber incidents are essential, we have a unified, centralised and specialised structure. Regarding operations, the Joint Operations Planning and Command & Control Center (CPCO) takes into account cyberdefense in the planning and conduct of military operations. The French White Paper on Defense and National Security of 2013 spells out our national doctrine which defines our capacity to respond to major cyberattacks.

An ambitious work is going to be implemented to identify the origin of the attacks, evaluate the offensive capabilities of potential enemies and the framework of their information systems.

Our national doctrine is based on a global approach, with two complementary aspects:

- The implementation of a strong and resilient posture of protection for the information systems of the State, including operators of vital importance and strategic industries, as well as an operational organization for defense of these systems. This is coordinated under the authority of the Prime Minister, based on a close relationship among the services of the State, to identify and characterise rapidly the threats against our nation;
- A governmental capacity for an appropriate global response to attacks of various nature and size, which uses initially all the diplomatic, legal or police means, and the gradual use of means of the Ministry of Defense, if the national strategic interests were to be threatened. More specifically, within the Ministry of Defence, the cyberdefence posture covers all military domains: land, air and sea.

The new military framework includes cyberdefense military capabilities, which are closely linked to Intelligence. In an unstable world, and in cyberspace in particular, where the frontiers are not clear, Intelligence has a major role to play, to be aware of and anticipate the threat, as the French white paper on defence and security states:

- Protection of information and resilience of our systems are a high priority. Several measures have already been taken, from prevention and protection to active cyberdefense, as well as to offensive capabilities, but the last one is highly classified;
- Staff resources are going to be increased as well as security measures for information systems;
- Beyond that, we must support scientific and technological expertise in cyberdefense because the ability to offer our own security products is part of our national sovereignty;
- The cyber chain of command is actively consolidating. Cyber is now fully incorporated into the other chains of operations. The aim is to all work together. Our cyberdefense military doctrine is also being updated.

Cyber Defense—A New Strategic Domain Requiring Close Cooperation with Partners

These examples prove that cyberdefense is a new strategic domain and that is why close relations with our usual partners will have to be sustained. Our priority is NATO, and particularly the European Union with a complementary approach. The European Union will have to deal with its critical infrastructures and rapidly reinforce its cyber security capabilities in all domains, including the military domain. It will be a high stake effort for the CSDP, particularly at the next European summit at the end of this year.

International cooperation is essential in a space in which conventional frontiers do not exist. So it is essential to promote international dialogue. This dialogue can take different forms. It is important that European cooperation develops, complementing NATO policy.

Chapter 31

Cyber Space: Addressing the Tactical and Influencing the Future

Mr. Haden Land
Vice President, Engineering and Chief Technology Officer
Lockheed Martin Information Systems and Global Solutions – Civil

My remarks will focus on one of the opening comments today concerning the lack of U.S. government attention to the Cyber Security threat. I will touch on a number of initiatives that will hopefully alleviate some of those concerns and share a number of Cyber warrior efforts that are occurring in industry and academia. Finally, I will wrap up with some specific examples that Lockheed Martin is focusing on and that are part of this journey to enhance Cyber resiliency across the globe.

Responding to the Cyber Threat—in the Climate of "Sequestration"

Starting with sequestration, I completely agree that it is entirely unreasonable. It will impact new development, contracts, startups, and dramatically cut into the operations and maintenance budgets of a number of our agencies. Based on my discussions with the CIOs of a number of agencies, the likely budget reduction is in a range between 7% and 20%, assuming that the sequestration is to play out as originally planned. Of course, we hope that this is not the case. In my business, we have received few contractual actions of actual cuts—we need a contractual action in order for a cut to be implemented. We anticipate that there will be more. Thus far, we have experienced contractual actions related to some furloughs and scope reductions.

I project a trend toward smaller procurements across our industry along with shorter program life cycles. Essentially, the program construct would include a one-year performance base with options after that, which is different from the norm of a three-year performance base. However, regarding investments in Cyber Security research and development, they are actually up in many areas, maybe flat in some, but they are certainly not declining. My organization's internal investment in Research & Development and Cyber slightly increased while I took fairly substantial cuts in other innovation areas. Regarding Capitol Hill and activity in our government, there have been fifty bills with Cyber Security content since 2008. That is a dramatic change from before, which illustrates the Hill's interest and focus there. U.S. Cyber Command has twelve new offensive operations and today, according to the FBI, there are well over 120 nations that have Cyber operations as part of their national security fabric.

Earlier this year, President Obama signed a Cyber Security Executive Order allowing for commercial service providers such as ourselves, Northrop Grumman, and others, to partner with the department of Homeland Security to leverage their classified signatures. This can be combined with our intellectual property and that of partners, which can be transformed into an offering and capability for the commercial industry. For the government to take that position is almost unheard of, but we are looking at how the same level of protection and hardening of solutions that we provide our government agencies can be provided to the commercial domain.

In a study conducted two years ago, Gartner projected through this year that global Cyber defense spending for companies to just defend their network is $86 billion for 2013. If you compare that to the $388 billion individual crime impact and the $1 trillion lost by corporations that Irish Minister Alan Shatter talked about earlier, the amount invested is much smaller than the losses. Much of this $86 billion is duplicate spending because we do not collaborate as we should across industry. If we communicated more and shared more, we would certainly make that $86 billion go a lot further.

Regarding Cyber warriors, there are over 150 U.S. colleges and universities that have received recognition as Cyber Security centers of academic excellence. Another 100 colleges and universities are members of the Cyber Watch Program that is sponsored by the National Science Foundation. So, these two initiatives represent over 250 academic institutions that are contributing to address that space.

I also see a number of Cyber Security battle labs being developed across the academic landscape with a dramatic increase in regional and national Cyber competitions in the U.S. and allied nations. In addition, there has been an amazing increase in doctoral level Cyber programs in information assurance that cover both Information Operations and Cyber defense.

It is of special importance to me to connect these initiatives with allied nations and to interact with academic leaders who share this interest, one being Candace Johnson, an international telecommunications expert. The creation of Cyber warriors must be aligned to support both a global need and country-specific market competitiveness. I encourage everyone to point to the need to serve both the objectives of global security as well as country specific competitiveness.

Countries and corporations must provide Cyber Security awareness training to their citizens and to members of their respective industries. The aerospace & defense, and financial industries understand this, and the energy industry is becoming more aware, but I am convinced that others lack the appropriate level of awareness of the evolving Cyber threat vectors.

The Decline in Science, Technology, Engineering and Math (STEM) Graduates

Within the U.S. and across allied nations, we have experienced a decline in science, technology, engineering and math (STEM) graduates. This is not necessarily due to the educational system but rather to a lack of interest among young students to pursue STEM careers. In the fall, the state of Maryland will be launching a creative initiative called Life Journey that will give students the opportunity to "test drive" careers in STEM. Both the NSA and DHS are stimulating Cyber careers and Lockheed Martin is stimulating data scientist careers. We are trying to bring visibility and experience through gamification, electronic field trips, and other practical means.

We have also launched an initiative in the U.S. that integrates the "A" of Arts to STEM and turns it into STEAM. This new program will create analytical as well as creative thinkers, allowing simultaneous "divergent" artistic thinking and "convergent" engineer thinking. We believe that many jobs like forensic game analysts or certain kinds of data scientists will require that skill. We also lack STEM icons that can demonstrate value and motivate our future workforce and this is particularly true for the Cyber Security field. In conjunction with this, we in the U.S. opened a national Cyber Security Hall of Fame last year and inducted eleven individuals who are icons that people can aspire to be.

My last point concerns external efforts and another broad initiative that is being supported by the World Economic Forum. The World Economic Forum is a group of 98 signature organizations involving CEOs and ministers, and it provides a global platform for collaboration in Cyber Security information sharing, policy development and critical infrastructure. The annual meeting on global information security was held in San Francisco. The produced deliverables will include ten steps for CEOs to take if they are responding to a breach; a list of legislative barriers that governments should address to help improve information sharing; and a letter to members of the participating CEOs to encourage them to share actionable data in attack attempts.

Experience at Lockheed-Martin

Lockheed Martin has been the number one IT provider, specifically to the U.S. government, for nineteen consecutive years. We will continue our commitment to our government and allies. Accordingly, we deeply understand the growing threat across the Cyber Security landscape within private industries. For that reason, we have established a commercial Cyber practice that is now serving energy, financial, health care, high-tech, and communication industries. The same advanced skills and training programs that prepare my professionals who serve programs like the FBI Next Generation Identification System, the Defense Cyber Crime Center, the Classified Intelligence Predictive Analytics Programs and DISA Computer Systems/Network Security, have been adapted and applied to serve the commercial market.

Incidentally, our own Lockheed Martin internal network collects over two billion events per day from our sensors and we experience roughly 55,000 unique attackers per day. We leverage our response to these events to model solutions for our customers' environments. Within the past four years, we have opened four world-class security and innovation centers that are specifically dedicated to our customers, partners, and allies for collaborating on experiments and scenarios. These centers are located in the U.S., U.K. and Australia. Each one houses a security intelligence capability focused on advanced predictive analytics detecting cyber dust. More specific to the U.S. Defense & Intelligence agencies, we recently opened a Cyber Center of Excellence at Fort Meade.

Finally, industry collaboration is of utmost importance in this particular field. So, we are leading the Cyber Security Research Alliance that works closely with government, industry, academia to develop/share technologies in the area of cyber physical security and formed the Lockheed Martin Cyber Security Alliance with over 20 partners in industry that focus on sharing Cyber Security best practices and advanced solutions.

Chapter 32

The Cyber Threat—a View from Industry

Mr. Hervé Guillou
EADS

Since earlier speakers have already discussed the cyber threat from a governmental and military point of view, I would like to share with you an industry point of view. Our concerns and priorities have two angles. Like most of our colleagues in the Defense and Security industry, at EADS we are a target so we can test on ourselves the problematics of reaction and international governance—and we have also developed within our Cassidian division significant capabilities in cyber defense that are offered to the market.

Developing the Public-Private Partnership for Cyber Security

First, we welcome the development of governments' awareness and a sense of urgency in our countries. This has fostered programs to promote government expertise—civilian or military driven—and highlighted the need to create dedicated cyber industrial policies and partnerships with the private sector. For some time, this has been true in the U.S. and it is now developing quickly in the U.K., Germany, France, and the EU, with the understanding that our problem is not only a military question but also a question of the economic resilience of our countries.

In fact, our first message is that developing this public/private partnership is the only way to better protect our economies and citizens. This can be done by:

- Sharing some critical information about threat detection and strategies in trusted circles through more flexible boundaries between government and the trusted circles of private industries and operators;
- Developing awareness, cyber risk governance, through regulation and governance incentives;
- Developing joint training and education to remedy the lack of experts in the job market via academic master/Ph.D. level training centers and professional capabilities.
- Developing an industrial policy in order to control some key technologies that are important for national resilience and sovereignty. In this respect, I am particularly happy to welcome the different initiatives in the EU, U.S., U.K., France (the Obama directive; the clear conclusions of the French White Paper; the EU directives; the U.K. joint declaration of the Foreign Office/UK TI).

The Need to Organize the Cyber Security Marketplace

Second, we industrialists have a lot to do on our side to organize the offer in the marketplace. In particular, there is too wide a stretch between high-grade defense solutions and commercially available B2C solutions and services. It is our duty to develop and bundle these offers and adapt them for large economic and government actors: operators, public services, industries, banks etc. In fact, we cannot just rely on government for protecting us all beyond what they already have to do, even with increased budgets, which is to protect themselves and provide top expertise.

We also need to foster private sector initiatives to complement what governments do or do not want to do themselves. Here, I would see three priorities:

- Develop the real time dimension of cyber defense via Security Operations Centers (SOCs) and real time support and protection. It is not only a question of raising the level of the infrastructure: remember the Maginot Line!

- Support and protect the small and medium-sized businesses (SMEs) that are bringing most of the innovative technology bricks: for example in Europe, there are more than 250 SMEs with turnovers in the range of 20 million euros.
- Be able to package and bundle mid-grade solutions necessary for critical infrastructures and large critical industries that cannot rely only on commercial stand and basic protection. This will be reinforced very soon in some European countries by laws and regulatory requirements.
- Transform cyber transparency and risk governance in industry and get CEOs and CFOs to rely on themselves and not only on their CIOs; also transfer the cyber risk management responsibility to the company risk manager. Examples would be SCADA and embedded IT.

Finding Appropriate Ways to Work with Trusted Partner Nations

Finally, we must contribute to developing and supporting strategies beyond national boundaries and, this is my third message, in particular in the relevant trusted partner nations. We understand perfectly well that sharing information between countries on these matters is and will remain extremely sensitive and often limited, but, on the other hand, critical industries and operators are now barely only national. We also understand the difficulty of stepping directly from national circles to more than 25 countries like in NATO or the EU.

We would therefore support any form of dialogue with our governments to develop better cooperation between countries that trust each other. This cooperation should not be limited to Intelligence and information sharing. It should evolve toward R/D and industrial cooperation, making it easier to protect our public and economic jewels with common (bi-national, tri-national) solutions that can be compatible and certified by the different national requirements and regulations.

In our view, this is a key condition to having an ecosystem that is large enough to amortize the investment-R/D ratio needed from the private sector in this domain. This question is also under study among EU member states and NATO countries. We will continue to follow and support these developments closely.

Chapter 33

The Way Ahead: a Danish View

Ambassador Carsten Søndergaard
Permanent Representative of Denmark on the North Atlantic Council

I will limit my remarks on the workshop discussions to six takes: (1) the Transatlantic Bargain, (2) How do we in NATO react to the challenges? (3) the NATO-EU relationship, (4) the continued importance of the Middle East despite the U.S. pivot to Asia, (5) the new threats—including cyber, and, finally, (6) Afghanistan.

The Transatlantic Bargain—Will Europeans Be Able to Do Their Part?

The first point is that the Transatlantic Bargain is still out there, but the bargain is being modified somewhat. In other words, Article 5 is still valid, but the world is changing, pivoting to Asia. The U.S. has a global outlook as usual, while, on the other hand, the EU and the Europeans suffer from austerity measures, reduced budgets, and capability limitations. One should not only focus on what Europeans are doing, but also on how input relates to output. In any case, the basic question remains: are the Europeans able and willing to do what they are supposed to do when the "What ifs" occur? The unexpected always happens. I do believe that many Europeans hope that, after the drawdown in Afghanistan, it will all be over. They believe that there will be no operations for some time to come. The world will be quiet. History tells us, however, and this was underlined by the discussion this morning, that the world is full of unpleasant surprises. So we will be challenged.

How Do We React to the Challenges—with NATO or Coalitions of the Willing?

Second point: how do we react to those challenges, especially when they have a military nature? Well, we are all fully aware of Afghanistan. Next, remember Libya, which began as a coalition, with France and the U.K. in the lead. Then remember Mali, where we had France, definitely active, with some Allies also there. It worked well because we have procedures for that. As I mentioned yesterday, and Deputy Secretary General Vershbow mentioned it as well, there are also thoughts about a possible Libya training mission.

Post-ISAF, we need to sustain the interoperability of our forces, hence we will have to work together on the ideas about the Connected Forces Initiative (CFI). In my view, when governments in the future face the issue about operations, there will be a choice: should it be handled by a coalition of the willing or should it be handled by NATO? I do believe that the long-term impact will be negative for NATO if the prevailing option is the coalition of the willing. We are all fully aware that all politics is local and there might be several reasons for pursuing the coalition of the willing option. But, in my view, there is definitely a downside to it.

The NATO-EU Issue Must be Handled

Third take: NATO-EU. I could not agree more with what my Canadian colleague, Ambassador Brodeur, said but, on the other hand, this is definitely not easy. At the end of the day, it is a question about high politics in some countries, but there is an issue out there which, in my view, ought to be handled.

The Middle East is Still Important—Despite the U.S. Pivot to Asia

Fourth Take: The Pivot to Asia has been mentioned a couple of times and I do not question the importance of the rise of Asia. So do not misunderstand me. But I will make a point that the Greater Middle East is still out there, and, as I believe Alain Juppé said when he was Foreign Minister for the first time in the mid-nineties, the Greater Middle East is producing seventy percent of this world's international problems and it will continue to do so. The region from Marrakech to Bangladesh, to use another expression, will continue to produce many of the international problems that we will have to face in the years to come. Bernard Lewis recently offered a very good argument as to the importance of the long-term problems in that part of the world. If you look at the export from the combined Arab world, then subtract the oil and gas (the energy industry), the export from the combined Arab world equals that of Finland. There are also long-term social problems facing that huge part of the world. Some of us are being paid in order to reflect on the "What Ifs" in that region: Syria, Egypt, Iran, and Yemen, etc. There are certainly elements for a perfect storm. As it was formulated in a session, we should be aware of this unpleasant fact.

The New Threats—Including Cyber

Fifth take: There have been very good discussions on the new threats—diffusion of powers, cyber, organized crime, proliferation, terrorism and so on, and I have difficulty summarizing them in a few sentences, but I will try. As to cyber, I do believe that we are in the early days. The speed with which the cyber threat evolves is quite impressive and, clearly, our societies as a whole do face major challenges. It is not only defense, it is banks, pensions, and the health sector. There are at least three challenges:

- *Mismatch between Threat and Defense.* I fully subscribe to the comments of the previous SACEUR, Admiral Stavridis, that there is a mismatch between our defense and the threat. So we really have to work on that, regarding it as a societal problem.
- *Asymmetry.* The threat is indeed very asymmetric by nature, speed and so on. Part of the response was underlined and discussed by the previous panel on cyber, but there is also a question about culture and about mindset. Therefore, we should really think about how the public sector can react to it.
- *Rules of the Game*. Is it possible to introduce rules of the game in a sector which, by its nature, is anarchic? This is a good question.

Afghanistan

This is the final point. It concerns Afghanistan. We have three transition tracks under way: military, political, and economic. Next year, 2014, will be very important in Afghanistan. There will be lots of challenges and many tests for the international community. In that context, I would like to make two points: we are in the process of providing a security platform for Afghanistan so that it can handle its security much better. We need to keep in mind that the first responsibility for the international community is to work on this and we should constantly broaden that responsibility.

The Way Ahead

As I come from NATO, I will mention three issues: collective defense, crisis management, and cooperative security. They are key issues. Down the road, it will be vital to involve partners in addressing these challenges.

Chapter 34

The Strategic Environment Surrounding Japan

Ambassador Ichiro Komatsu
Ambassador of Japan to France

An Asia-Pacific View on International Security

I am very honored to be given this opportunity to speak before you today. Considering the limit of time allocated to me, without preamble, I will get to the heart of the subject that I wish to discuss, namely, the strategic environment surrounding Japan. My intention is not to be parochial, but I thought that the best way I could be useful would be by putting in an Asia-Pacific point of view in what seems to be an essentially Atlantic forum.

Since the end of the so-called "Cold War", the security environment in the Asia-Pacific Region has undergone and is undergoing significant changes. What is regrettably not always well understood in Europe, where the strategic environment did ameliorate since the fall of the Berlin Wall, is that it is another story in our part of the World. In sharp contrast to Europe, where your strenuous efforts and creativity gave birth to multilateral frameworks of regional integration in the economic, political, and defense and security fields (such as the EU and NATO), Asia is, let's face it, far behind. Asia is a region where there are many countries with very diverse sizes, political regimes, historical and cultural backgrounds, degrees of economic development, and, degrees in the adhesion to fundamental values such as freedom, democracy, respect for human rights and the rule of law. There is still, well and truly, a remnant of Cold War in the Korean Peninsula. Because of all these elements combined, the strategic environment in our part of the world has degraded since the demise of the Cold War, unlike in Europe where people enjoy the dividend of peace. I think that what is important is the notion of indivisibility of security between Europe and the Asia-Pacific region.

Japan's Security Challenges

Let me present to you a rough sketch of the various security challenges that Japan is facing in this precarious strategic environment.

North Korea. First, the North Korean nuclear and missile issue is the greatest threat to our national security. DPRK poses a clear and serious danger not only to Japan and East Asia nations, but also to the whole international community. Regarding Japan's basic policy on North Korea, the normalization of our diplomatic relations is only conceivable by addressing all the pending issues between Japan and North Korea such as (i) abductions of Japanese citizens, (ii) North Korea's nuclear weapons program, (iii) North Korea's missiles program, and, (iv) the settlement of the unfortunate past between us.

It is deeply regrettable that, despite repeated calls by Japan and the international community, North Korea is still continuing its provocative and dangerous actions. On 12 December 2012, North Korea launched a so-called "satellite rocket"and, two months later, it announced it had conducted a third nuclear test. Such actions are a real risk for the disarmament and the non-proliferation of nuclear weapons, especially as North Korean authorities are pursuing a program of developing ballistic missiles capable of carrying weapons of mass destruction. These actions are also an offense against the authority of the Security Council and other international frameworks.

Perhaps may I briefly note that, for Japan, North Korea's medium range missiles (we believe that hundreds of them have already been deployed and aimed at Japan) and the possibility of miniaturization of nuclear warheads represent a much greater threat than North Korea's supposed ICBMs.

It is essential that the international community keep on condemning and providing a strong response to such repeated provocations. Even if North Korea has recently showed a willingness to resume dialogue, the international community must continue to respond appropriately to this matter, as we know from past experience that North Koreans could change their mind again.

Russia. Secondly, with Russia, there are still some important issues to be resolved, like the resolution of Japan's Northern Territories issue and the conclusion, thereby, of a peace treaty that is still pending 65 years after the end of the Second World War. This being said, we are making substantial progress in our bilateral cooperation in other areas, such as security, economy, culture and personnel exchanges. In late April of this year, Prime Minister Shinzo Abe paid an official visit to Russia, the first one by a Japanese premier over the last 10 years. He and President Putin agreed, among other things, to accelerate the negotiations towards the solution of the territorial issue and the signing of a peace treaty.

Japan-China. Thirdly and most importantly, we cannot discuss Japan's security without addressing China which is increasing its economic and military presence. Japan-China relations are a key factor in the stability and prosperity of the Asia-Pacific region. We, in Japan, firmly believe that we should deepen our "mutually beneficial strategic relationship" (this is the exact term used in the Joint Statement between Prime Minister Yasuo Fukuda and President Hu Jintao issued at the time of the Chinese President's visit to Japan in 2008). At the same time, I would be dishonest if I did not say we have some concerns.

One of our major concerns is the rapid and continuous development of China's military budget. According to the official figures, China's defense spending has grown 30 times over the past 24 years while Japan's military expenditure has hardly evolved for almost a decade. We are talking here of official figures only, whereas a big problem we see is a lack of transparency.

In recent days, China has been intensifying its assertive maritime activities especially in the East and South China Seas, thus becoming a destabilizing factor in the Asia-Pacific region. As to the Senkaku Islands, which are frequently portrayed by the French media, there is not an iota of doubt to the fact that these Islands are clearly an inherent part of the territory of Japan, in light of historical facts and based upon international law. I can speak for two hours on the legal details, but today I will content myself with a résumé on the subject. Let me only underline the fact that the Senkaku Islands are under the valid control of Japan, and it is the Chinese side which is attempting to change the status quo by force.

Dealing with Mounting Tensions with China

Tension between Japan and China continues to mount because of many provocations on the part of China. These provocations include (i) repeated incursions into Japan-controlled waters by Chinese vessels, and sometimes in a violent manner, (ii) illegal landing of Chinese activists on the Senkaku Islands, (iii) violation of Japanese airspace by a Chinese surveillance plane. On 30 January 2013, a Chinese military frigate locked its weapons-targeting radar on a vessel of the Japan Maritime Self-Defense Force. Being specialists in defense and security matters, you must know how serious and dangerous such an act is. In 2012, Japan Air Self-Defense Force (ASDF) scrambled fighter jets against Chinese planes suspected of violating Japan air space 306 times, which almost doubled the 2011 figure. This by far outnumbers the number of scrambles against Russian aircraft, which has always been the highest as far as the ASDF is concerned.

Last May, two Chinese academics published an article in the People's Daily, the official organ of China's Communist Party, which questioned Japan's sovereignty over Okinawa. In November 2012, the former U.S. Secretary of State Hillary Clinton revealed that her Chinese interlocutor had suggested to her they might be able to assert territorial rights on Hawaii. Here is my simple question. How far will the Chinese unilateral territorial claims go?

During his recent state visit to Japan, French President François Hollande called in his address to Japan's Parliament to ease tensions in Asia through dialogue and in conformity with international law.

Japan remains firmly committed to a peaceful solution of problems based on international law. Prime Minister Shinzo Abe has been repeating that he favors summit-level discussions with Chinese President Xi Jinping but, so far, he has received no response.

Former United Nations Secretary-General Javier Pérez de Cuéllar once said, while dealing with Iraq under Sadam Hussein: "It takes two to tango."

I hope de Cuéllar's words will not fall on deaf ears this time.

Chapter 35

An Unpredictable Future—The Way Ahead

Ambassador Yves Brodeur
Canadian Ambassador to NATO

Since the workshop's title is "Peace and Security—The Challenges Ahead," I have the difficult task of trying to define the way ahead. My approach to that goal has been very practical. As an ambassador, I have to provide advice to my minister. What shall I take away from this two-day workshop and report to my minister, especially concerning the future? Here are my observations.

Factors Influencing Future Security

An unpredictable future. As we were reminded during the workshop, the future is more and more unpredictable. It was already difficult to predict a few years ago, and prediction is becoming even more complicated. None of us here could have predicted the Arab uprising and its consequences, which are still unfolding; so trying to imagine what could happen between now and even three or four years later is therefore rather difficult. As an example, I got my first computer in 1989, almost 25 years ago, and we take for granted things that have existed for quite a long time. Yet, we still have difficulties tackling the cyber dimension of the Internet. And who would have imagined that the Internet would change our lives the way it did? Again, that was something that we could not predict.

The fragmentation of power. If we look specifically at the security dimension of the Internet, we know that the future will continue to bring a fragmentation of power. In this context, we often hear the word "multipolar." It would be more appropriate, however, to talk about fluidity. Why? Because if something has a pole, it suggests or implies something quite solid, even though there might be one or many poles. But if there are poles, they are a little shaky at this point. So perhaps we should be thinking about a very amorphous situation that is evolving quickly and over which we have little control.

A disfunctional global governance architecture. This point is very important for all of us who are dealing with security and defense issues. For instance, the U.N., and the Security Council in particular, is more and more difficult to govern and seems to be increasingly challenged to arrive at decisions that can help promote a global agenda of peace and security—not to mention international laws. This is a real issue that we need to discuss. And sometimes, when I look at the NATO Council, I have the impression that we are also turning into something that looks a little like the U.N.: lots of words, few decisions, with more preoccupation about national interests instead of global collective interests. The EU is also challenged, but since I am not a member of a EU nation and have no vocation to become one, I think it is not my business to comment on it.

The demography factor. Very little was said about demography during these two days, but I think that demography is an important factor in security. If you look at the world population, which is seven billion, America and Europe represent approximately one billion people. What happens to the six other billion? Someone made the comment that with one billion people you can create between the United States and Europe a great space of free trade (that would eventually, I hope, include Canada), but it includes only one billion people. What does that do for the 6 other billion? This is a question that we have to ask ourselves because demography is playing against us. We all come from countries where the population is aging, while the population in the other part of the world is not. I think that many of the assumptions that we base our actions on will have to be reviewed through the prism of demography over the next two years.

New threats and new trends. I would also mention to my minister the new threats and trends that are emerging. We spoke about the proliferation of missile technology, cyber, and terrorism. Terrorism is not a new thing, but what is new is that it is now in our backyard. It is coming to our nations thanks to the Internet, thanks to homegrown radicalization, and what we can do about it is a big question mark. Earlier, I was mentioning that two of the attackers in Algeria at a gas production facility had Canadian passports, but they were not from Muslim roots. They were Canadians born in Christian families who converted and became radicalized. How we deal with that kind of situation is an issue that will start to haunt us.

Similarly, on the subject of biochemical proliferation, any fourteen year-old with bad intentions can download from the Internet and cook in their mother's kitchen a recipe that could actually kill quite a few people. And we cannot even imagine what some new trends, such as 3D printing, will bring us. When it was initiated, the Internet was seen as a curiosity and a nice way to obtain vast amounts of information quickly. Now it is possible to buy weapons on the Internet.

The shifting energy paradigm. This is an issue that we have already spoken about. What if the United States, which is energy independent, actually decided that it might not be in its interest to be so preoccupied with what is happening in another part of the world? There are implications to the shifting energy paradigm that are important for us and we should look at them. I believe that we do not discuss this enough.

The growing gap between technological innovation and policy. As we speak now, some of our nations are investing in capabilities that will be totally obsolete by the time we deploy them. The cycle of development design is ten to fifteen years. What is going to happen in ten or fifteen years? We don't know, but there is a fair chance that the hundreds of millions of dollars, if not billions, that are being spent right now may actually not be very productive in the end. How to think outside of the box and start to prepare for the future is going to be a real challenge. It was already a challenge and I believe it will become a bigger one.

What Needs to Be Done

Where does that leave us? In an American cartoon from the seventies called Pogo, a character says, "we have met the enemy and he is us." What the enemy is called is lack of coherence, lack of priorities, difficult economic circumstances, duplication, political paralysis, and fear of risk. These are all things that are actually stopping us from making the sort of courageous and difficult decisions that we must now make in order to be ready ten years from now. What I would tell my minister is that we need to:

- First, fix the EU-NATO cooperation dilemma, not invent new structures.
- Second, make the right choices, focus on essential capabilities that we badly need.
- Third, eliminate surpluses and accelerate regional integration. I believe this is a must. For many nations, maintaining the full range of assets makes no sense. It is just a distraction from the things that what must do collectively, which are deployability, sustainability, specialization and interoperability.
- Concerning burden sharing, we should stop being obsessed with numbers and start to really focus on output, quality, and relevance. That is the most important. What we bring to the table is more important than how much we bring.
- Finally, we need to understand the risks and make some very difficult decisions. We must tell our publics that we are investing in defense matters but not in an indiscriminate way. We should be selective, clearly explain the consequences of not making certain decisions, and see if our publics are prepared to live with that risk or not.

To summarize, I will say that there is an urgent need for us to develop a coherent and realistic approach to security and defense that brings together NATO, the EU, and willing partners outside of the scope of these two institutions that are actually interested and willing.

Chapter 36

Prospects for Afghanistan: a Chinese Perspective

Major General (Ret.) Jihua Cai
Chinese Institute of International Strategic Studies

First, the international community should strengthen international cooperation under the framework of the U.N.. Currently the Afghan security situation remains fragile and will get worse after the withdrawal of the U.S. troops. Much will depend on the capability of the Afghan security forces to control the situation. It is a fact that NATO member states and the Shanghai Cooperation Organization (SCO) share common interests in maintaining security and stability in Afghanistan. Moreover, Afghanistan is not only America's important ally outside NATO but also an observer state in SCO. Therefore, in the near future, the creation of a coordination mechanism between NATO and SCO under the framework of the U.N. should be considered.

For over ten years, NATO, headed by the U.S., has maintained a special post in Afghanistan. NATO needs to take into account the concerns of other countries in launching an international counter-terrorism war in Afghanistan. For example, Russia and Central Asian countries are concerned about the proliferation of Afghan drugs and hope to cut off the sources. Pakistan is concerned about the impact of Afghan refugees on its economic and social stability and also about U.S. drone strikes, which might harm its sovereignty and independence. Other neighboring countries of Afghanistan worry about the penetration of terrorists, and China is concerned about the security of its western border areas.

Chapter 37

Coalitions, Partnerships, and Foresight: Why They Matter

Ms. Neyla Arnas
Senior Research Fellow, Center for Technology and National Security Policy,
National Defense University[1]

> "Relationships matter more than ever. Coalitions and partnerships add capability, capacity, and credibility to what we see as shared security responsibilities. We are committed to expanding the envelope of cooperation at home and abroad."
> Chairman of the Joint Chiefs of Staff, General Dempsey, 13 October 2011 ("House Armed Services Committee Hearing")

Workshop Observations[2]

The 2013 International Workshop on Global Security covered a tour d'horizon of topics, ranging from the post-2014 challenges facing the Euro-Atlantic community and the ongoing developments in the Middle East and North Africa (MENA) to problems and prospects of navigating internal and external cyber threats.

NATO offers connectedness. The alliance is a community of shared values and aspirations for the world as well as a means for military connectedness. As SACEUR General Philip M. Breedlove says, "you cannot surge trust and engagement." Perhaps this is the most underrated attribute of NATO, not only for its member states but also for its vast array of partners. It is a coalition-enabling institution: the ultimate tool for coalition building that also brings with it international legitimacy.

NATO's uncontested strength is derived from its ability to project stability. The question of the moment is how to sustain that capability in the face of fiscal challenges. This will require: partners to be sources of stability in their regions; national defense budgets that are analyzed in terms of deployability; decreasing the overreliance on the U.S. in the long term; and European nations doing more financially and collectively.

NATO is an international institution where European objectives can be achieved by focusing on capabilities. European participants saw challenges in duplicative and parallel structures. In their view, Europe needs to focus on building capabilities rather than institutions in order to strengthen its military contribution to Euro-Atlantic security. They called for improving European production and procurement systems, particularly among E.U. Allies, where fragmented programs exceed collaborative ones. This fragmentation duplicates production and causes variations in standards of equipment, weakening military interoperability.

The US sequester/budget concerns—not the shift to Asia—will affect the U.S. force structure overseas, including in Europe. Former Chairman of the Joint Chiefs of Staff Admiral Mike Mullen has stated that the single biggest threat to national security is the U.S. national debt, drawing a connection between the resources used by the military to the economic health of the nation.[3] Contrary to the concerns of many European participants, the U.S. strategic shift to Asia will not be the prime driver of U.S. force reduction in Europe. A sequester means that all U.S. military forces get smaller—not just those in Europe.

Decades of under-investment in European militaries, coupled with the contraction of the U.S. defense budget, will require the pooling and sharing of resources now more than ever. One workshop participant made the case to stop the hand wringing and to accept the new strategic environment characterized by austerity, economic, and fiscal crises—these will not soon pass. Even so, the question remains the same: do we continue to spend on defense? *The focus should be on pooling resources to purchase interoperable and useful defense tools ("smart defense").* The requirement for robust ground forces still remains as these forces work amongst the population—while the morality and limitations of unmanned warfare continue to be debated.

[1] The views expressed in this article are the author's and do not reflect the official policy or position of the National Defense University, Department of Defense, or the U.S. Government.

[2] General Dempsey, Admiral Mullen, and General Breedlove who are quoted here were not present at the workshop.

[3] http://www.defense.gov/news/newsarticle.aspx?id=60621

NATO's challenges, ranging from cyber policy, the future of the MENA region, and defense spending, require thinking about the long-term implications of current day decisions. Those *decisions need to be regularly revisited and recalibrated based on changing circumstances,* including advances in technology, changing demographics and climate, and global economic performance.

NATO should expect more engagements along the lines of Bosnia, Afghanistan, Libya, and Mali. In each case, *the adversary typically has had the strategic advantage of knowing the culture and population and intimate understanding of* the *issues which drive the conflict.* The international community has fallen short in addressing with equal vigor the day-to-day aspirations of populations—through education and business opportunities, for example. Another way to look at it has been acknowledged by several U.S. generals and diplomats: we do not know the operating environment.[4] DIA Director, LTG Michael Flynn notes that one of the primary enduring lessons from our recent years at war is that we need "to understand the cultures and environments in which we operate." Doing so would provide "decision advantage."[5]

Calling for a New Paradigm: Foresight

We are still preoccupied with linear formulations to issues, yet the world is increasingly confronted with nonlinear interactions amongst seemingly unrelated topics.[6] The old paradigm based on Cold War assumptions which shaped our current international organizations and government security systems no longer applies. The global security context has changed; so too must our organizational structures and thinking. All these issues lend themselves to a more disciplined analysis of alternative futures.

How and what to change to meet 21st century challenges is much less intuitively obvious, not to mention threatening to established institutions. To which government or international organization can we point to see a foresight, network, feedback loop that incorporates foresight into strategic thinking?[7] No matter how hard we continue to work within institutions designed for a different era, we are likely to continue to come up short.

The Value of Foresight to Security Challenges

Disciplined 'foresight' is needed to guide investment and development of capabilities that are sufficiently flexible to adapt to these evolving requirements and opportunities, even when they are not predicted by 'strategic analysis.' Investing in these 'foresight' capabilities and institutions will pay dividends.

Foresight is the disciplined analysis of alternative futures.[8] Foresight should not be confused with forecasting or prediction. It is about looking at weak signals and at the improbable. Because we cannot be prepared for every possible contingency, the result of foresight should be a resilient system that can respond systematically, flexibly and efficiently to surprise and fluid global events. If forecasting and strategic analysis are the examination of extrapolated predictions based on already identified trends, then foresight is about anticipating the broader range of possibilities that could emerge from developing

[4] See Lieutenant General George Flynn, A Decade of War: Enduring Lessons from the Past Decade of Operations (Suffolk, VA: Joint Chiefs of Staff, June 15, 2012). Also, "Odierno Admits U.S. Failure in Iraq" (Al Masallah News, October 24) U.S. Army Chief of Staff, Gen. Ray Odierno, said that U.S. troops failed to turn the U.S. invasion of Iraq into a strategic success, noting that U.S. ground force commanders are working to extract lessons learned from the past decade of war in Iraq and Afghanistan. Gen. Robert Cone, Chairman of the Education and Training Department for the U.S. Army said that "We had an extraordinary campaign. We achieved all our goals, except one. We crossed the Iraqi border with a list of targets and were ordered to fight, but what was missing was a deeper understanding of the country's history, culture, and its tribal structure." For a diplomat's view, see Ryan Crocker, Supplying arms to Syria or military intervention could make matters worse," July 23, 2013 at http://yaleglobal.yale.edu/content/containing-fire-syria.

[5] LTG Michael T. Flynn, USA, Director, DIA. "Accelerating Change: Today's Imperative." Presented at SMA Conference, 13 November 2013. LTG Flynn describes an environment where the irregular is regular and crises become routine. As far as lessons learned from a decade of war in Afghanistan and Iraq, (CJCS Enduring Lessons, Vol 1 June 2012) one of the primary points is to understand the cultures and environments in which we operate. It's about providing decision advantage. Changing the way we think changes the way we fight.

[6] For example, in simplistic terms, cyber security has become an issue as technology has been used by non-state and state actors as a "weapon." The unrest in the MENA region has been characterized as a confluence of demographics, climate change, food shortages. (See Center for American Progress, February 2013, The Arab Spring and Climate Change.)

[7] See Anticipatory Governance: Practical Upgrades. Leon S. Fuerth with Evan M.H. Faber. Anticipatory Governance would make foresight a component of the policy process using networked systems to support whole-of-government responsiveness, applying feedback systems to monitor performance and speed up learning from results.

[8] A joint project between National Defense University and the Department of State, called "Actionable Foresight" focused on the linkage between longer term analysis and national security decision-making. In this context, foresight is defined as the disciplined analysis of alternative futures that provides decision makers with the understanding needed to better influence the future environment (Leon Fuerth). How do we incorporate foresight into the national security process so that it is considered seriously—and acted upon—in planning and decision-making?

strategic conditions.[9]

More often than not, forecasting models, wargames and the like, focus on the "likely/big impact" possibilities, sidelining if not completely dismissing, the "unlikely/low impact/high impact" possibilities. With such preparation, is it any wonder that we remain perpetually caught in strategic surprise?

Foresight can be characterized by the following:[10]

- Buys time for reflection and reason;
- Is the ability to manipulate possibilities in the mind rather than in the battlefield or street;[11]
- Continuously revisits assumptions;
- Is not strictly data driven or about prediction, but hypothetical, in considering how unrelated parts may interact;
- Is the ability to think across categories;
- Is insisting on asking the hard, unasked questions;
- Is understanding the full implications of an issue as opposed to a compartmentalized single issue focus;
- Is engaging in "mindfulness" as a model, an awareness of how an event affects the operations of an entire system;
- Is different from intelligence which largely focuses on analysis rather than synthesis;
- Actively seeks diverse ideas from diverse backgrounds.

These characteristics aside, the human reflex still tends toward the desire to predict the future. By definition the future is unpredictable and we would do well to acknowledge this. It is true we can examine trend lines (linear). Yet in combination with other trend lines and human nature, the picture becomes more complex. We default to examining the most likely, most probable, and the consensus of experts, which can boil down to lowest common denominator conclusions. We seek input that reinforces biases. However it is the things we dismiss as highly improbable that catch us by surprise when they happen. We need to change fundamentally how we think about issues, which requires embracing nonlinear, cross disciplinary, creative, and (currently) unconventional thinking.

Foresight can be a tool in strengthening NATO's ability to prepare for evolving security challenges by:

- Exploring hypothetical contingencies and solution sets to complement evidence-based approaches.
- Alerting stakeholders to consensus—"lowest common denominator"—habits that preclude outlier ideas.
- Considering trend projections across topics and regions in non-linear, interdisciplinary approaches.
- Bringing together people from diverse backgrounds and disciplines.
- Identifying opportunities that are not only responsive, but preventative and out-of-the-box.

Foresight offers a different way of thinking about an uncertain strategic landscape. When considering the traditional areas of security concerns, future security challenges will likely occur at the interplay of technology convergence, changing demographics, and climate change impacts such as food scarcity. In addition, emerging technologies level the playing field between institutions and non-state actors, governments and publics. Coupled with changing demographics, these networked publics become distanced from the historical accomplishments of the trans-Atlantic link. The threat perception between publics and governments is very different and that gap is growing. This poses a risk to the influence of international institutions such as NATO.

Take the immense economic and governance challenges in the MENA region, for example. Is the existing partnership toolbox within NATO (Mediterranean Dialogue, Istanbul Cooperation Initiative) appropriate to the new realities in the region? How does an international organization consciously take into account a largely youthful demographic fluent in social media? Does the organization allow consideration of income inequality, unemployment, and a young demographic, empowered and connected by emerging technologies in the development of policies geared toward the region?

[9] Josh Kerbel, Chief Analytic Methodologist, U.S. Defense Intelligence Agency.

[10] These ideas were developed during a series of workshops in 2010 and 2011 on "Actionable Foresight" at the National Defense University in partnership with the Department of State, Bureau of Intelligence and Research. The author wishes to particularly acknowledge the contributions of Mr. Warren Fishbein and Dr. Susan Nelson.

[11] Leon Fuerth, Research Professor of International Affairs, The Elliott School of International Affairs, The George Washington University, The Project on Forward Engagement.

Using Foresight to Do More

Workshop discussions called for the need to do more, accepting the new normal of economic crises and political turbulence. We seem to be focused on maintaining the status quo in a changing environment, whereas we should be clear about supporting and spending on what is required for security. Here again, applying foresight could help develop alternative courses of action.

Ambassador Victoria Nuland, Assistant Secretary of State for European Affairs (and former U.S. Permanent Representative to NATO), has characterized this evolving environment in terms of an "inflection point" calling for a "trans-Atlantic renaissance" that goes beyond maintaining the status quo. It is a message in keeping with the conclusions of the workshop:

> Today, as a trans-Atlantic community, we're standing at another vital inflection point. Recovery should not be enough for us. What's required is a trans-Atlantic renaissance—a new burst of energy, confidence, innovation and generosity rooted in our democratic values and ideals. When so much of the world around us is turbulent and unmoored, we have to be that beacon. Together we must lead, or we will see the things that we value and our global influence recede.[12]

[12] http://www.atlanticcouncil.org/news/transcripts/transcript-toward-a-transatlantic-renaissance-ensuring-our-shared-future

international workshop series on global security

PRESENTED BY

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

PRINCIPAL SPONSORS

French Ministry of Defense | United States Department of Defense | North Atlantic Treaty Organization

MAJOR SPONSORS

Northrup Grumman | Orange | MITRE | Tiversa | Area S.p.A.

ASSOCIATE SPONSORS

URS | Juniper

CENTER FOR STRATEGIC DECISION RESEARCH & STRATEGIC DECISIONS PRESS
2456 Sharon Oaks Drive | Menlo Park, California 94025 USA | www.csdr.org