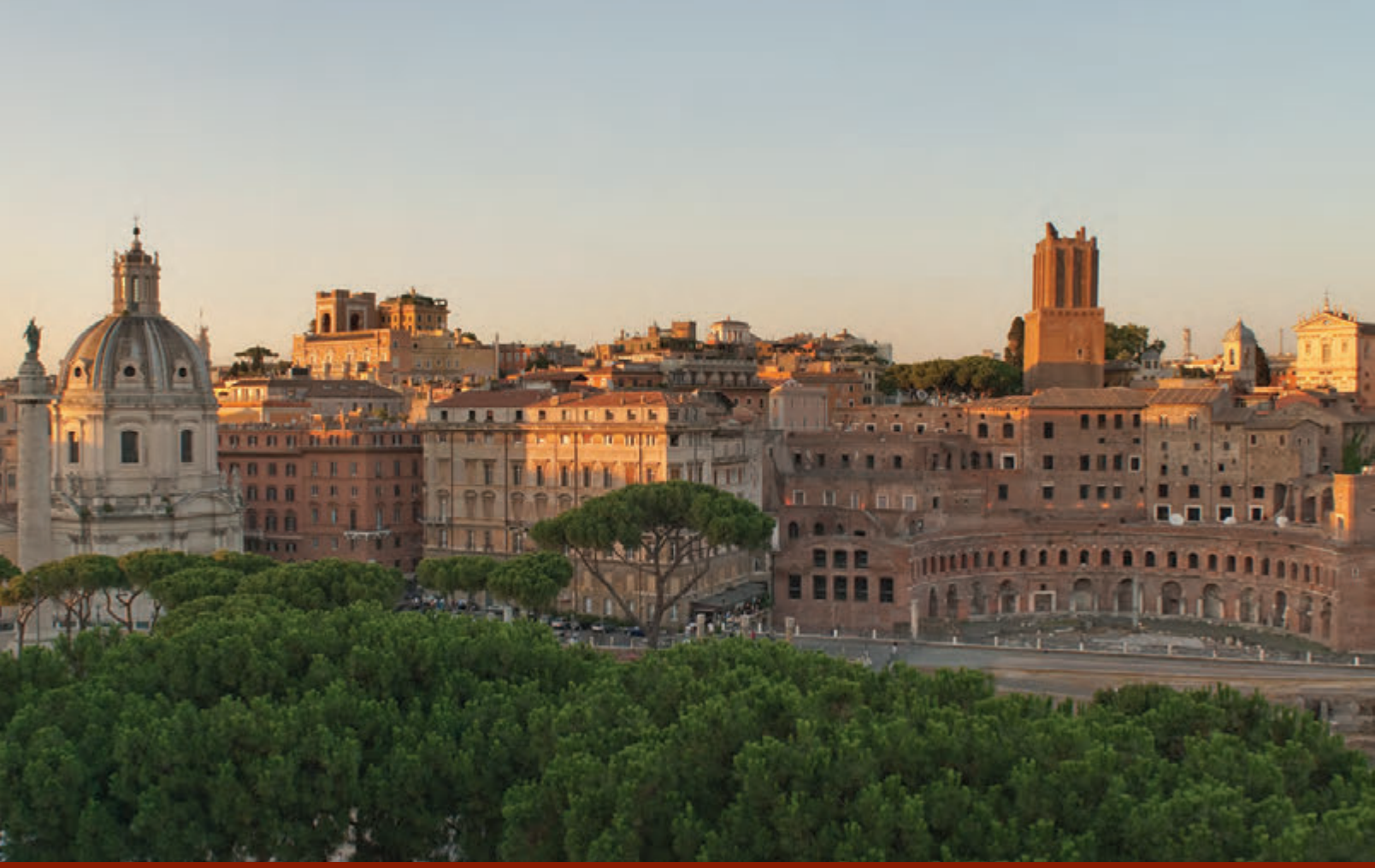


Critical Challenges to Peace and Security

The Economic Crisis, the Arab Spring, Afghanistan & the Rapid Growth of Cyber Threats

PROCEEDINGS OF THE 29*th* INTERNATIONAL WORKSHOP ON GLOBAL SECURITY

His Excellency Giorgio Napolitano, President of the Italian Republic
His Excellency Admiral Giampaolo Di Paola, Minister of Defense of Italy
Workshop Patrons

Dr. Roger Weissinger-Baylon, Co-Director of CSDR
Workshop Chairman

Anne D. Baylon
Editor

Critical Challenges to Peace and Security

The Economic Crisis, the Arab Spring, Afghanistan & the Rapid Growth of Cyber Threats

PROCEEDINGS OF THE 29*th* INTERNATIONAL WORKSHOP ON GLOBAL SECURITY

His Excellency Giorgio Napolitano, President of the Italian Republic
His Excellency Admiral Giampaolo Di Paola, Minister of Defense of Italy
Workshop Patrons

General Biagio Abrate, Chief of Defense General Staff of Italy
Honorary General Chairman

Dr. Roger Weissinger-Baylon, Co-Director of CSDR
Workshop Chairman

Anne D. Baylon
Editor

FRONT COVER

View of the Forum of Trajan from the Vittorio Emanuele II Monument terrace

INSIDE TITLE PAGE

Night view of the Roman Forum from the Capitoline Museum

BACK COVER

Statue atop Vittorio Emanuele II Monument of the goddess Victoria riding on a quadriga

---

International Standard Book Number: 1-890664-19-7

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

Photography by Jean Lee.

Center for Strategic Decision Research

&

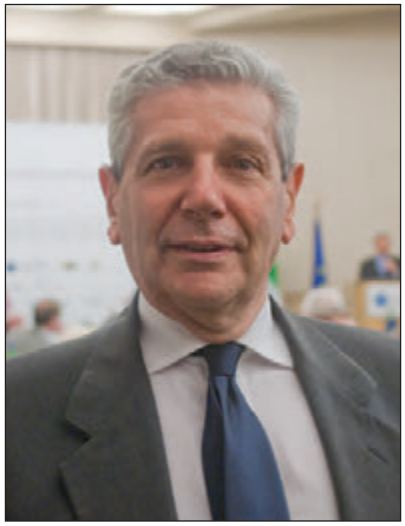
Strategic Decisions Press

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

His Excellency Giorgio Napolitano
President of the Italian Republic
Workshop Patron



His Excellency Admiral Giampaolo Di Paola
Minister of Defense of Italy
Workshop Patron

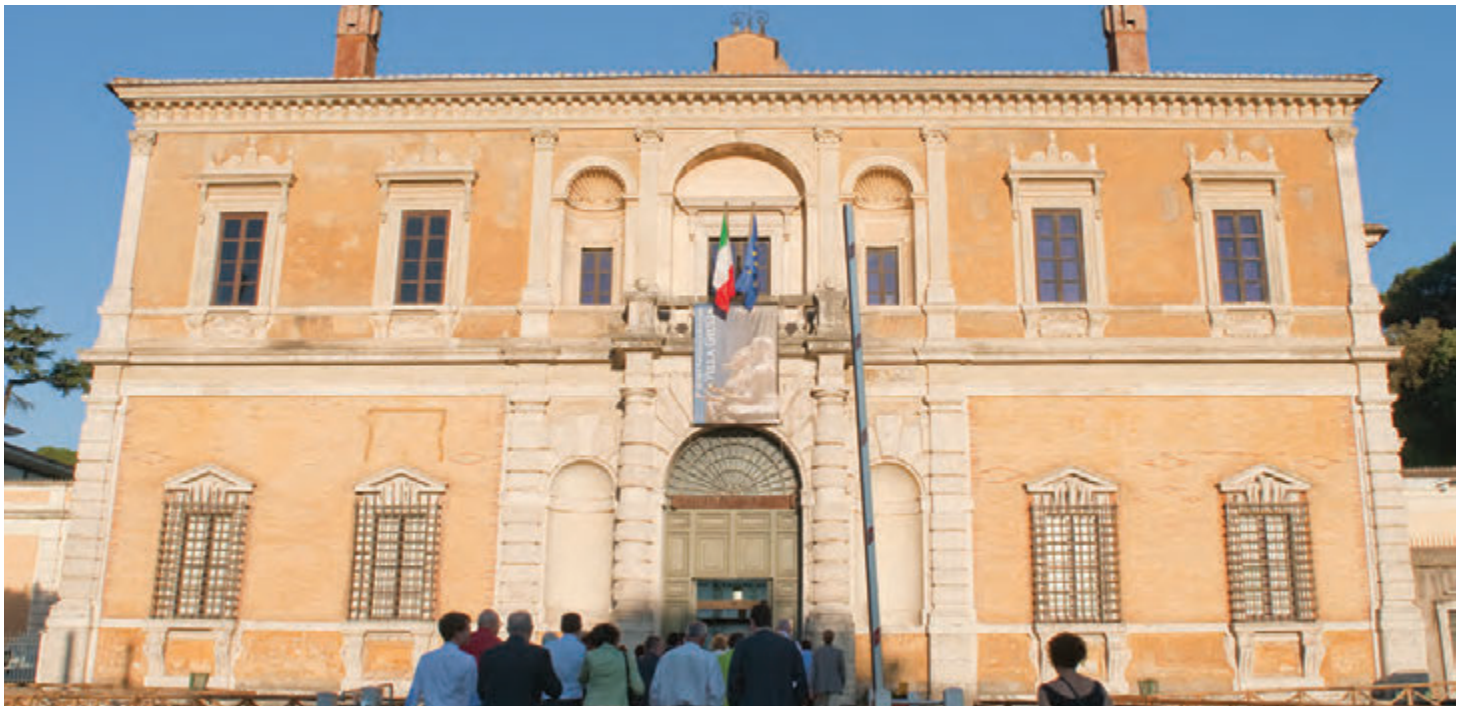
TOP ROW
Participants arrive at Villa Giulia for a private visit of the Etruscan National Museum in Rome.

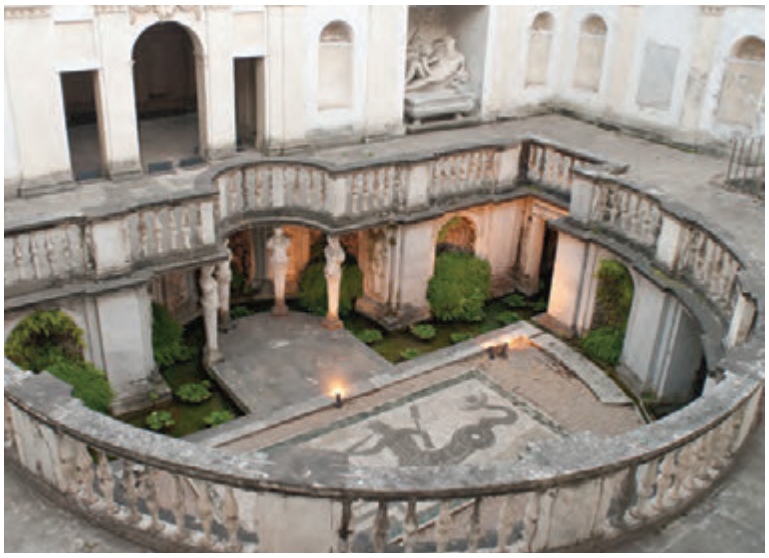
MIDDLE ROW
left photo
The *nymphaeum,* designed by Bartolomeo Ammannati.

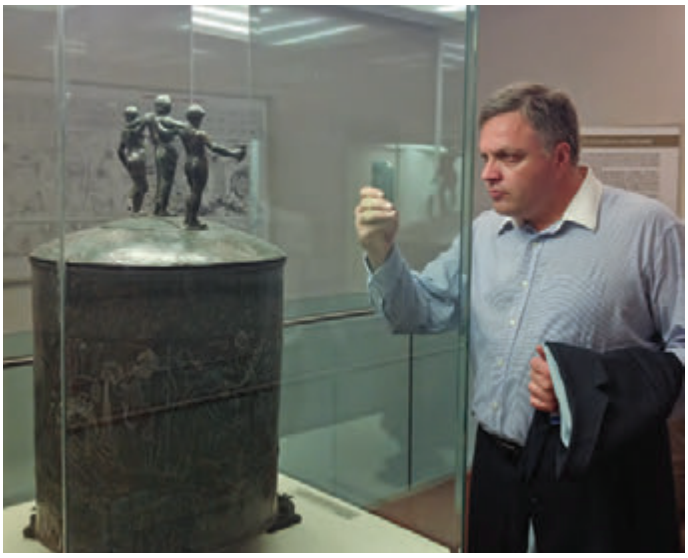
right photo
Georgian Vice Prime Minister Giorgi Baramidze with the *Cista Ficoroni,* an incised metal cylinder from the 4th century BC. *Cistaes* were funerary objects that accompanied the deceased into the next world.

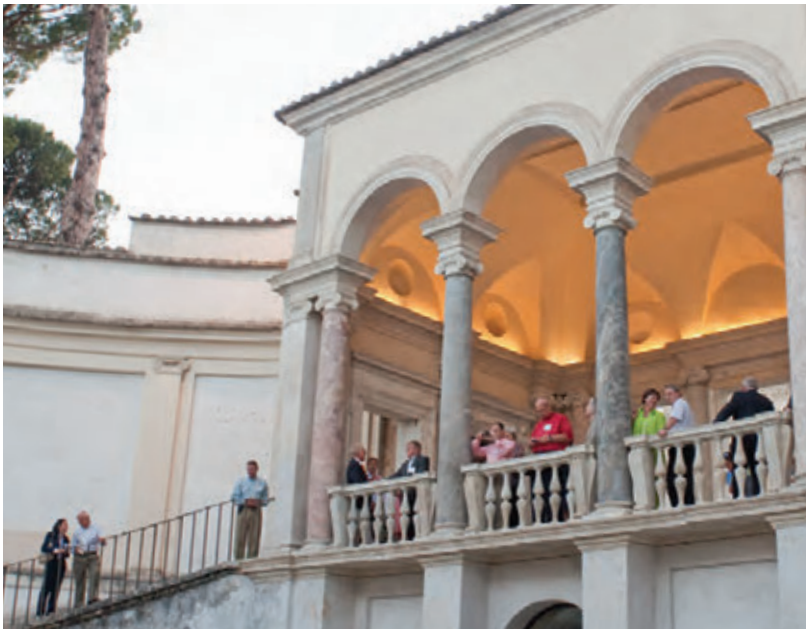
BOTTOM ROW
left photo, from left to right
Colonel Michael B. Warlick, AFCEA International, and Mrs. Diane Warlick;
Mrs. Maria Schneider and Mr. Kent Schneider, President and CEO, AFCEA International.

right photo
Villa Giulia's loggia overlooking the *nymphaeum.*









TOP ROW
left photo
Visit of Villa Giulia's gardens with Mr. Sandro Pellegrini, Rome Travels guide.

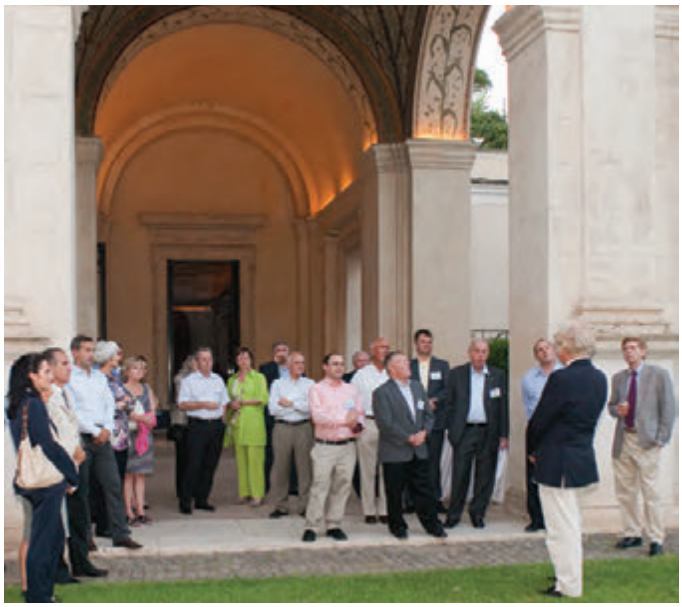
right photo, from left to right
Ms. Anne D. Baylon, Co-Director, Center for Strategic Decision Research;
Colonel Alessandro Carile, Centro Militare di Studi Strategici (CeMISS);
Ms. Caroline Baylon, Vice President, Center for Strategic Decision Research.

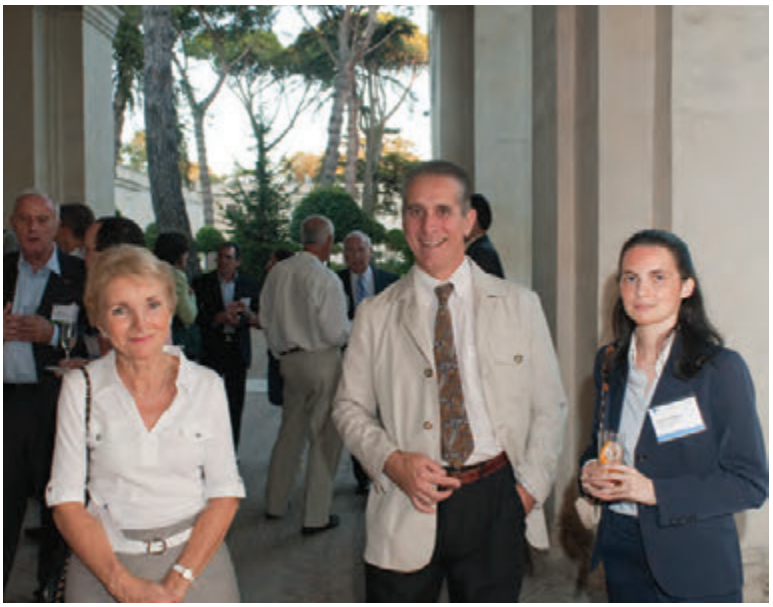
MIDDLE ROW
left photo
The famous Etruscan terracotta funerary monument called the Sarcophagus of the Spouses, a bride and groom reclining at a banquet in the afterlife.

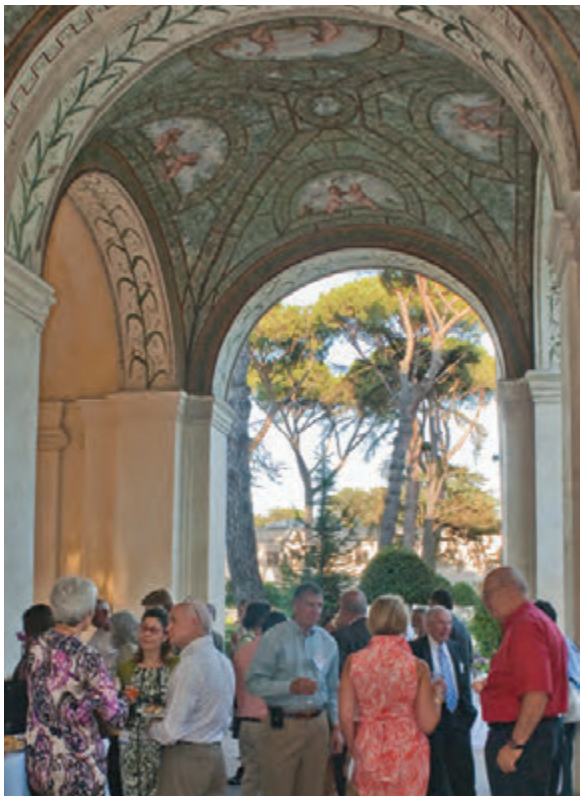
right photo
Ambassador Mariot Leslie in front of the ancient Etruscan jewelry display.

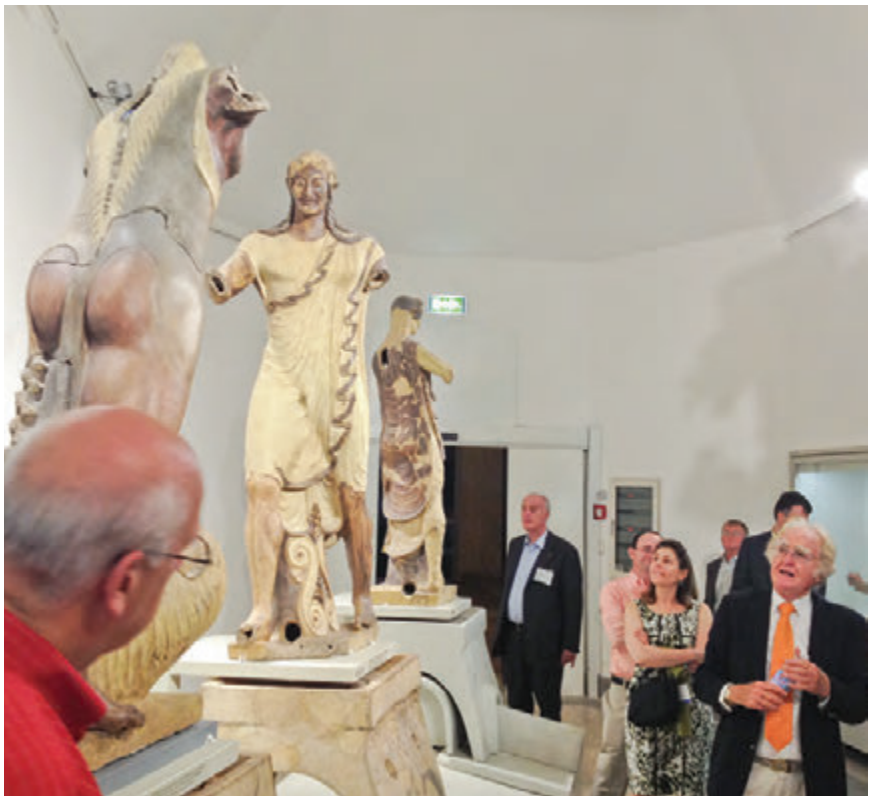
BOTTOM ROW
left photo
The large hemispheric portico of Villa Giulia adorned with frescoes by Pietro Venale depicting rare birds and chubby baby boys (putti).

right photo
Sandro Pellegrini comments on Etruscan art.









TOP ROW
left photo
Opening Session of the 29th International Workshop.

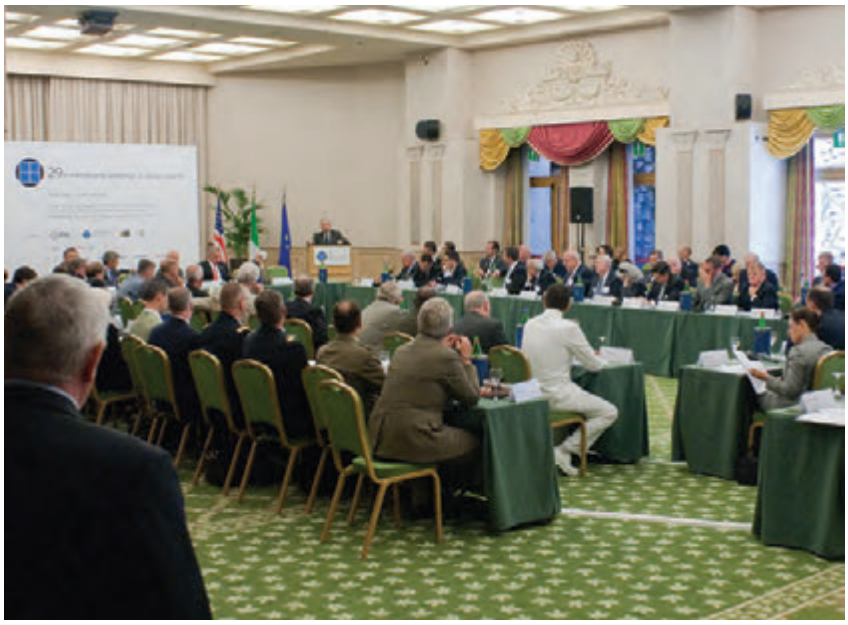
right photo
Admiral Giampaolo Di Paola, Minister of Defense of Italy and
Patron of the 29th International Workshop, during the Opening Session.

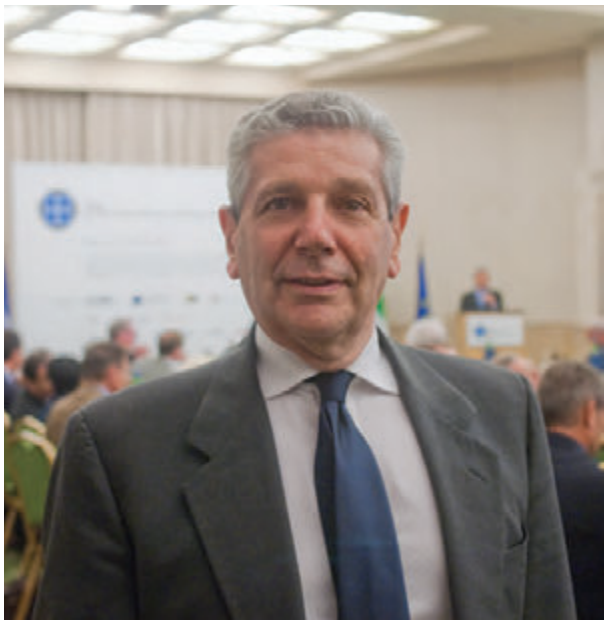
MIDDLE ROW
from left to right
Mr. Giuseppe Orsi, CEO, Finmeccanica;
Ambassador Stefano Stefanini, Diplomatic Advisor to the President of Italy;
Minister Giampaolo Di Paola;
Workshop Chairman and Founder Dr. Roger Weissinger-Baylon;
Ambassador David Thorne, U.S. Ambassador to Italy;
General Biagio Abrate, Chief of Defense General Staff of Italy and workshop Honorary Chairman.

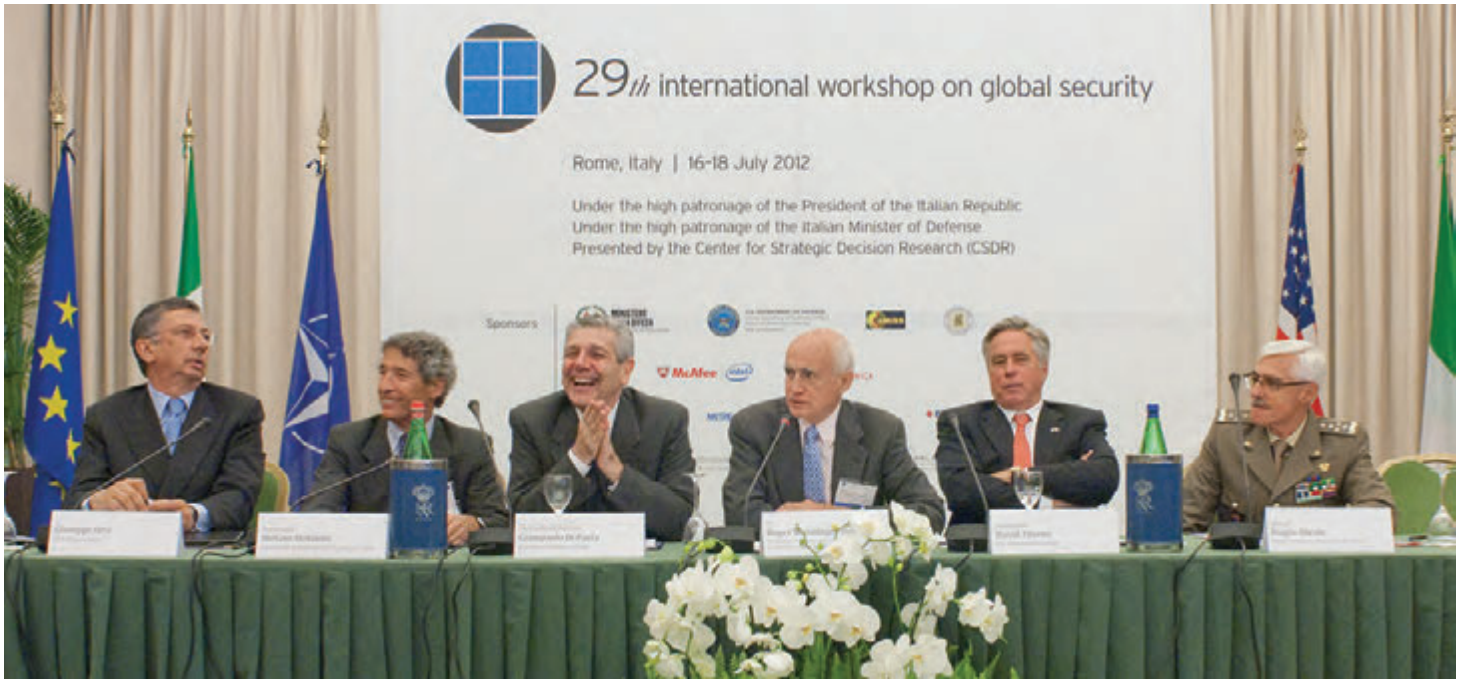
BOTTOM ROW
left photo, from left to right
Defense Minister Giampaolo Di Paola;
Workshop Chairman and Founder Dr. Roger Weissinger-Baylon;
General Biagio Abrate, Chief of Defense General Staff of Italy.

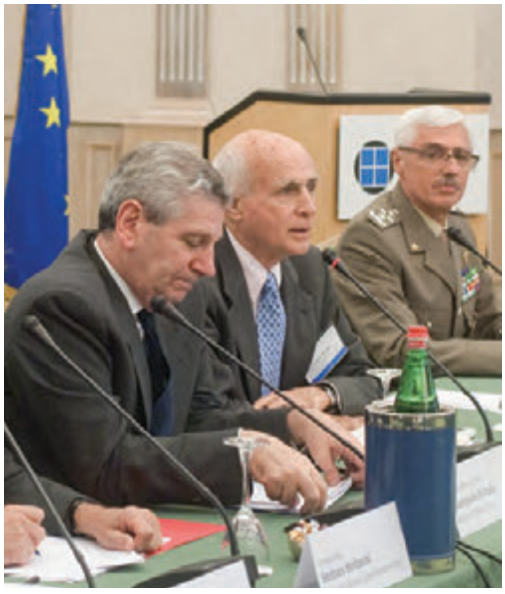
middle photo
Ambassador David Thorne, U.S. Ambassador to Italy *(l)*
and Mr. Giuseppe Orsi, CEO, Finmeccanica *(r).*

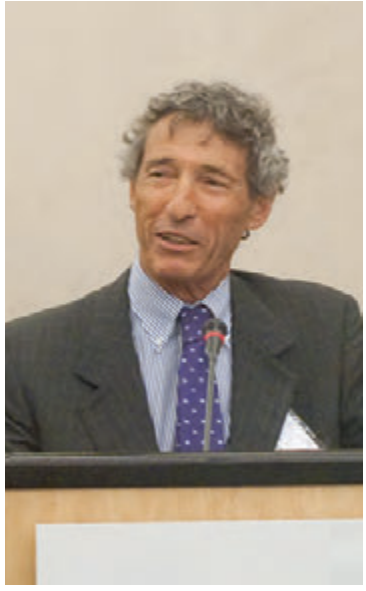
right photo
Ambassador Stefano Stefanini, Diplomatic Advisor to the President of Italy.






29/// international workshop on global security
Rome, Italy | 16-18 July 2012
Under the high patronage of the President of the Italian Republic
Under the high patronage of the Italian Minister of Defense
Presented by the Center for Strategic Decision Research (CSDR)
Sponsors





TOP ROW
left photo
Rear Admiral Nicola De Felice, Director, CID, Italian Defense General Staff *(l)*
and Mr. Jiang Zhenxi, Senior Research Fellow, China Institute for International Strategic Studies *(r).*

right photo, from left to right
Ms. Melissa Hathaway, former U.S. Cyber Security Coordinator;
Mr. Donald Proctor, Senior Vice President, Office of the CEO, Cisco;
Mr. Terry Morgan, Principal, Global Thought.

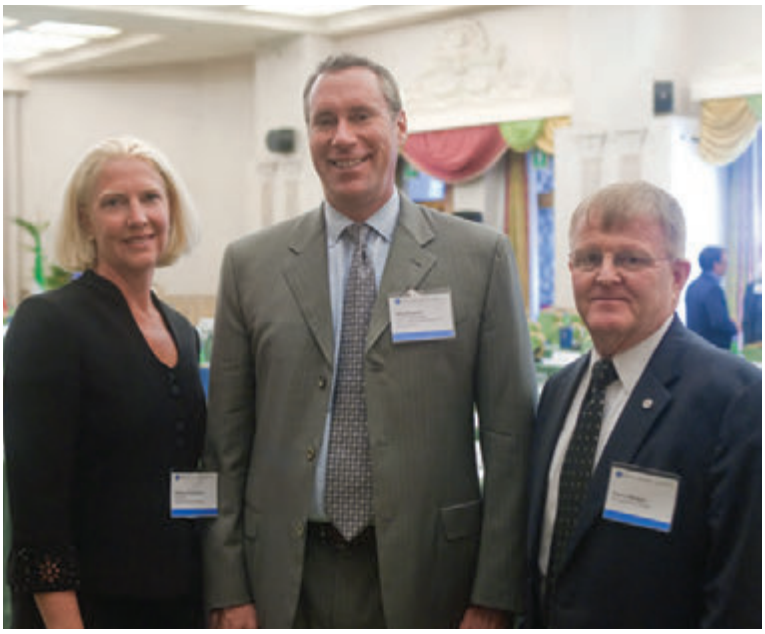
MIDDLE ROW
left photo
Ambassador Bogusław Winid, Undersecretary of State, Polish Foreign Ministry *(l)*
and Ambassador Mariot Leslie, United Kingdom Permanent Representative to NATO *(r).*

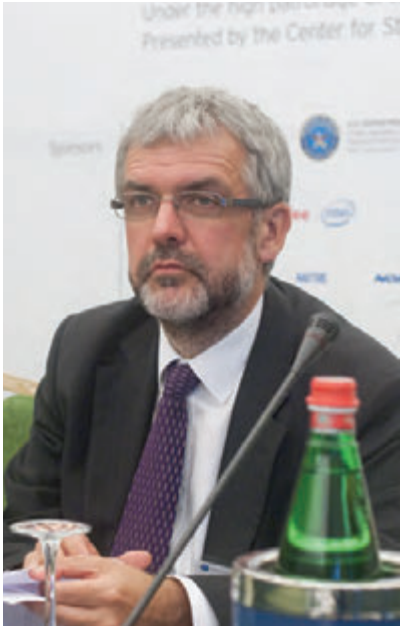
middle photo
Mr. Jiří Schneider, First Deputy Minister of Foreign Affairs of the Czech Republic.

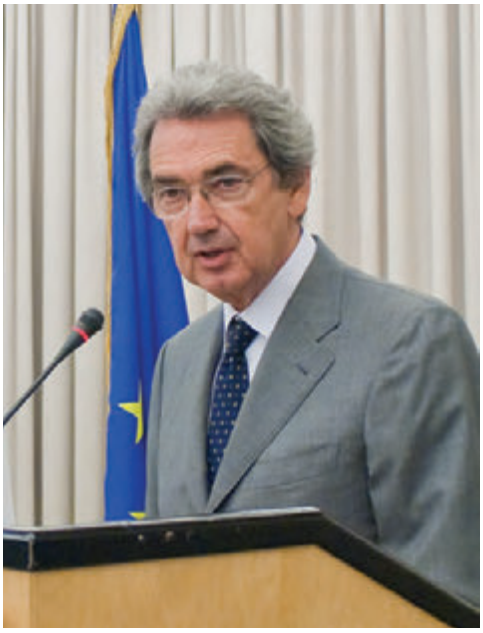
right photo
Mr. Franco Bernabè, Chairman and CEO, Telecom Italia.

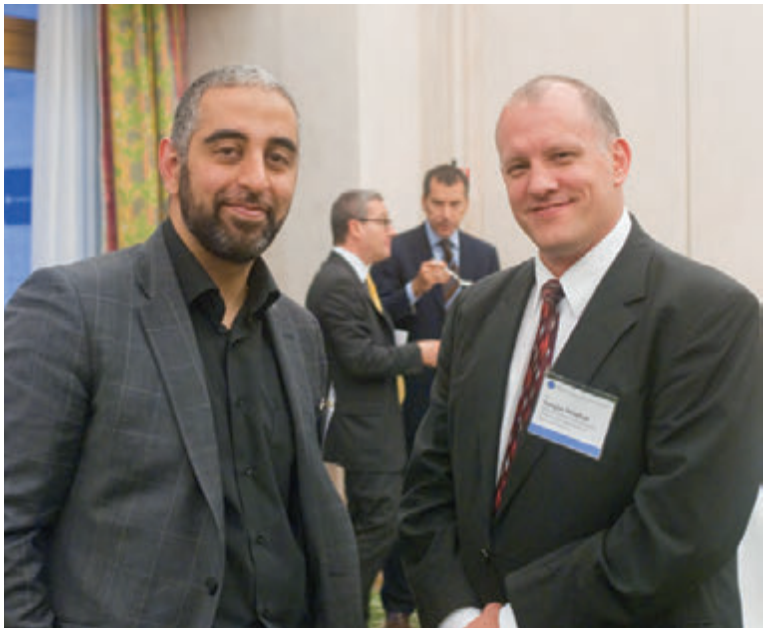
BOTTOM ROW
left photo
Mr. Raj Samani, Chief Technical Officer (CTO) EMEA, McAfee | Intel *(l)*
and Dr. Douglas Maughan, U.S. Department of Homeland Security *(r).*

right photo
His Excellency Dr. Artis Pabriks, Defense Minister of Latvia.




Presented by the Center for





TOP ROW
left photo, from left to right
Mr. Sergio Attilio Jesi, Vice President, ELT | Elettronica;
Ambassador Stefano Stefanini, Diplomatic Advisor to the President of Italy;
Ambassador Bogusław Winid, Undersecretary of State, Polish Foreign Ministry;
Ambassador Haydar Berk, Permanent Representative of Turkey to NATO;
Ambassador Rolf Nikel, Federal Government Commissioner, German Federal Foreign Office.

right photo
Mr. John Horridge, AeroSpace Defence Security (ADS).

SECOND ROW
left photo, from left to right
Ambassador Michel Foucher, Institut des hautes études de défense nationale (IHEDN) and his wife, Ms. Velga Lukaža;
Ingénieur Général Robert Ranquet, Institut des hautes études de défense nationale (IHEDN);
Ms. Anne D. Baylon, Co-Director, Center for Strategic Decision Research.

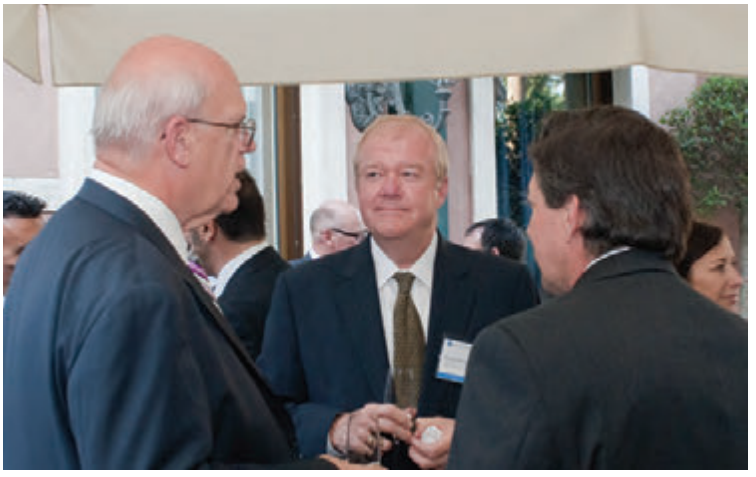
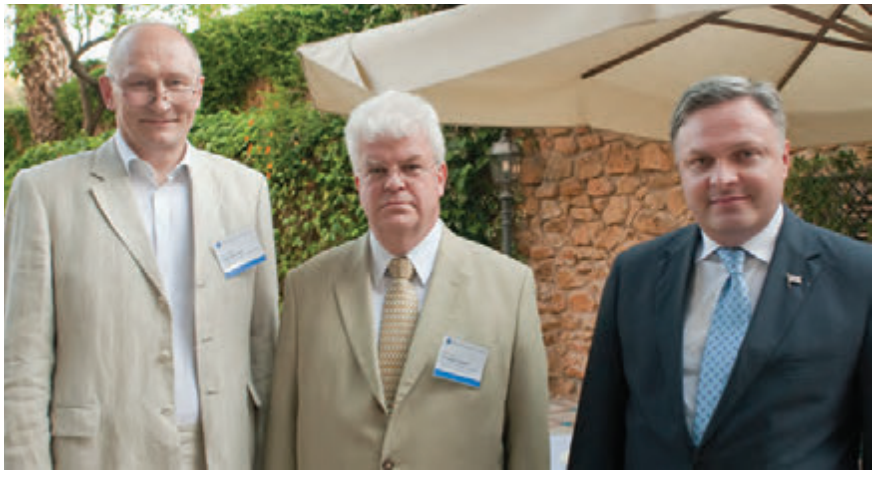
right photo, from left to right
Mr. Kent Schneider, President and CEO, AFCEA International;
Mr. David Swindle, Executive President, URS Federal Services;
Mr. Raymond Haller, Senior Vice President, The MITRE Corporation.

THIRD ROW
left photo, from left to right
His Excellency Jaak Aaviksoo, Minister of Education and Research of Estonia;
Ambassador Vladimir Chizhov, Russian Permanent Representative to the EU;
His Excellency Giorgi Baramidze, Georgian Vice Prime Minister.

right photo
Ambassador Haydar Berk, Permanent Representative of Turkey to NATO *(l)*
and His Excellency Dr. Zlatko Lagumdžija, Foreign Minister of Bosnia and Herzegovina *(r).*

BOTTOM ROW
Senator Francesco Rutelli gives a Keynote Dinner Address.



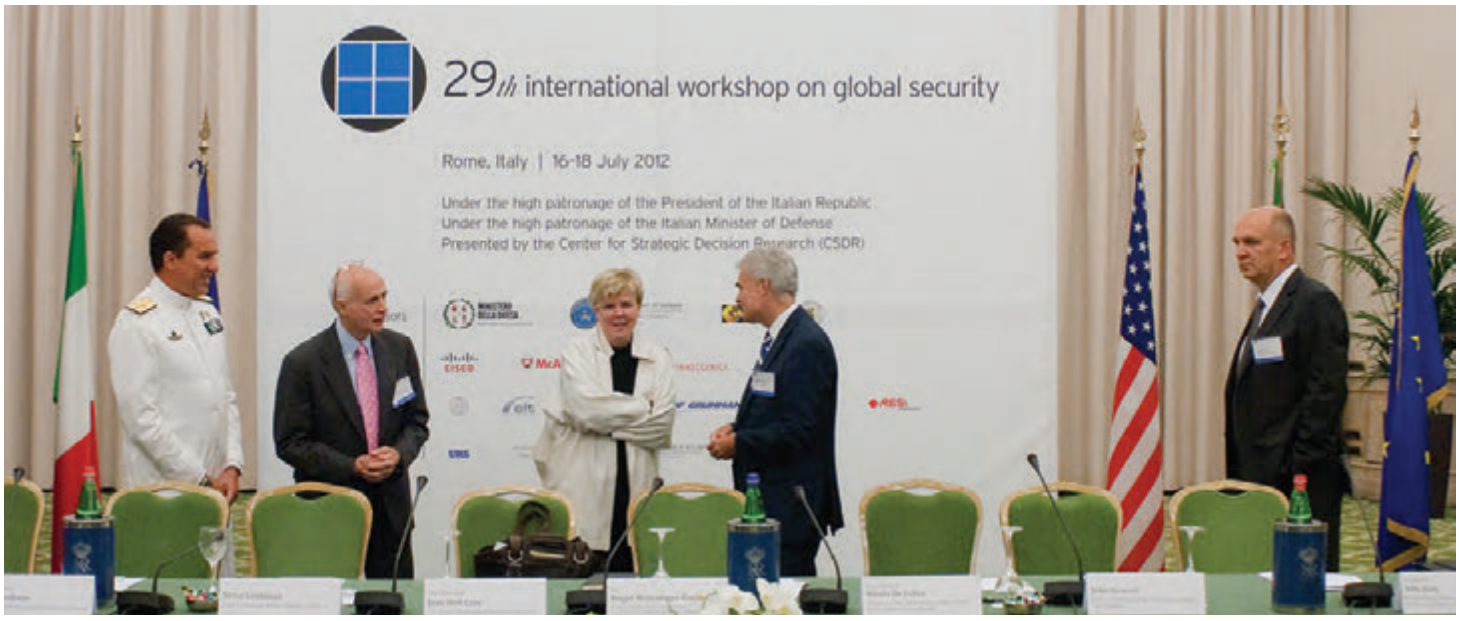
TOP ROW
from left to right
Rear Admiral Nicola De Felice, Director, Centro Innovazione Difesa (CID);
Workshop Chairman and Founder Dr. Roger Weissinger-Baylon;
The Honorable Jane Holl Lute, U.S. Deputy Secretary of Homeland Security;
Polish Undersecretary Dr. Zbigniew Włosowicz, Ministry of Defense of Poland;
Lieutenant General Arto Räty, Permanent Secretary, Finnish Defense Ministry.

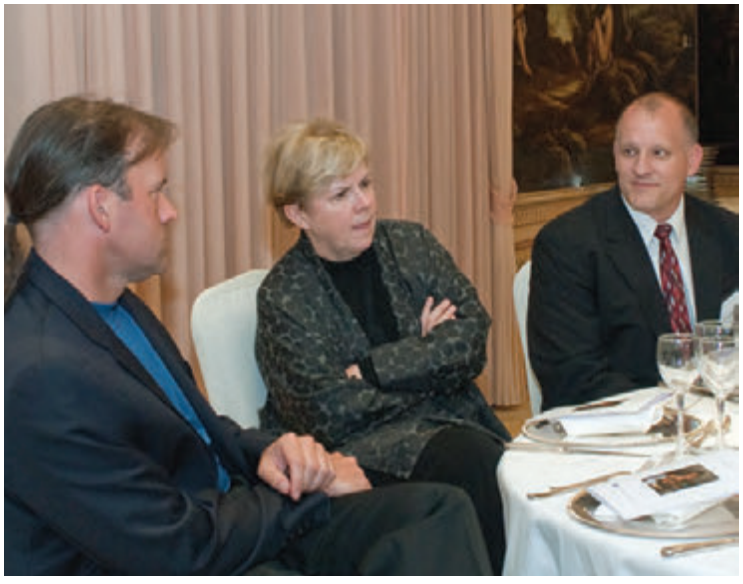
MIDDLE ROW
left photo, from left to right
Mr. John Stewart, Senior Vice President and Chief Security Officer, Cisco Systems;
The Honorable Jane Holl Lute, U.S. Deputy Secretary of Homeland Security;
Dr. Douglas Maughan, U.S. Department of Homeland Security.

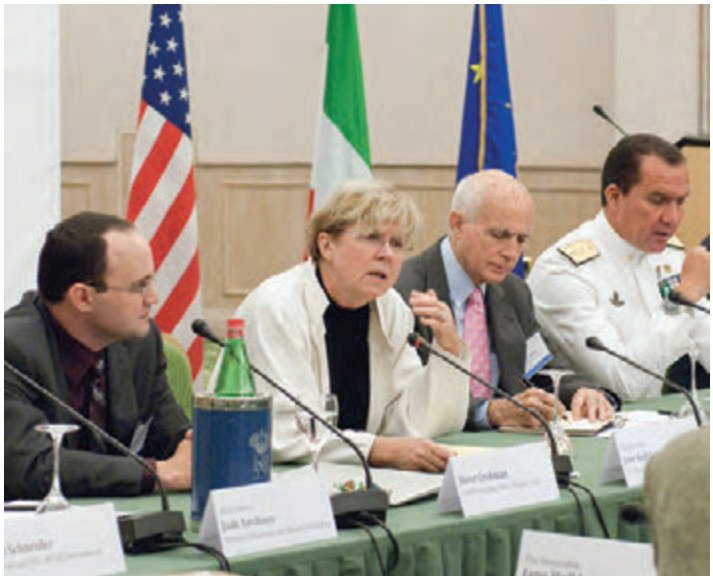
right photo, from left to right
Mr. Steve Grobman, Chief Technology Officer, McAfee | Intel Technologies;
The Honorable Jane Holl Lute, U.S. Deputy Secretary of Homeland Security;
Workshop Chairman and Founder Dr. Roger Weissinger-Baylon;
Rear Admiral Nicola De Felice, Director, Centro Innovazione Difesa (CID).

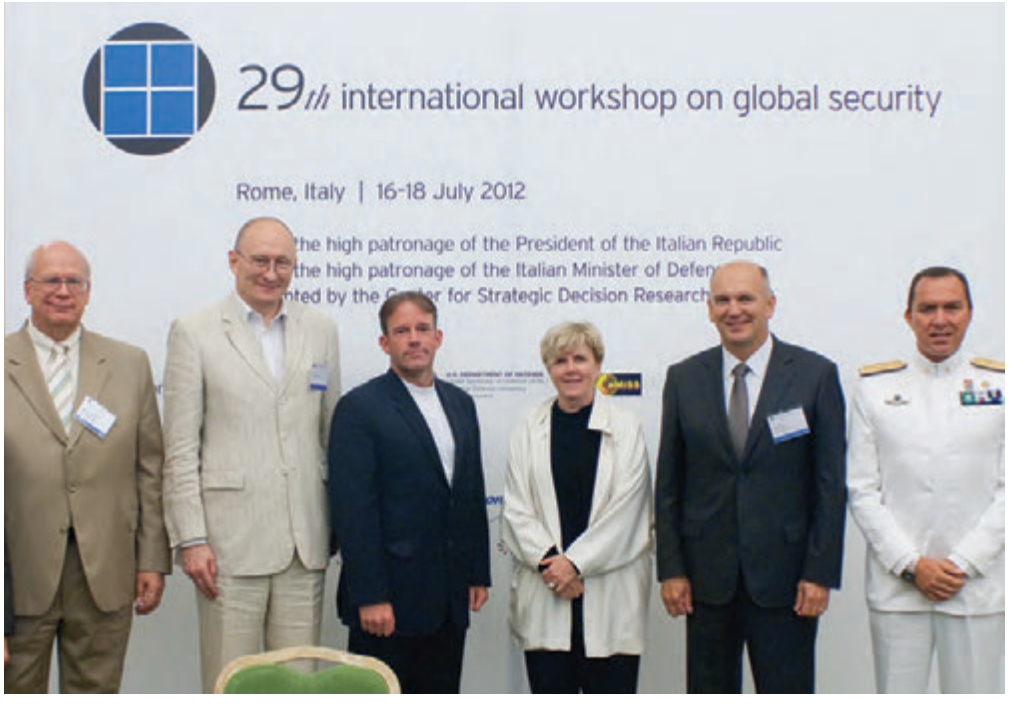
BOTTOM ROW
left photo, from left to right
Mr. Kent Schneider, President and CEO, AFCEA International;
His Excellency Jaak Aaviksoo, Minister of Education and Research of Estonia;
Mr. John Stewart, Senior Vice President and Chief Security Officer, Cisco Systems;
The Honorable Jane Holl Lute, U.S. Deputy Secretary of Homeland Security;
Lieutenant General Arto Räty, Permanent Secretary, Finnish Defense Ministry;
Rear Admiral Nicola De Felice, Director, Centro Innovazione Difesa (CID).

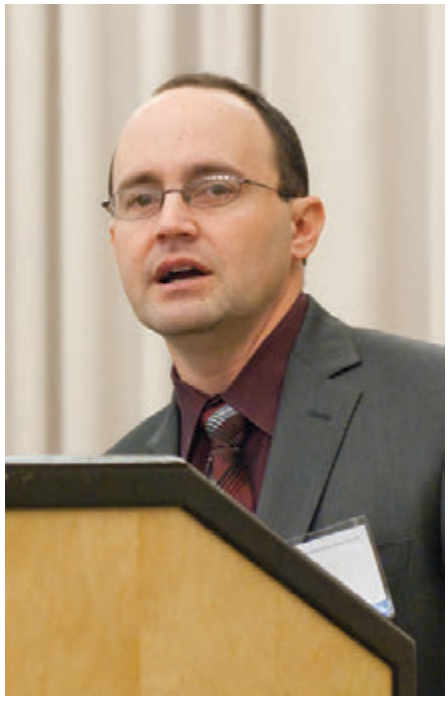
right photo
Mr. Steve Grobman, Chief Technology Officer, McAfee | Intel Technologies.


29th international workshop on global security
Rome, Italy | 16-18 July 2012
Under the high patronage of the President of the Italian Republic
Under the high patronage of the Italian Minister of Defense
Presented by the Center for Strategic Decision Research (CSDR)






29th international workshop on global security
Rome, Italy | 16-18 July 2012



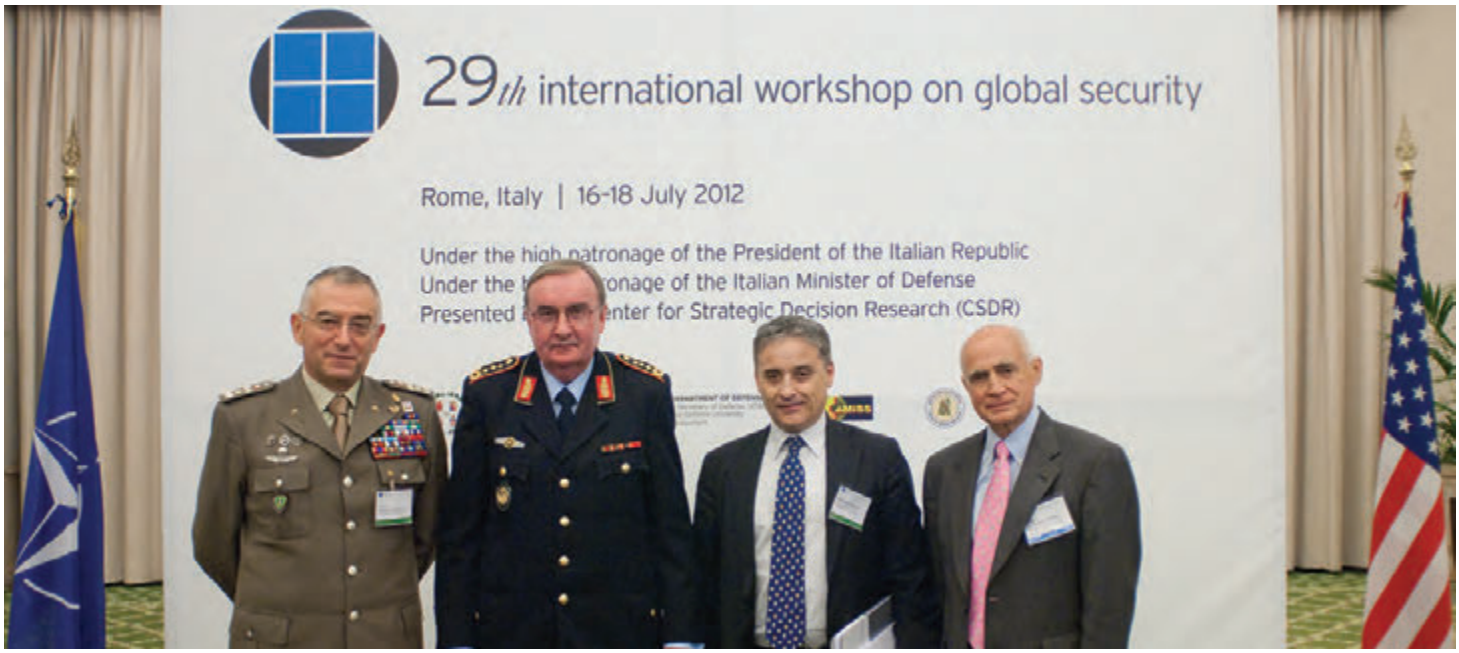
TOP ROW
from left to right
Lieutenant General Claudio Graziano, Chief of General Staff, Italian Army;
General Manfred Lange, Chief of Staff, SHAPE;
Ambassador Maurizio Massari, Italian Special Envoy, Mediterranean & Middle East;
Workshop Chairman and Founder Dr. Roger Weissinger-Baylon.

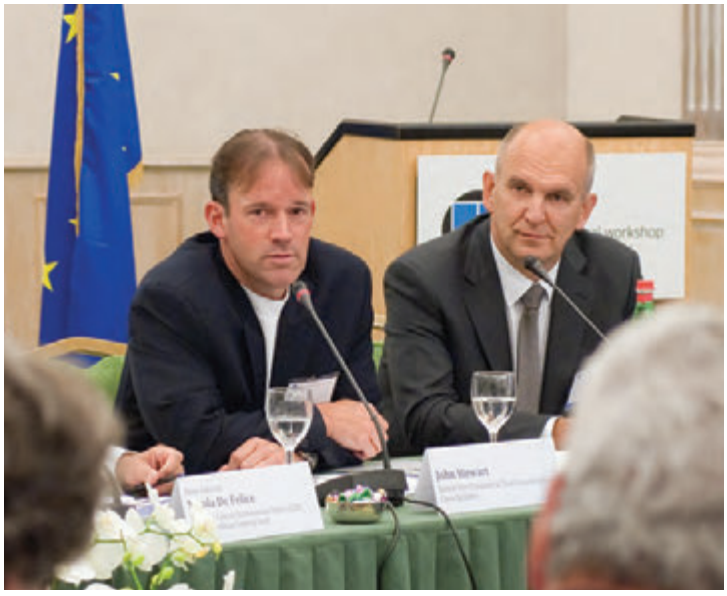
MIDDLE ROW
left photo
Mr. John Stewart, Senior Vice President and Chief Security Officer, Cisco Systems *(l)*
and Lieutenant General Arto Räty, Permanent Secretary, Finnish Defense Ministry *(r).*

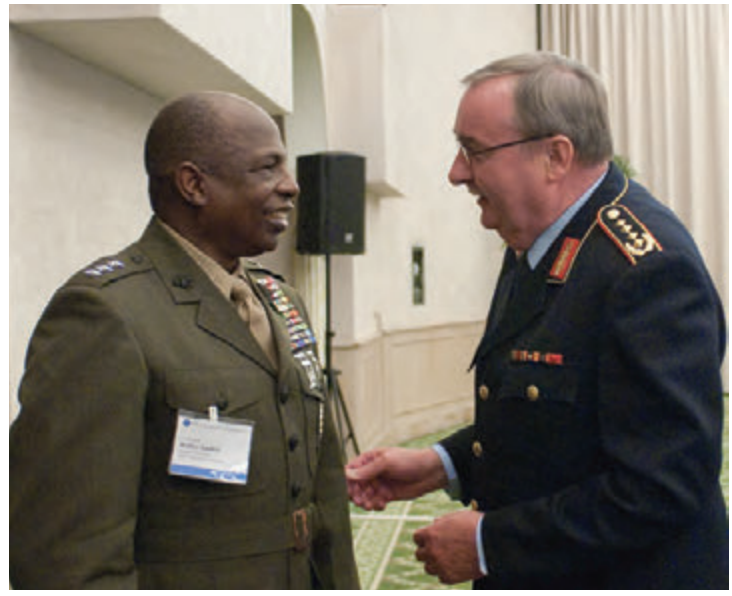
right photo
Lieutenant General Walter Gaskin, Deputy Chairman, NATO Military Committee *(l)*
and General Manfred Lange, Chief of Staff, SHAPE *(r).*

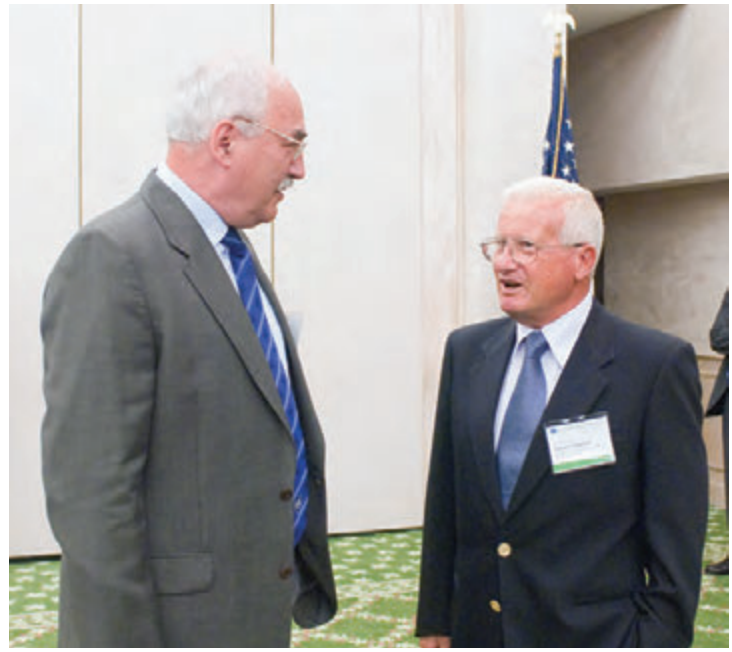
BOTTOM ROW
left photo
Ms. Neyla Arnas, Senior Research Fellow, National Defense University *(l)*
and Ms. Harriet Goldman, Executive Director of Cyber Mission Assurance, MITRE *(r).*

right photo
General Mieczysław Cieniuch, Chief of the General Staff, Armed Forces of Poland *(l)*
and Admiral Luciano Zappata (Ret.), Former NATO Deputy Supreme Allied Commander *(r).*


29th international workshop on global security
Rome, Italy | 16-18 July 2012







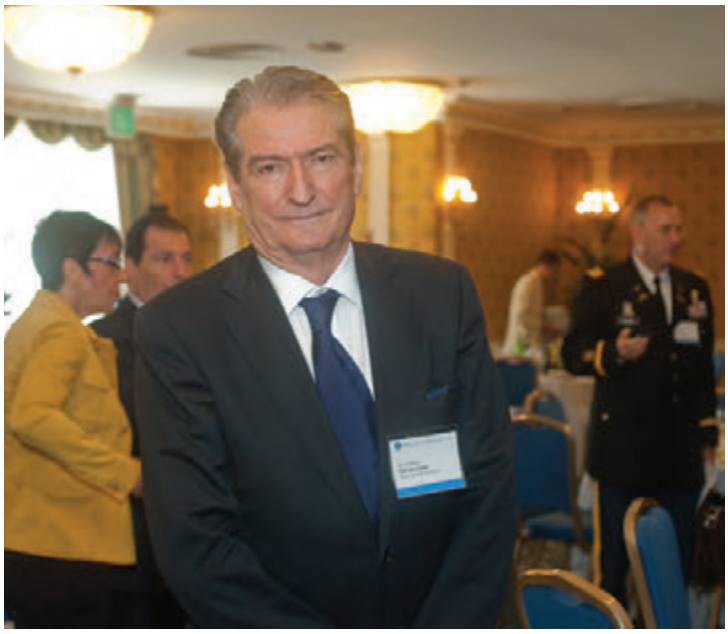
TOP ROW
left photo
His Excellency Sali Berisha, Prime Minister of Albania.

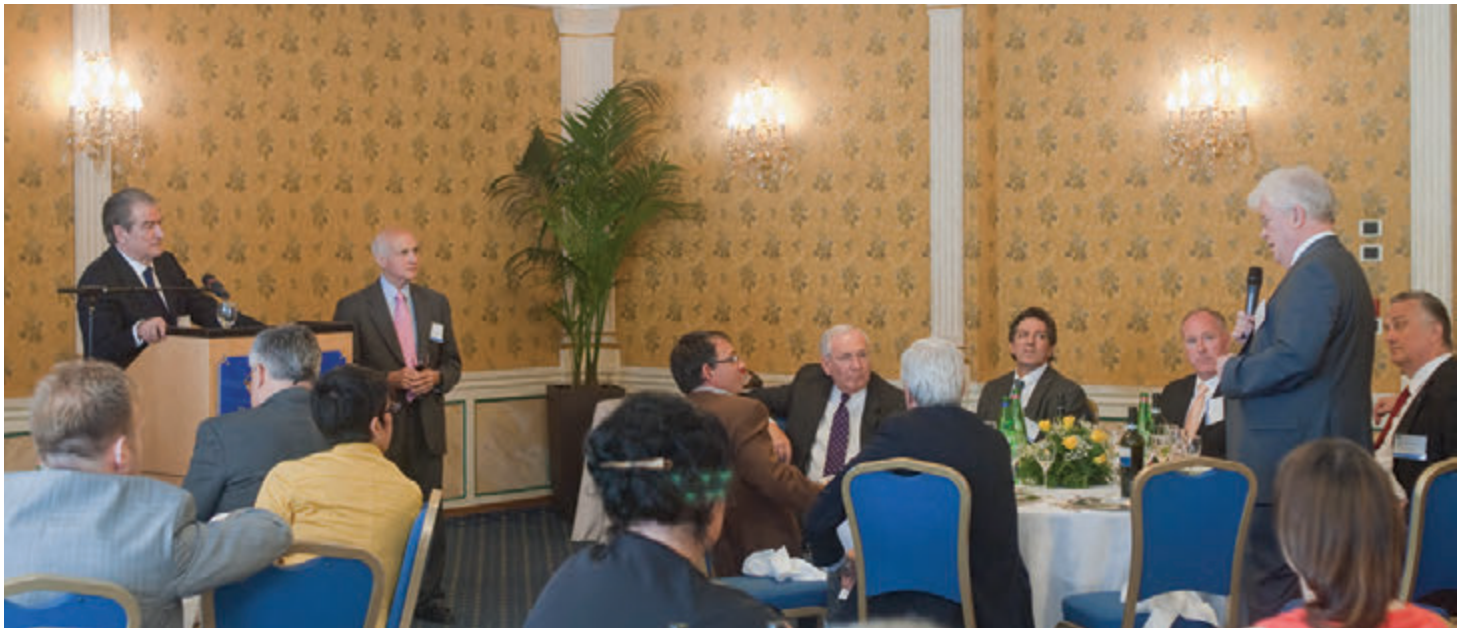
right photo
Albanian Prime Minister Sali Berisha presents the Keynote Luncheon Address.

MIDDLE ROW
from right to left
Russian Ambassador Vladimir Chizhov and Prime Minister Sali Berisha.

BOTTOM ROW
left photo
Mr. Ashton Peery, CEO, Renesys *(l)*
and Mr. James Cowie, Chief Technical Officer, (CTO), Renesys *(r).*

right photo, from left to right
Workshop Chairman and Founder Dr. Roger Weissinger-Baylon;
Ambassador Artur Kuko, Permanent Representative of Albania to NATO;
Mr. Glori Husi, Advisor to the Prime Minister of Albania.





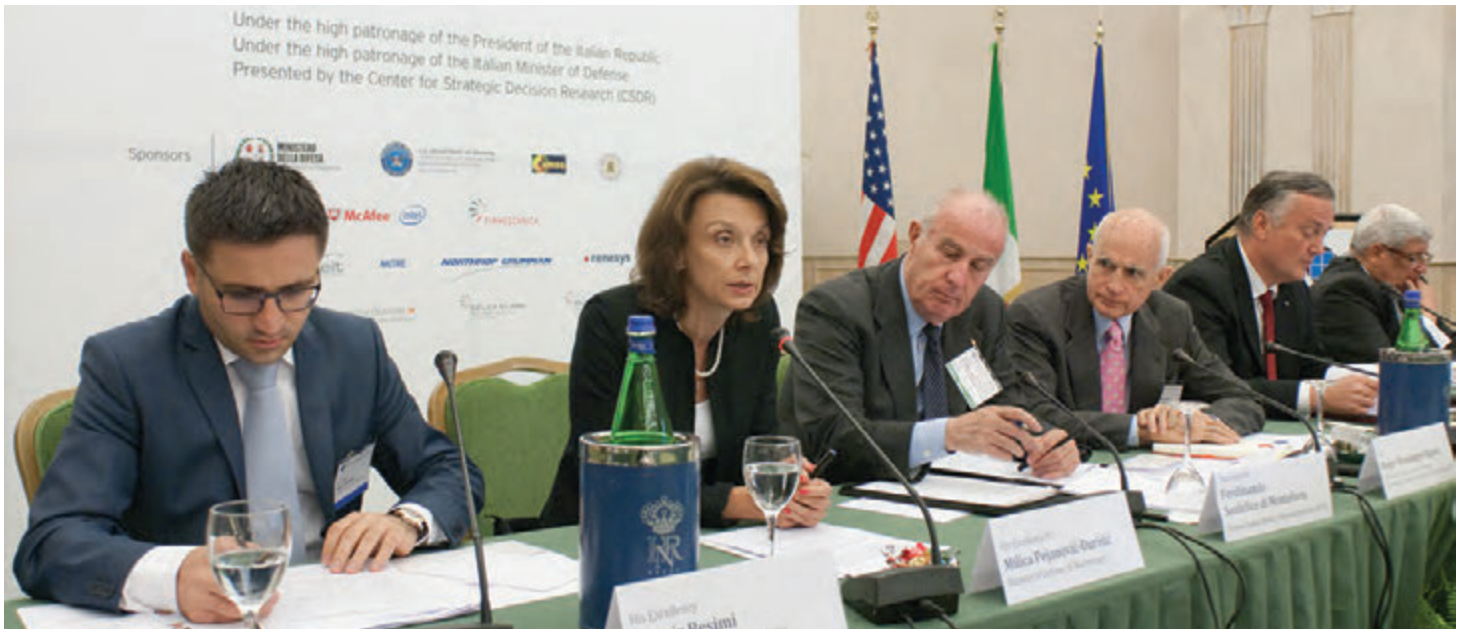
TOP ROW
from left to right
His Excellency Fatmir Besimi, Minister of Defense of Macedonia;
Her Excellency Professor Milica Pejanović-Durišić, PhD, Minister of Defense of Montenegro;
VADM Ferdinando Sanfelice di Monteforte, Former Italian Military Representative to NATO;
His Excellency Dr. Zlatko Lagumdžija, Foreign Minister of Bosnia and Herzegovina;
His Excellency Anyu Anguelov, Minister of Defense of Bulgaria.

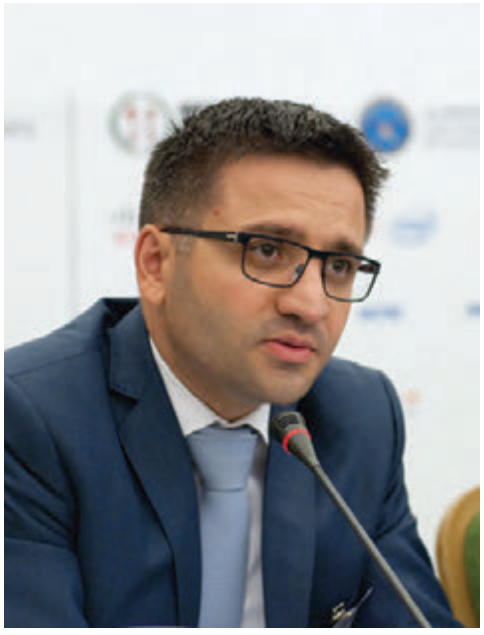
MIDDLE ROW
left photo
His Excellency Fatmir Besimi, Minister of Defense of Macedonia.

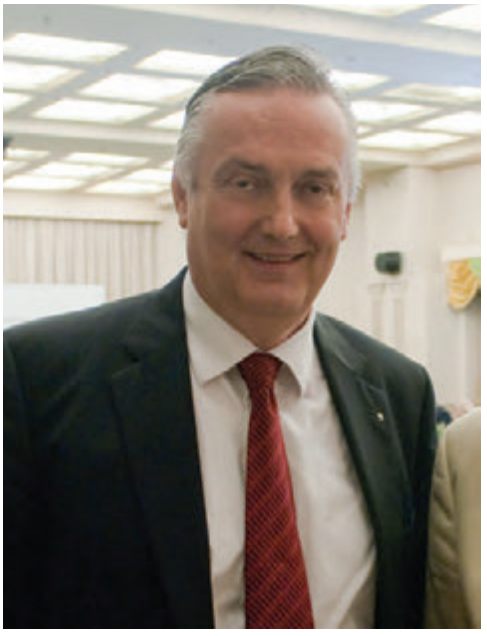
middle photo
His Excellency Dr. Zlatko Lagumdžija, Foreign Minister of Bosnia and Herzegovina.

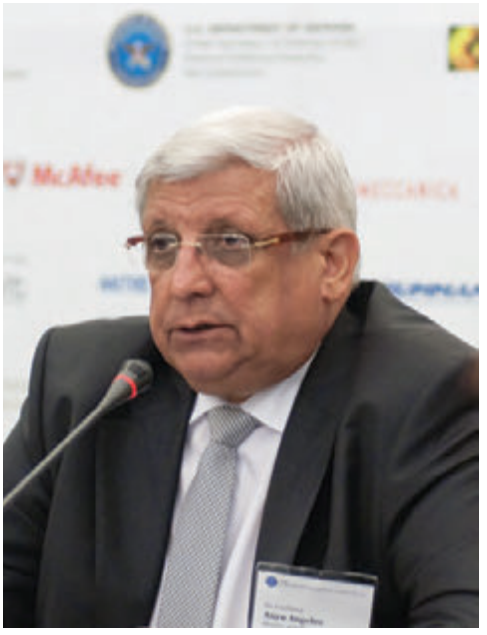
right photo
His Excellency Anyu Anguelov, Minister of Defense of Bulgaria.

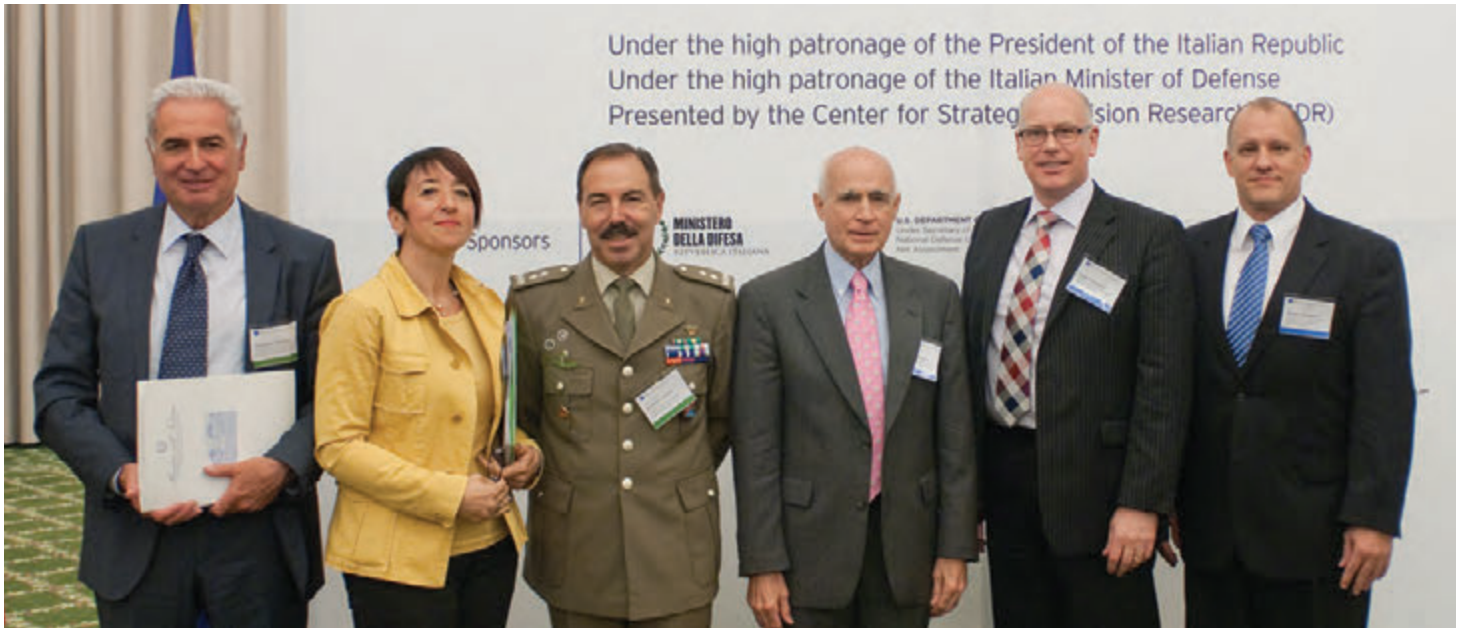
BOTTOM ROW
from left to right
Mr. Domenico Vulpiani, Director General, State Police, Coordinator for Information Security and Protection of Critical Infrastructure;
Ing. Daniela Pistoia, Vice President, ELT | Elettronica;
Major General Salvatore Farina, Italian Defense General Staff;
Workshop Chairman and Founder Dr. Roger Weissinger-Baylon;
Mr. David Pollington, Director of International Security Relations, Microsoft;
Dr. Douglas Maughan, U.S. Department of Homeland Security.


Under the high patronage of the President of the Italian Republic
Under the high patronage of the Italian Minister of Defense
Presented by the Center for Strategic Decision Research (CSDR)
Sponsors








Under the high patronage of the President of the Italian Republic
Under the high patronage of the Italian Minister of Defense
Sponsors
MINISTERO DELLA DIFESA

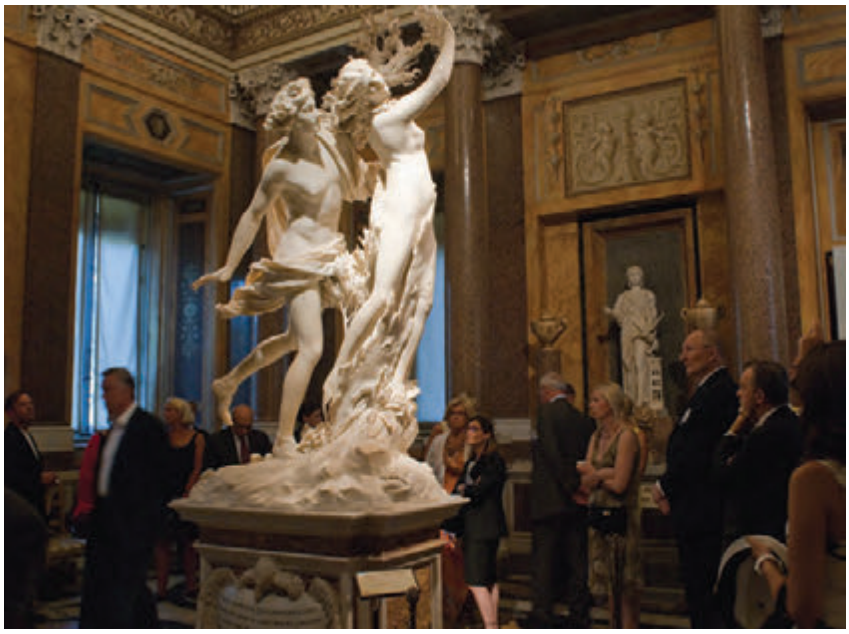
TOP ROW
left photo
Apollo and Daphne, Gian Lorenzo Bernini's sculpture depicting Daphne's transformation into a graceful tree.

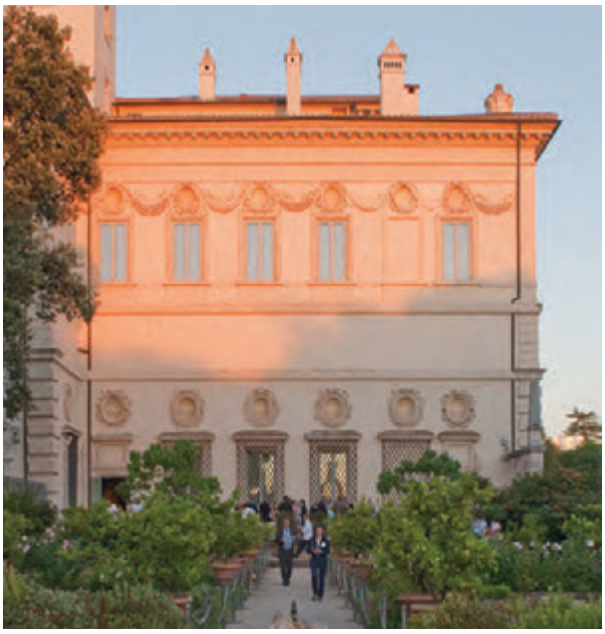
right photo
A side view of Galleria Borghese and its gardens.

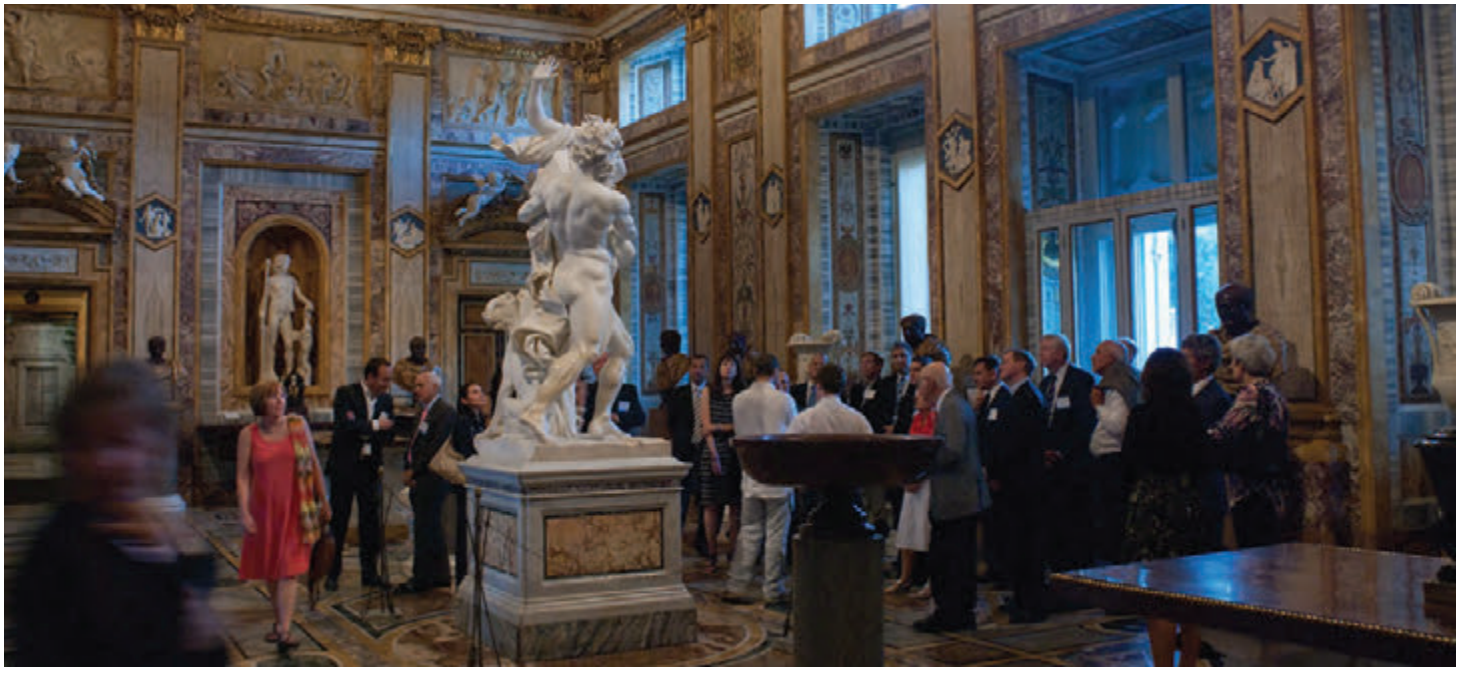
MIDDLE ROW
Bernini's marble sculpture of Pluto and Proserpina, which shows the abduction of Proserpina, daughter of Ceres, by Pluto, the god of the underworld.

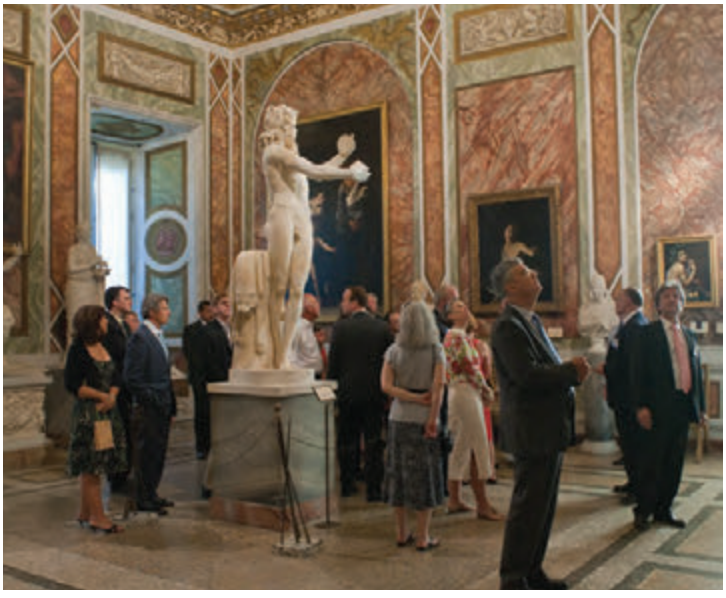
BOTTOM ROW
left photo
Reception and buffet dinner in the "Secret Garden" of Cardinal Scipione Borghese.

right photo
Some masterpieces of the Galleria Borghese collections.









TOP ROW
from left to right
Mr. Marco Morucci, Rome Lab Leader, IBM;
Ms. Harriet Goldman, The MITRE Corporation;
Workshop Chairman and Founder Dr. Roger Weissinger-Baylon;
Mr. Kevin Scheid, NATO Communications and Information Agency;
Rear Admiral Francesco Covella, Italian Ministry of Defense;
Mr. Massimo Piva, Senior Vice President, SELEX Sistemi Integrati;
Lieutenant General Nazzareno Cardinali, Chairman of the Board, SELEX Elsag;
Mr. Jim Moseman, Director, Europe and NATO, Northrop Grumman International.

———————

MIDDLE ROW
left photo, from left to right
Mr. Marco Morucci, Rome Lab Leader, IBM;
Ms. Harriet Goldman, The MITRE Corporation;
Mr. Jim Moseman, Director, Europe and NATO, Northrop Grumman International.

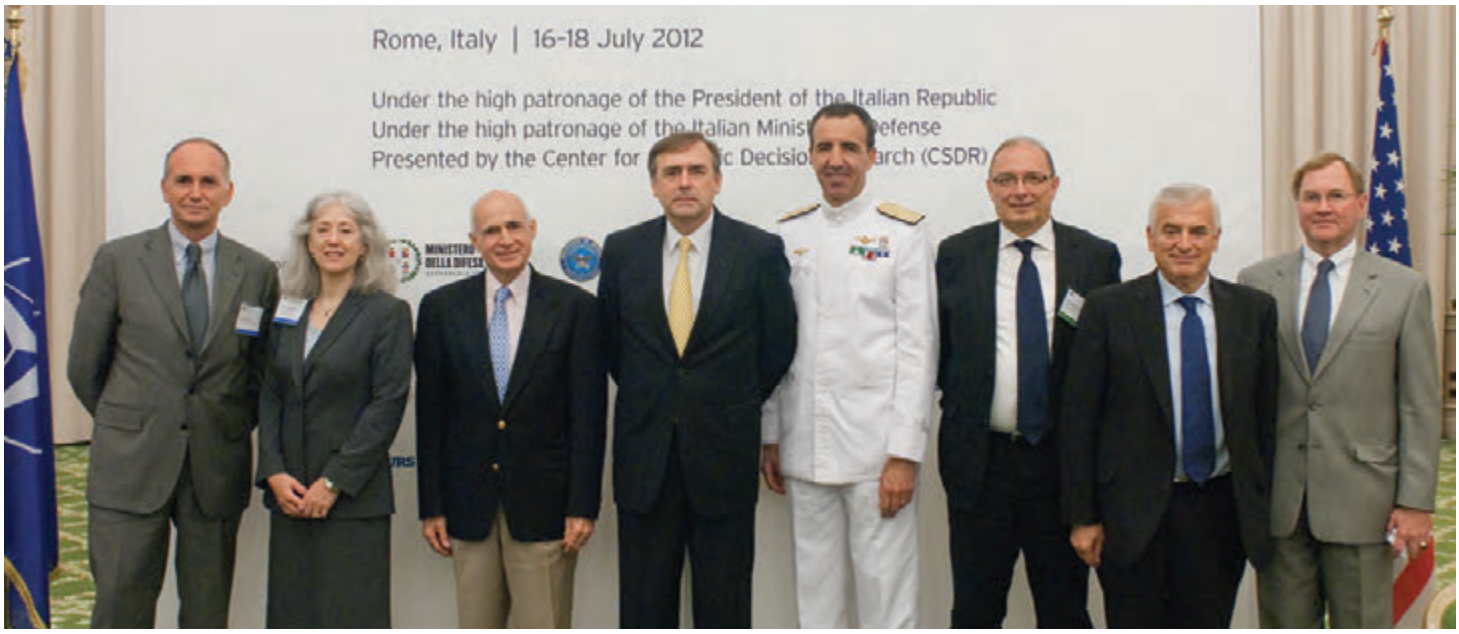
middle photo
Ing. Domitilla Benigni, Chief Operating Officer, Elettronica S.p.A *(l)*
and Ing. Daniela Pistoia, Vice President, ELT | Elettronica *(r).*

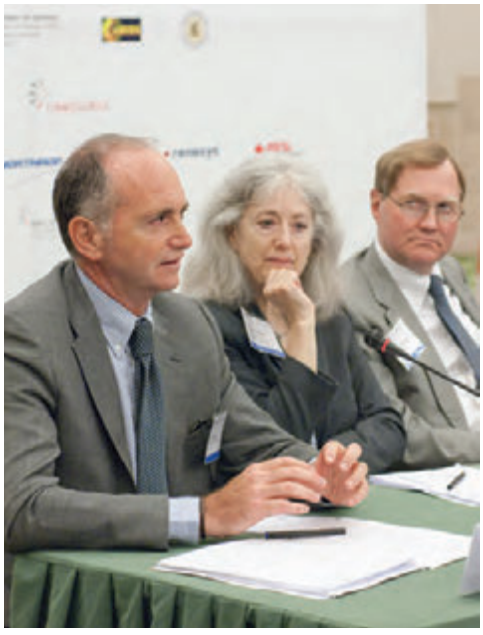
right photo
Admiral Luciano Zappata (Ret.), Former NATO Deputy Supreme Allied Commander *(l)*
and Mr. David Patterson, National Defense Business Institute, University of Tenessee *(r).*

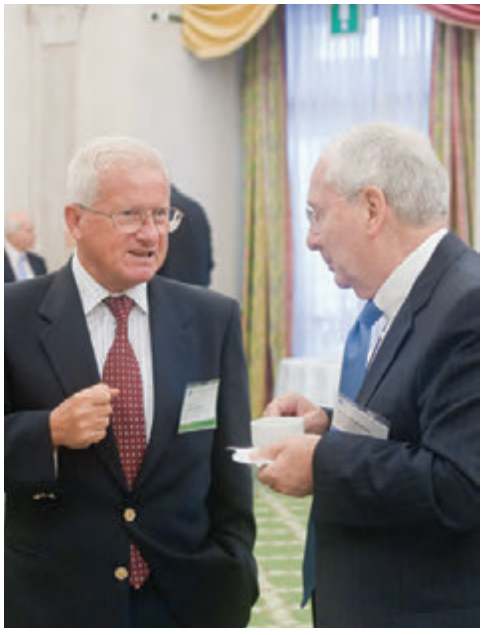
———————

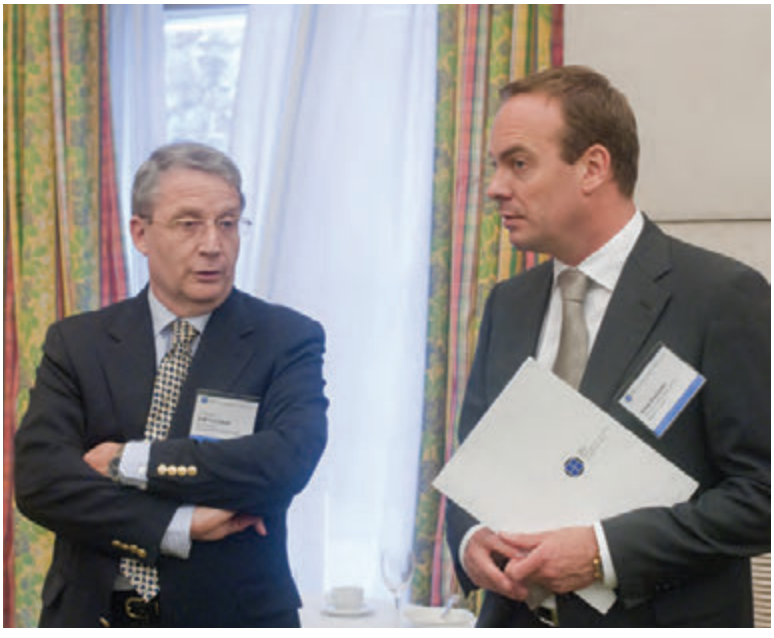
BOTTOM ROW
left photo
Ambassador Michel Foucher, Institut des hautes études de défense nationale *(l)*
and Admiral Jean Betermier, EADS *(r).*

right photo
Lieutenant General Ton van Loon, Commander, 1 (German/Netherlands) Corps *(l)*
and Mr. Rene Roersma, Director, Global Public Sector, McAfee | Intel *(r).*


Rome, Italy | 16-18 July 2012
Under the high patronage of the President of the Italian Republic
Under the high patronage of the Italian Minist
efense
Presented by the Center for
ic Decisio
arch (CSDR)







TOP ROW
left photo
Dr. Luisa Franchina, Director General, Secretariat for Critical Infrastructures, Presidency of the Council of Ministers.

right photo, from left to right
Mr. James Cowie, Chief Technical Officer, Renesys;
Mr. Don Proctor, Senior Vice President, Cisco Systems;
Dr. Jamie Shea, NATO Deputy Assistant Secretary General, Emerging Security Challenges;
Mr. Mauro Collalto, CEO, Resi Group.

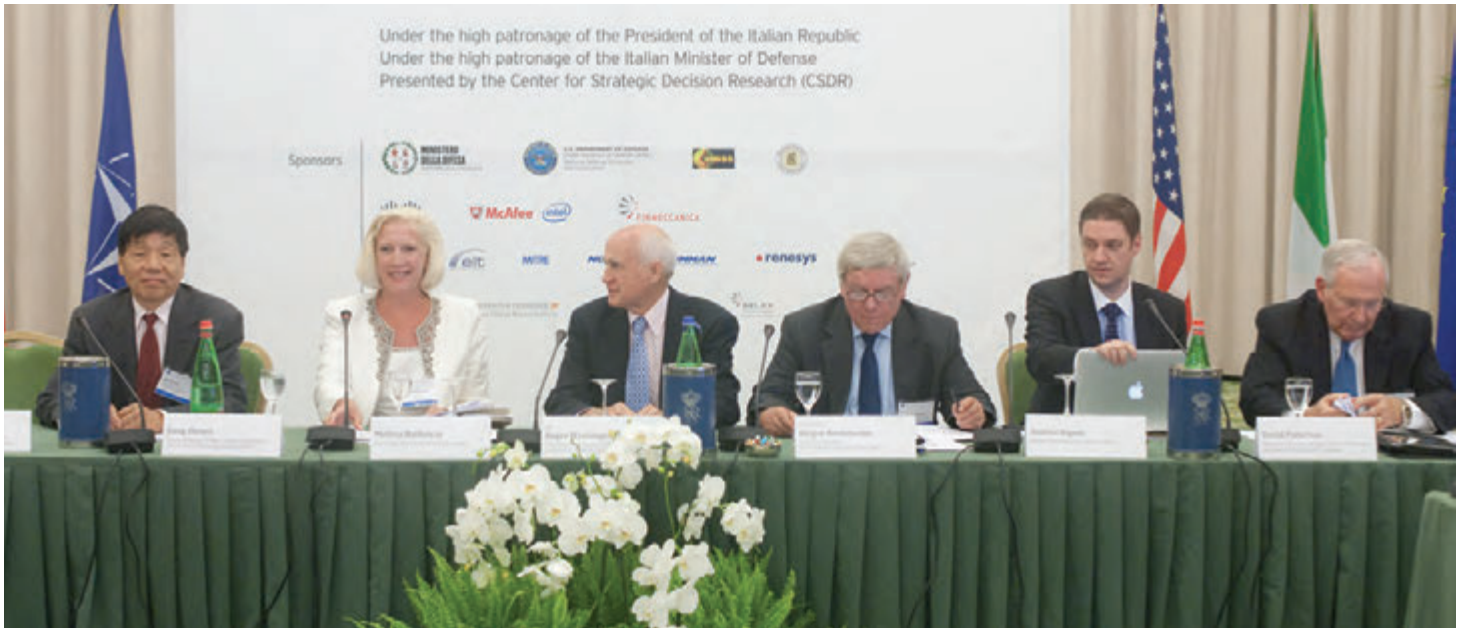
MIDDLE ROW
from left to right
Mr. Jiang Zhenxi, Senior Research Fellow, China Institute for International Strategic Studies;
Ms. Melissa Hathaway, President, Hathaway Global Strategies;
Workshop Chairman and Founder Dr. Roger Weissinger-Baylon;
Lieutenant General Jürgen Bornemann, NATO International Military Staff;
Mr. Andrea Rigoni, Director General, Global Cyber Security Center;
Mr. David Patterson, University of Tennessee.

BOTTOM ROW
left photo
Lieutenant General Frederik Meulman, Netherlands Military Representative to NATO and the EU *(l)*
and Mr. Rene Roersma, Director, Global Public Sector, McAfee | Intel *(r).*

middle photo
Lieutenant General Jürgen Bornemann, NATO International Military Staff *(l)*
and Ms. Melissa Hathaway, President, Hathaway Global Strategies *(r).*

right photo
Mr. David Pollington, Director of International Security Relations, Microsoft *(l)*
and Mr. David Swindle, Executive President, URS Federal Services *(r).*


ne, Italy | 16-18 July 2012


Under the high patronage of the President of the Italian Republic
Under the high patronage of the Italian Minister of Defense
Presented by the Center for Strategic Decision Research (CSDR)
Sponsors
McAfee
intel
renesys


atronage of the President of t
atronage of the Italian Ministe
Center for Strategic Decision

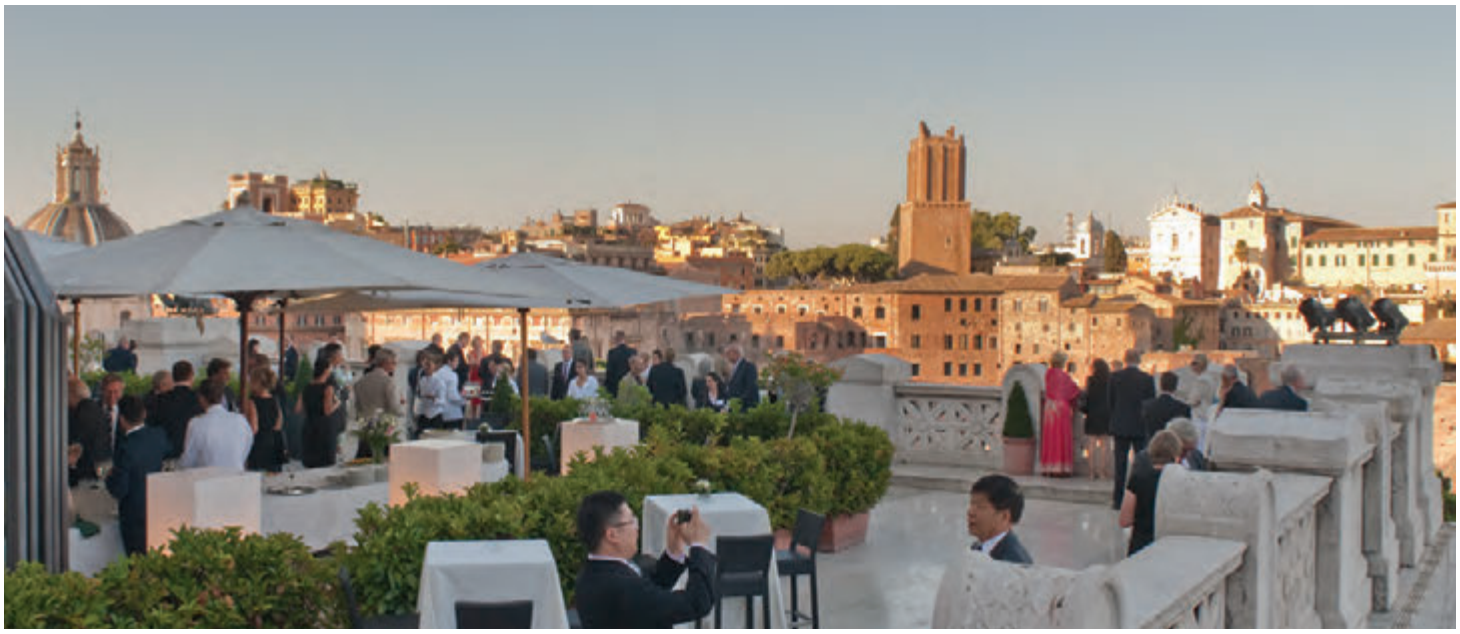
TOP ROW
Reception and dinner on the terrace of the Victor Emmanuel II Monument, also called Vittoriano.

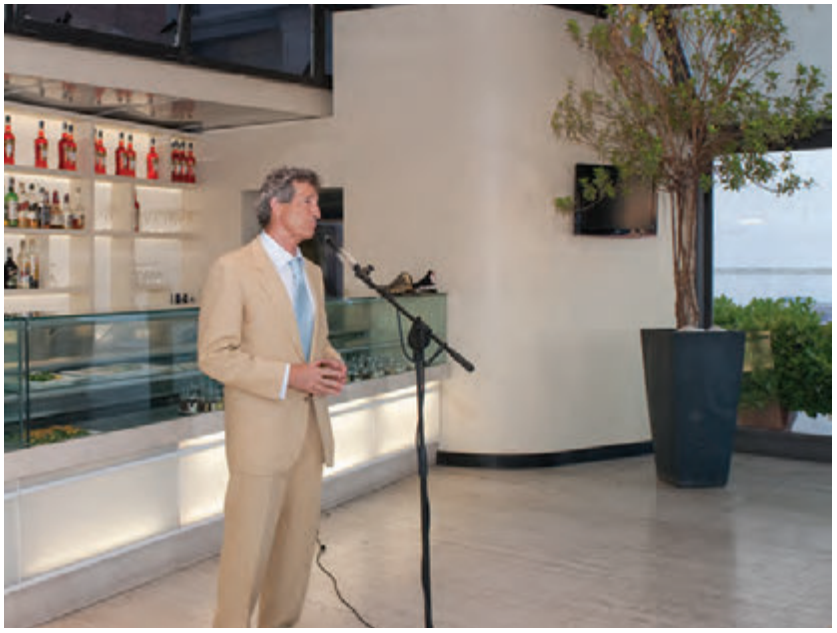
MIDDLE ROW
left photo
Ambassador Stefano Stefanini introduces His Excellency Franco Frattini,
Member of Parliament and former Foreign Minister of Italy.

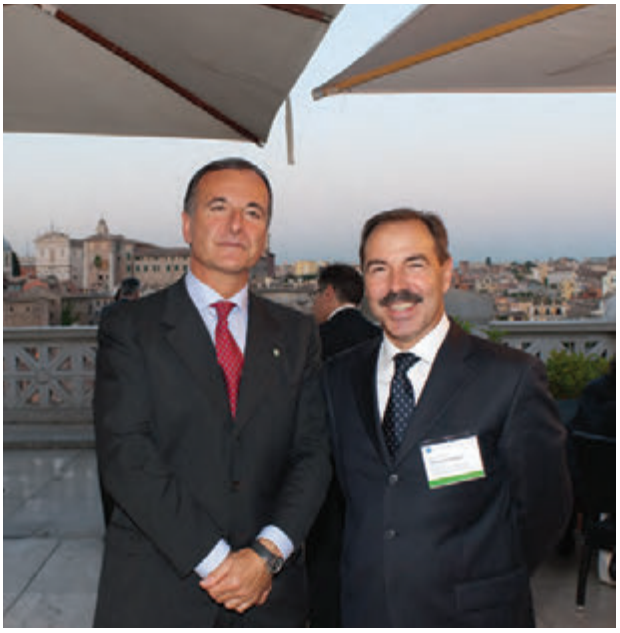
right photo
His Excellency Franco Frattini, Member of the Italian Parliament *(l)*
and Major General Salvatore Farina, Italian Defense General Staff *(r)*.

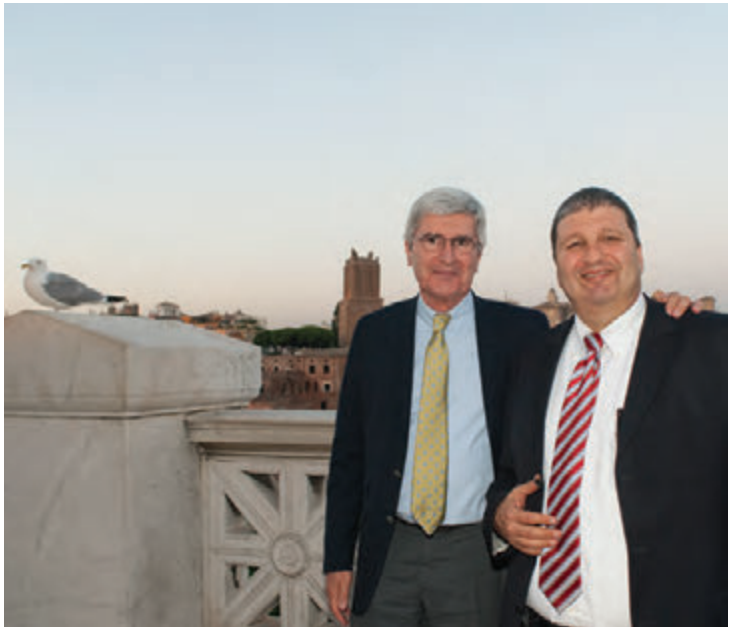
BOTTOM ROW
left photo
Mr. Yvon Le Roux, Vice President, Cyber Security, Cisco Systems *(l)*
and Mr. Eyal Bavli, Director Vertical Sales, Cisco Systems *(r)*.

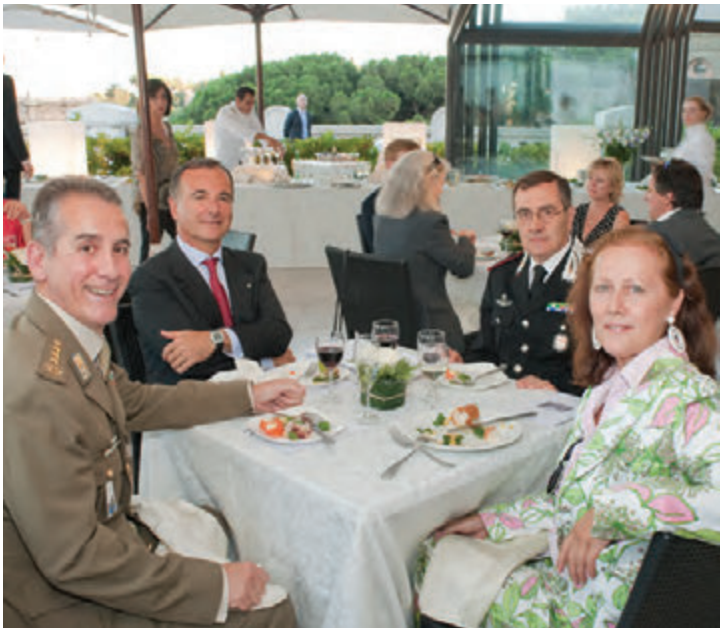
right photo, from left to right
Colonel Alessandro Carile, Centro Militare di Studi Strategici (CeMISS);
His Excellency Franco Frattini, Member of the Italian Parliament;
Major General Eduardo Centore, Director, Centro Militare di Studi Strategici (CeMISS);
Mrs. Carile.











TOP ROW

left photo

Mr. Gianluca Carmine Ansalone, Office of the Diplomatic Advisor to the President of Italy *(l)* and Mr. Andrea Rigoni, Director General, Global Cyber Security Center *(r)*.

right photo

View over the Forum of Trajan from the Capitoline Museums.

MIDDLE ROW

left photo

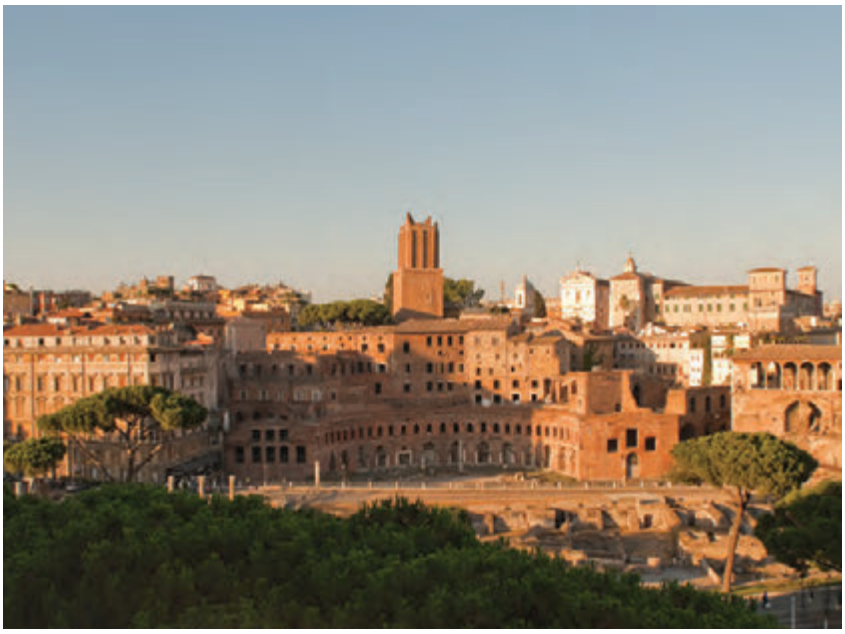
Private visit of the Capitoline Museums.

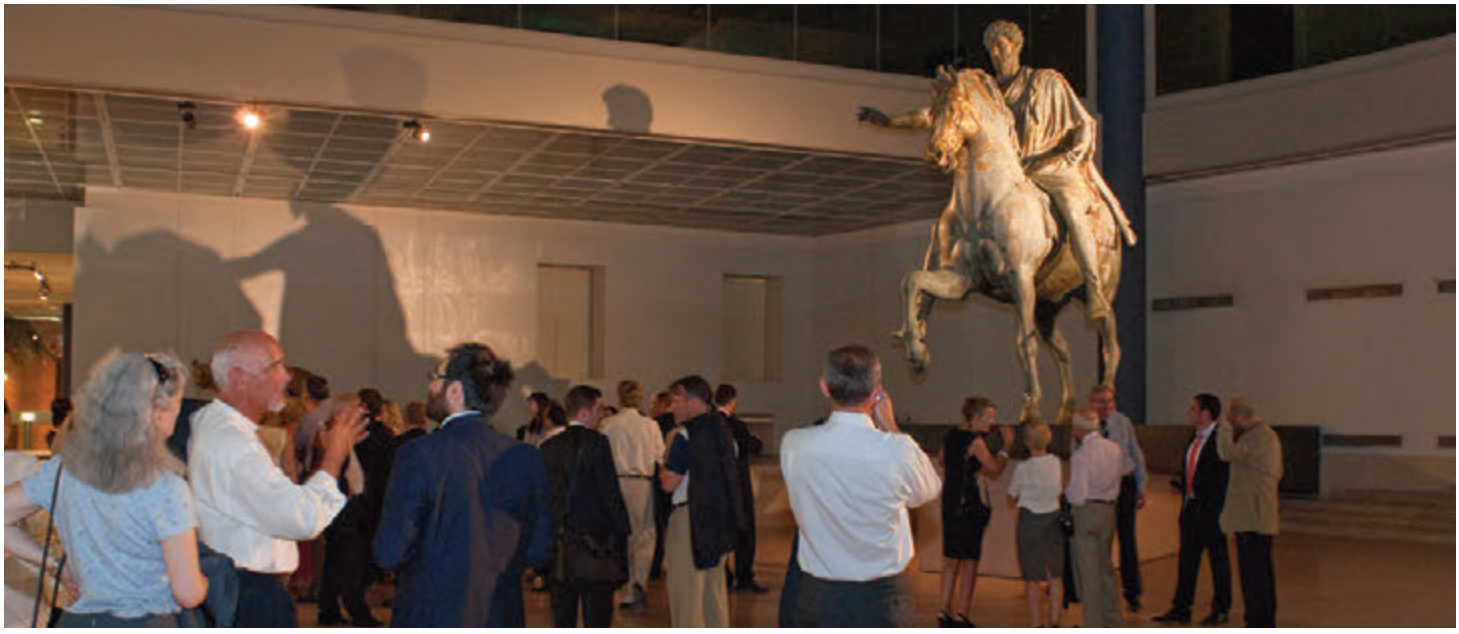
right photo

General and Mrs. Manfred Lange and the Etruscan statue of the She-Wolf. The Romulus and Remus twins, representing the founders of the city of Rome, were added later in the 15th century.

BOTTOM ROW

The ancient equestrian statue of Marcus Aurelius from approximately 175 AD.





The *29th international Workshop on Global Security* is presented by the *Center for Strategic Decision Research* with the sponsorship of the following governments and organizations:

IL PRESIDENTE DELLA REPUBBLICA ITALIANA

MINISTERO DELLA DIFESA
REPVBBLICA ITALIANA

U.S. DEPARTMENT OF DEFENSE
Under Secretary of Defense (AT&L)
Defense Threat Reduction Agency
Net Assessment

eMiSS

CENTRO INNOVAZIONE DIFESA
CENTRE for DEFENCE INNOVATION

PRINCIPAL SPONSORS

CISCO

McAfee | intel

FINMECCANICA

MAJOR SPONSORS

AFCEA

elt
MIND IS THE FIRST DEFENCE

MITRE

NORTHROP GRUMMAN

renesys

RES GROUP

URS

THE UNIVERSITY of TENNESSEE
NATIONAL DEFENSE BUSINESS INSTITUTE

IBM

SELEX ELSAG
Secure Networking Solutions
A Finmeccanica Company

SELEX
Sistemi Integrati
A Finmeccanica Company

ACKNOWLEDGEMENTS OF PAST HOST AND SPONSORING GOVERNMENTS

Czech Republic

Kingdom of Denmark

Federal Republic of Germany

Republic of Greece

Republic of Hungary

Kingdom of the Netherlands

Kingdom of Norway

Republic of Poland

Republic of Portugal

Ministry of Defense of Austria

Ministry of Defense of France

Ministry of Defense of Italy

Ministry of Defense of Turkey

Canadian Armed Forces

Russian Ministry of Industry, Science, and Technology

Contents

Contributors

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

General Biagio Abrate
Chief of Defense General Staff of Italy

His Excellency Anyu Anguelov
Minister of Defense of Bulgaria

Mr. Gianluca Carmine Ansalone
Office of the Diplomatic Advisor to the President of Italy

Ms. Neyla Arnas
Senior Research Fellow, National Defense University

His Excellency Giorgi Baramidze
Vice Prime Minister and State Minister for European and Euro-Atlantic Integration of Georgia

Mr. Eyal Bavli
Director Vertical Sales, Cisco Systems

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

Ing. Domitilla Benigni
Chief Operating Officer (COO), ELT | Elettronica

His Excellency Sali Berisha
Prime Minister of Albania

Ambassador Haydar Berk
Permanent Representative of Turkey to NATO

His Excellency Fatmir Besimi
Minister of Defense of Macedonia; former Minister of the Economy

Admiral Jean Betermier (Ret.)
EADS

Mr. Andrea Biraghi
Senior Vice President, Business Unit Cyber Security, SELEX Elsag

Lieutenant General Jürgen Bornemann
Director General, NATO International Military Staff

Mr. Andrea Campora
Senior Vice President, Sales and Business Development, SELEX Elsag

Lieutenant General Nazzareno Cardinali (Ret.)
Chairman of the Board, SELEX Elsag

Colonel Alessandro Carile
Chief, External Relations Office, Centro Militare di Studi Strategici (CeMiSS)

Mr. Alessandro Cattaneo
Office of the Diplomatic Advisor to the President of Italy

Major General Eduardo Centore
Director, Centro Militare di Studi Strategici (CeMiSS)

Ambassador Vladimir Chizhov
Permanent Representative of the Russian Federation to the EU

General Mieczysław Cieniuch
Chief of the General Staff, Armed Forces of Poland

Mr. Mauro Collalto
CEO, RESI Group

Mr. James Cowie
Chief Technical Officer (CTO), Renesys

Mr. Eugenio Creso
SELEX Sistemi Integrati

Mr. Oris E. Davis, Jr.
Director, Southern Europe, International Business Development (IBD) Boeing Defense, Space & Security (BDS)

General S.A. Claudio Debertolis
Italian Secretary General of Defense and National Armaments Director

Rear Admiral Nicola De Felice
Director, Centro Innovazione Difesa (CID), Italian Defense General Staff

Mr. Nicola de Santis
Head, Middle East and North Africa Section, Political Affairs and Security Policy Division, NATO Headquarters

Prefect Carlo De Stefano
Undersecretary of State, Ministry of the Interior of Italy

Mr. Giovanni Di Meo
Innovation Department, SELEX Elsag

His Excellency Admiral Giampaolo Di Paola
Minister of Defense of Italy

Major General Salvatore Farina
Director of Military Policy and Planning, Italian Defense General Staff

General Pietro Finocchio (Ret.)
President, AFCEA Italy

Dr. Lorenzo Fiori
Senior Vice President and Chief Technical Officer (CTO), Finmeccanica

Mr. Goffredo Forcinella
Team Leader, Difesa e Finmeccanica, IBM Italy

Dr. Marco Forlani
Executive Vice President External Relations, Finmeccanica

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

Dr. Luisa Franchina
Director General, Secretariat for Critical Infrastructures, Presidency of the Council of Ministers

Mr. Jacques Francoeur
Executive Director, Union of Concerned Cybersecurity Leaders

His Excellency Franco Frattini
Member of Parliament; former Minister of Foreign Affairs of Italy

Mr. Gary Gagnon
Senior Vice President and Chief Security Officer, The MITRE Corporation

Ms. Daniela Garozzo
Head of Cyber Security Business Development, SELEX Elsag

Lieutenant General Walter Gaskin
Deputy Chairman, NATO Military Committee

Major General Nicola Gelao
Chief of the Information and Security Division, Italian Defense General Staff

Major General Franco Girardi
Italian Defense General Staff

Ms. Harriet Goldman
Executive Director of Cyber Mission Assurance, The MITRE Corporation

Lieutenant General Claudio Graziano
Chief of General Staff, Italian Army

Mr. Steve Grobman
Chief Technology Officer (CTO), McAfee | Intel Technologies, McAfee

Mr. Raymond Haller
Senior Vice President, The MITRE Corporation

Ms. Melissa Hathaway
President, Hathaway Global Strategies

Mr. John Horridge
Honorary Advisor Italy, AeroSpace Defence Security (ADS)

Mr. Glori Husi
Advisor to the Prime Minister of Albania

Dr. Edward M. Ifft
Adjunct Professor, School of Foreign Affairs, Georgetown University

Mr. Sergio Attilio Jesi
Vice President, External Relations and New Markets Promotion, ELT | Elettronica

Mr. Jiang Zhenxi
Senior Research Fellow, China Institute for International Strategic Studies (CIISS)

Major General Miroslav Kocian
First Deputy Chief of the General Staff, Armed Forces of Slovakia

Ambassador Llesh Kola
Ambassador of Albania to Italy

Ambassador Artur Kuko
Permanent Representative of Albania to NATO

His Excellency Dr. Zlatko Lagumdžija
Deputy Chairman of the Council of Ministers and Minister of Foreign Affairs of Bosnia and Herzegovina

General Manfred Lange
Chief of Staff, Supreme Headquarters Allied Powers Europe (SHAPE)

Mr. Yvon Le Roux
Vice President, Cyber Security, Cisco Systems

Ambassador Mariot Leslie
Permanent Representative of the United Kingdom to NATO

The Honorable Jane Holl Lute
U.S. Deputy Secretary of Homeland Security

Mr. Maurizio Massari
Italian Special Envoy for the Mediterranean and Middle East

Dr. Ivan Mašulović
Deputy Minister of Defense of Montenegro

Mr. Lorenzo Mariani
Chief Operating Officer (COO), SELEX Sistemi Integrati

Dr. Douglas Maughan
Division Director, Cyber Security Division, U.S. Department of Homeland Security

Mr. Alessandro Menna
Business Unit Cyber Security, SELEX Elsag

Lieutenant General Frederik Meulman
Military Representative of the Netherlands to NATO and the EU

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

Mr. Terry Morgan
Principal, Global Thought

Mr. Marco Morucci
Rome Lab Leader IBM

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

His Excellency Giorgio Napolitano
President of Italy

Ambassador Rolf Nikel
Federal Government Commissioner for Disarmament and Arms Control, Federal Foreign Office of Germany

Mr. Giuseppe Orsi
CEO, Finmeccanica

His Excellency Dr. Artis Pabriks
Minister of Defense of Latvia

Mr. David Patterson
Executive Director, National Defense Business Institute, University of Tennessee

Mr. Ashton Peery
CEO, Renesys

Her Excellency Professor Milica Pejanovic-Djurisic, PhD
Minister of Defense of Montenegro

Mr. Emiliano Pierdominici
McAfee | Intel

Ing. Daniela Pistoia
Vice President, Research and Advanced Systems Design, ELT | Elettronica

Mr. Massimo Piva
Senior Vice President, SELEX Sistemi Integrati

Mr. David Pollington
Director of International Security Relations, Microsoft

Mr. Don Proctor
Senior Vice President, Office of the Chairman and CEO, Cisco Systems

Mr. Qian Zhongli
Associate Research Fellow, China Institute for International Strategic Studies (CIISS)

Mr. Antonio Raiano
Senior Vice President, External Relations, SELEX Elsag

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

Lieutenant General Arto Räty
Permanent Secretary, Ministry of Defense of Finland

Ambassador Maris Riekstins
Permanent Representative of Latvia to NATO

Mr. Andrea Rigoni
Director-General, Global Cyber Security Center (GSEC)

Mr. Rene Roersma
Director, Global Public Sector, McAfee | Intel

Mr. Marco Romani
Chairman, RESI Group

Senator Francesco Rutelli
Member of the Italian Senate; former Mayor of Rome

Mr. Raj Samani
Chief Technical Officer (CTO) EMEA, McAfee | Intel

Vice Admiral Ferdinando Sanfelice di Monteforte
Former Italian Military Representative to NATO

Mr. Kevin Scheid
Deputy General Manager, NATO Communications and Information Agency (NCI)

Mr. Jiří Schneider
First Deputy Minister of Foreign Affairs of the Czech Republic

Mr. Kent Schneider
President and CEO, AFCEA International

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

Mr. Stefan Sohm
Head of the Strategy and Police Branch, Ministry of Defense of Germany

Mr. Sergio Staro
Chief, Italian State Police

Ambassador Stefano Stefanini
Diplomatic Advisor to the President of Italy

Mr. Amedeo Vitagliano Stendardo
Member of Observatory for National Security of Ministry of Defense of Italy

Mr. John Stewart
Senior Vice President and Chief Security Officer (CSO), Cisco Systems

Mr. David Swindle
Executive Vice President, URS Federal Services

Ambassador David Thorne
U.S. Ambassador to Italy

Major General Klaus-Peter Treche (Ret.)
General Manager Europe, AFCEA International

Ms. Selma Užičanin
Minister Counselor, Ministry of Foreign Affairs of Bosnia and Herzegovina

Lieutenant General Ton van Loon
Commander, 1 (German / Netherlands) Corps

Ms. Maja Vuković
Advisor, International Cooperation Department, Ministry of Defense of Montenegro

Mr. Domenico Vulpiani
Director General, State Police, Coordinator for Information Security and Protection of Critical Infrastructure

Colonel Michael B. Warlick, USMC (Ret.)
Vice President, Chapter Outreach and Deputy for Operations, AFCEA International

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

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

Dr. Zbigniew Włosowicz
Undersecretary of State for International Affairs, Ministry of Defense of Poland

Admiral Luciano Zappata (Ret.)
Former NATO Deputy Supreme Allied Commander

Observers and Support Staff

His Excellency Nerkez Arifhodzic
Ambassador of Bosnia and Herzegovina to Italy

His Excellency Petr Burianek
Ambassador of the Czech Republic to Italy

Ms. Aurora Cappiello
External Relations, SELEX Elsag

Colonel Stefano Chille
1 (German / Netherlands) Corps

Colonel Christopher Cook
Air Force Attaché, U.S. Embassy

Lieutenant Colonel Scott Davis
Military Assistant to the Deputy Chairman of the NATO Military Committee

Mr. Brian de Vallence
Chief of Staff, U.S. Department of Homeland Security

Mr. Marco Donfrancesco
Head of Special Programs and Projects, SELEX Sistemi Integrati

Ms. Bora Dushku
Political Councillor, Embassy of the United Kingdom to Italy

Ms. Hana Honkova
Deputy Head of Mission, Embassy of the Czech Republic to Italy

Major Ryan Hoyle
Aide-de-Camp to the Deputy Chairman of the NATO Military Committee

Colonel Kevin Judd
Office of Defense Cooperation, U.S. Embassy

Major Petteri Korvala
Military Assistant to the Permanent Secretary, Finnish Ministry of Defense

Ms. Marija Lakic
First Secretary, Embassy of Montenegro to Italy

Dr. Lucio Martino
Senior Researcher, Centro Militare di Studi Strategici (CeMiSS)

Ms. Vesna Njegic
Minister Counselor, Embassy of Bosnia and Herzegovina to Italy

Captain Mateo Osterhagen-Zalles
Supreme Headquarters Allied Powers Europe (SHAPE)

Captain Anthony Parisi
Defense Attaché, U.S. Embassy

Ms. Bindi Patel
Political-Military Officer, U.S. Embassy

Mr. Fabio Romani
Market Strategy and Institutional Relations, RESI Group

Ms. Sofio Samushia
Euro-Atlantic Integration Coordination Department, Office of the State Minister of Georgia

Mr. Ugo Santillo
Sales Director, RESI Group

Mr. Philip Stupak
Special Assistant, U.S. Department of Homeland Security

Ms. Maura Taschler
Italian Presidency of the Council of Ministers

His Excellency Vojin Vlahovic
Ambassador of Montenegro to Italy

Dr. Domenico Vozza
Security Division Chief, ENEL Roma

Warrant Officer Slawomir Witkowski
Aide-de-Camp to the Polish Chief of General Staff

International Workshop Staff

Caroline Baylon, BA, Stanford University; MSc, University of Oxford
Dr. Ania Garlitski, MD, Assistant Professor of Medicine, Tufts University
Grace Wong, MA, Stanford University
Sebastian Haug, MSc, University of Oxford
Jean Lee, BA, Stanford University
Lucia de Ferrari, John Cabot University (Rome)

Preface and Acknowledgments

With the High Patronage of the President of the Italian Republic, His Excellency Giorgio Napolitano, and of the Italian Minister of Defense, His Excellency Giampaolo Di Paola, this year's 29th International Workshop on Global Security was presented in Rome on 16-18 July at the Hotel Parco dei Principi, which is happily located immediately adjacent to Rome's Villa Borghese Park. General Biagio Abrate, Chief of the Italian Defense General Staff, was the Honorary Chairman. The workshop themes, "Today's Critical Challenges to Peace and Security: The Global Economic Crisis, the Unpredictable Evolution of the Arab Spring, the Complex Transition in Afghanistan and Pakistan—and the Rapid Growth of Cyber Threats," were especially appropriate given the spreading economic crisis, the impending withdrawal of NATO forces from the Afghanistan/Pakistan conflict, the extraordinary political and social developments arising from the Arab Spring, and the rapidly growing concern for the security of cyber space, which is truly central to modern societies. Many of the workshop presentations and discussions sought to understand the relationships between these events.

Patronage of the Italian President and Defense Minister. We are grateful to Ambassador Stefano Stefanini, Diplomatic Advisor to the President of Italy, who opened the 29th International Workshop on behalf of the President. We appreciate his considerable assistance as well as that of his colleagues, Mr. Gianluca Carmine Ansalone and Mr. Alessandro Cattaneo, in coordinating the participation of Senator Francesco Rutelli, former Mayor of Rome; Member of the Italian Parliament Franco Frattini, former Minister of Foreign Affairs; Ambassador Maurizio Massari, Italian Special Envoy for the Mediterranean and Middle East; and Mr. Andrea Rigoni, Global Cyber Security Center. Ambassador Stefanini's office, together with the Defense General Staff, also were instrumental in arranging the workshop evening events at the Villa Giulia (the National Etruscan Museum), the Galleria Borghese, and the Capitoline Museum.

We would also like to thank Defense Minister Giampaolo Di Paola for his patronage, especially since he has been such a strong supporter of past workshops, including our 25th International Workshop in Italy in June 2008, for which he was a key opening speaker in his then-role as Chief of the Defense General Staff. Minister Di Paola's observations in his keynote opening address set the tone for thoughtful discussions at the 29th International Workshop. Rear Admiral Nicola De Felice, Director of the Centro Innovazione Difesa (CID), headed the initial study which recommended that the Italian Defense Minister invite this year's workshop to Rome. Major General Eduardo Centore, as Director of the CeMiSS, also played a vital organizational role, especially through the energetic support of Colonel Alessandro Carile, head of external relations in his institute. As our principal liaison with the Defense Ministry, he contributed to a great many aspects of the workshop organization, if not to all of them. Other key Italian official supporters were Lieutenant General Claudio Debertolis, Italy's Secretary General of Defense; Lieutenant General Claudio Graziano, Chief of General Staff of the Italian Army; Major General Farina; Major General Nicola Gelao; and Major General Franco Girardi.

Within the Interior Ministry, we owe a great deal to Prefect Carlo De Stefano, Undersecretary of State, and especially to Mr. Domenico Vulpiani, Director General, State Police, Coordinator for Information Security and Protection of Critical Infrastructure, as well as Mr. Sergio Stare within his organization. Finally, within the office of the Military Advisor to the Prime Minister, we would like to acknowledge the many contributions of Dr. Luisa Franchina, Director General, Secretariat for Critical Infrastructures.

Key address by Deputy Secretary of Homeland Security Jane Holl Lute and U.S. co-sponsorship. Since the workshop was co-sponsored by the U.S. government, the personal participation of Deputy Secretary of Homeland Security Jane Holl Lute as a key speaker was especially significant. Her remarks on key policy questions helped frame the conversation about cyber security at the workshop. Dr. Douglas Maughan played a major role in arranging her participation and also gave an important address of his own. The U.S. Ambassador to Italy, David Thorne, also delivered a key address on cyber security. Among other senior U.S. participants was Lieutenant General Walter Gaskin, Deputy Chairman of NATO's Military Committee. Dr. Linton Wells II, Distinguished Research Professor at the U.S. National Defense University, was represented by Ms. Neyla Arnas, Senior Research Fellow. Ms. Melissa Hathaway, former U.S. Cyber Security Coordinator, chaired the final workshop session.

Industry leaders. We would also like to thank the other principal speakers of the workshop, including Mr. Giuseppe Orsi, CEO of Finmeccanica, who gave an opening address, following Minister Di Paola. Equally important were the major industry presentations by McAfee|Intel Technologies' Mr. Steve Grobman as well as Mr. John N. Stewart and Mr. Donald Proctor, Senior Vice Presidents at Cisco.

Defense ministers and other high officials. We greatly appreciate the presentations by a large number of government leaders including Albanian Prime Minister Sali Berisha, who addressed the workshop for the second time; Estonia's Minister for Education and Research (and former Defense Minister) Jaak Aaviksoo; Bulgarian Defense Minister Anu Anguelov; Macedonian Defense Minister Fatmir Besimi; General Mieczysław Cieniuch, Chief of the Polish General Staff; Mr. Glori Husi, Advisor to the Albanian Prime Minister; Bosnia and Herzegovina's Deputy Chairman of the Council of Ministers and Minister of Foreign Affairs Dr. Zlatko Lagumdžija; Dr. Ivan Mašulović, Montenegrin Deputy Minister of Defense; Latvian Defense Minister Dr. Artis Pabriks; Montenegrin Defense Minister Professor Milica Pejanović-Durišić, Ph.D.; as well as Finland's Permanent Secretary in the Ministry of Defense, Lieutenant General Arto Räty; Ambassador Bogusław Winid, Undersecretary of State, Polish Ministry of Foreign Affairs; Mr. Jiří Schneider, Czech First Deputy Minister of Foreign Affairs; Dr. Zbigniew Włosowicz, Undersecretary of State for International Affairs, Polish Ministry of Defense; and Georgian Vice Prime Minister Giorgi Baramidze. They all made important contributions that deepened our understanding of the issues ranging from the Baltic region to Central Europe, the Balkans, and the Black Sea, and the turmoil in the Arab Spring countries.

NATO's important participation. We are thankful as well for the continued participation again this year of senior NATO officials and especially to General Manfred Lange, Chief of Staff, Supreme Headquarters Allied Powers Europe (SHAPE), who gave his personal assessment of the future challenges in Afghanistan. Permanent Representatives on the North Atlantic Council were Ambassador Mariot Leslie (United Kingdom), Ambassador Haydar Berk (Turkey), Ambassador Artur Kuko (Albania), and Ambassador Maris Riekstins (Latvia). The NATO Military Committee representatives, in addition to Lieutenant General Gaskin, were Lieutenant General Jürgen Bornemann, Director General of the International Military Staff, and Lieutenant General Frederik Meulman (Netherlands). Other senior officials included Dr. Jamie Shea, Deputy Assistant Secretary General for Emerging Security Challenges, and Mr. Kevin Scheid, Deputy General Manager, NATO Communications and Information Agency.

United Nations and the EU. From the United Nations in New York, we greatly valued the active support of Croatia's Ambassador Ranko Vilović, even though he was unable to join the workshop this year. From Brussels, Ambassador of the Russian Federation to the EU Vladimir Chizhov, one of his country's senior diplomats, was a strong contributor to the workshop debates.

Other senior officials. Given the outstanding support of the French government during last year's 28th International Workshop in Paris, it was a pleasure to welcome Ing. General Robert Ranquet, Deputy Director of the Institut des hautes études de défense nationale (IHEDN); Ambassador Michel Foucher, Director of Studies and Research at IHEDN; and Admiral Jean Betermier, EADS.

WORKSHOP VENUES

The Villa Giulia, National Etruscan Museum. Early arriving participants were welcomed on 15 July by a reception and private visit of the Villa Giulia. Built by Pope Julius III in 1550–1555, the villa is located within the vast Villa Borghese Park and it houses the Museo Nazionale Etrusco—the National Etruscan Museum. It offers one of the world's best collections of Etruscan art, with some of the most famous pieces from the 8th to 5th centuries BC, including the celebrated "Sarcophagus of the Spouses."

The Galleria Borghese. The gallery is located in the Villa Borghese, which was built by Cardinal Scipione Borghese, nephew of Pope Paul V, in the 16th century as a summer residence and home for his art collection. Scipione Borghese was a great patron of Bernini as well as an avid collector of paintings, assembling an impressive collection by such artists as Caravaggio, Titian, Raphael, and Peter Paul Rubens.

Capitoline Museums. The Capitoline Museums are comprised of two palaces—one built by Michelangelo in 1536—situated on the beautiful Campidoglio Square atop the Capitoline Hill. The museums con- tain an ancient Roman sculpture collection, including the famous bronze She-Wolf nursing Romulus and Remus which is an important symbol of Rome. At the final dinner in the museum, Italy's former Foreign Minister, Franco Frattini, gave the workshop's closing address.

Parco dei Principi. The opening dinner address by Senator Francesco Rutelli was held in the Garden Room of the Parco dei Principi. The hotel was an ideal venue for the workshop sessions; we appreciate its contributions to the event's success.

PRINCIPAL SPONSORS

We would like to acknowledge the principal sponsors of the 29th International Workshop who, through their sponsorship and efforts, made this workshop possible:

- The President of the Italian Republic
- The Italian Minister of Defense
- The United States Department of Defense (Under Secretary of Defense for Acquisition, Technology, and Logistics; Office of the Director of Net Assessment in the Office of the Secretary of Defense; National Defense University)
- Cisco
- McAfee|Intel
- Finmeccanica

Under Secretary of Defense for Acquisition, Technology, and Logistics. Mr. Alfred Volkman, Director of International Cooperation in the Office of the Under Secretary of Defense for AT&L, who retired from the U.S. Defense Department shortly before the workshop, helped develop a session on how industry can contribute to handling the challenges in Afghanistan and Pakistan while coping with shrinking defense resources. Ms. Mary Miller and Mr. Frank Kenlon provided valuable coordination with the U.S. Embassy in Rome.

Office of the Director of Net Assessment. Since the very beginning of this workshop series nearly 30 years ago, Mr. Andrew Marshall, Director of Net Assessment in the Office of the Secretary of Defense, has provided sponsorship and guidance. We are extremely grateful for his valuable input and backing. For many years now, Ms. Rebecca Bash has ably overseen the administration of this project.

Defense Threat Reduction Agency. DTRA has been a very important workshop supporter for a quarter-century. Colonel Robert Dickey has worked with great diligence to ensure smooth coordination with the agency.

Cisco. Now in its fourth year as a workshop sponsor, Cisco was represented by Mr. John N. Stewart, Chief Security Officer; Mr. Donald Proctor, Senior Vice President, Office of the President and CEO; Mr. Eyal Bavli, Director of Vertical Sales; and Mr. Yvon Le Roux, Vice President, Cyber Security.

McAfee|Intel. We were delighted that McAfee|Intel has continued its support as a Principal Sponsor, and appreciate the assistance of Kent Rounds, Vice President, Global Defense/Central Government; Mr. Rene Roersma, Director, Global Public Sector; Mr. Raj Samani, Chief Technical Officer (CTO) EMEA; and Mr. Emiliano Pierdominici. Most importantly, Mr. Steve Grobman, CTO for McAfee|Intel Technologies, was the company's keynote speaker.

Finmeccanica. While Finmeccanica has sponsored the workshop for at least two decades, this was the first time that the workshop was addressed by its CEO, Mr. Giuseppe Orsi. We are especially grateful to Dr. Lorenzo Fiori, Senior Vice President and Chief Technical Officer (CTO), and Dr. Marco Forlani, Executive Vice President External Relations.

MAJOR SPONSORS

AFCEA. We are pleased to welcome back AFCEA as a sponsor with special thanks to Mr. Kent Schneider, President and CEO, who gave an important workshop address; Colonel Michael B. Warlick, USMC (Ret.), Vice President, Chapter Outreach and Deputy for Operations; Major General Klaus-Peter Treche (Ret.), General Manager Europe; and finally General Pietro Finocchio (Ret.), President, AFCEA Italy.

Northrop Grumman. Our association with Northrop Grumman goes back even prior to the Northrop Grumman merger. We are delighted that Mr. James Moseman, Director, Europe and NATO, was able to represent the company at the workshop. Moreover, we owe a special debt to Mr. William Ennis, Director International Programs, for his continued support.

The MITRE Corporation. MITRE has been a supporter and sponsor of the workshop for nearly 30 years. Our thanks go to Mr. Raymond Haller, Senior Vice President and Director, DoD C3I FFRDC, for his many years of participation as well as to Mr. Gary Gagnon, Senior Vice President and Chief Security Officer; and Ms. Harriet Goldman, Executive Director of Cyber Mission Assurance.

ELT | Elettronica. At ELT, we are most grateful for the strong support and participation by Ms. Domitilla Benigni, Chief Operating Officer (COO); Ing. Daniela Pistoia, Vice President, Research and Advanced Systems Design; and Mr. Sergio Attilio Jesi, Vice President, External Relations and New Markets Promotion.

URS Federal Services. At URS Federal Services, we thank Mr. David Swindle, Executive Vice President, for participating again this year.

Renesys. Sponsoring the workshop for the first time this year were Mr. Ashton Peery, CEO, Renesys and Mr. Jim Cowie,

Chief Technical Officer.

IBM. We appreciate the important workshop address by Mr. Marco Morucci, Rome Lab Leader, and the support of Mr. Goffredo Forcinella Team Leader, Difesa e Finmeccanica, as well as Mr. Stefano Rebattoni.

University of Tennessee, National Defense Business Institute. As a workshop sponsor for the fourth year, the University of Tennessee was represented by Mr. J. David Patterson, Executive Director, National Defense Business Institute.

RESI Group. For the first time, the workshop was sponsored by the RESI Group through Mr. Marco Romani, Chairman; and Mr. Mauro Collalto.

Selex Elsag. At Selex Elsag, we would like to thank General Nazzareno Cardinali, Chairman of the Board, as well as Mr. Andrea Biraghi, Mr. Andrea Campora, Ms. Aurora Cappiello, Mr. Giovanni Di Meo, Ms. Daniela Garozzo, Mr. Alessandro Menna, Mr. Giorgio Mosca, and Mr. Antonio Raiano.

Selex Sistemi Integrati. The representatives of Selex S.I. were Mr. Lorenzo Mariani, Chief Operating Officer (COO) and Mr. Massimo Piva, Senior Vice President, as well as Mr. Eugenio Creso.

PATRONS, ADVISORS, AND PARTICIPANTS

Workshop Patrons, Honorary Chairmen, and Keynote Speakers. We gratefully acknowledge the support of our past and present workshop patrons, general chairmen, and keynote speakers:

His Excellency Giorgio Napolitano, President of the Italian Republic (Workshop Patron, 2012)
His Excellency Sali Berisha, Prime Minister of Albania (Keynote Speaker, 2012, 2010)
His Excellency Admiral Giampaolo Di Paola, Minister of Defense of Italy (Patron and Keynote Speaker, 2012, 2008)
The Honorable Jane Holl Lute, U.S. Deputy Secretary of Homeland Security (Keynote Speaker, 2012)
General Biagio Abrate, Chief of Italian Defense General Staff (Honorary Chairman, 2012)
Mr. Giuseppe Orsi, CEO, Finmeccanica (Keynote Speaker, 2012)
His Excellency Gérard Longuet, Minister of Defense of France (Workshop Patron and Keynote Speaker, 2011)
The Honorable William J. Lynn III, Deputy Secretary of Defense of the United States (Keynote Speaker, 2011)
Mr. Louis Gallois, CEO, EADS (Opening Key Address, 2010, 2011)
State Secretary Rüdiger Wolf, German Federal Ministry of Defense (Keynote Speaker, 2010)
His Excellency Vecdi Gönül, Minister of Defense of Turkey (Patron, 2009; Keynote Speaker, 2009, 2008, 2004)
His Excellency Ignazio La Russa, Minister of Defense of Italy (Workshop Patron, Keynote Speaker, 2008)
His Excellency Hervé Morin, Minister of Defense of France (Workshop Patron, 2007)
His Excellency Franz Josef Jung, Minister of Defense of Germany (Workshop Patron, Keynote Speaker, 2006)
Her Excellency Michèle Alliot-Marie, Minister of Defense of France (Workshop Patron, 2005, 2007; Keynote, 2005)
His Excellency Peter Struck, Minister of Defense of Germany (Keynote Speaker, 2004)
His Excellency Rudolf Scharping, Minister of Defense of Germany (Workshop Patron, Keynote Speaker, 2002, 2000)
His Excellency Jan Trøjborg, Minister of Defense of Denmark (Workshop Patron, 2001)
His Excellency Arpád Göncz, President of Hungary (Workshop Patron, Keynote Speaker, 1999)
His Excellency Dr. Werner Fasslabend, Minister of Defense of Austria (Workshop Patron, Keynote Speaker, 1998)
His Excellency Václav Havel, President of the Czech Republic (Workshop Patron, 1997; Keynote Speaker, 1997, 1996)
His Excellency Aleksander Kwaniewski, President of Poland (Patron, 1996; Keynote, 2002, 2000, 1998, 1997, 1996)
His Excellency Volker Rühe, Minister of Defense of Germany (Workshop Patron, 1995)
General Vincenzo Camporini, Chief of General Staff of Italy (Honorary Chairman, Keynote Speaker, 2008)
General James Jones, Supreme Allied Commander Europe (Keynote Speaker, 2007, 2006, 2004)
General Henri Bentégeat, Chair of EU Military Committee, former Chief of General Staff of France (Keynote, 2007)
General George Joulwan, Supreme Allied Commander Europe (Honorary General Chairman, 1997, 1996, 1995, 1994)
General John Shalikashvili, Supreme Allied Commander Europe (Keynote Speaker, 1993)

Advisory Board. Our informal board of advisors, which has provided excellent input in developing the workshop agenda over the years, was joined by a large number of other officials and experts who helped in planning this year's workshop, including Minister Jaak Aaviksoo, the current Minister of Education and Research of Estonia and a former Minister of Defense; Admiral Jean Betermier, Senior Advisor to the CEO, EADS; Mr. William Ennis, Northrop Grumman; Rear Admiral Nicola De Felice, Director of the Centro Innovazione Difesa, Italian Defense General Staff; Mr. Lorenzo Fiori,

Senior Vice President and CTO, Finmeccanica; Mr. Ray Haller, Senior Vice President, MITRE; General George A. Joulwan (Ret.), former Supreme Allied Commander, Europe; Mr. Robert Lentz, former U.S. Deputy Assistant Secretary of Defense; Mr. Donald Proctor, Senior Vice President, Cisco; Ing. Général Robert Ranquet, Directeur Adjoint, IHEDN; Mr. Kent Rounds, Senior Vice President, McAfee|Intel; Vice Admiral Sanfelice di Monteforte, former Italian Military Representative to the NATO Military Committee; Ambassador Stefano Stefanini, Diplomatic Advisor to the President of Italy; Mr. John N. Stewart, Senior Vice President, Cisco; Mr. David Swindle, Executive Vice President, URS; Dr. Linton Wells II, Distinguished Research Professor, U.S. National Defense University; Ambassador Bogusław Winid, Under Secretary of State, Polish Ministry of Foreign Affairs; Admiral Luciano Zappata, former Deputy Supreme Allied Commander, Transformation.

CSDR TEAM

Workshop International Staff. This year's international workshop staff comprised Dr. Ania Garlitski, Jean Lee, Grace Wong, Sebastian Haug, Lucia de Ferrari, and Caroline Baylon. Professor Ania Garlitski, M.D., is a binational American and Polish cardiologist and Assistant Professor at Tufts-New England Medical Center. She began working with CSDR when she was a Stanford University undergraduate in 1995. Jean Lee, who became our graphic designer and photographer shortly after graduating from Stanford University in 1995, worked on all the workshop graphics and was the workshop photographer. Grace Wong, an American journalist with degrees from the University of Michigan and Stanford University, is based in London and San Francisco and returned to the workshop for the fourth year. Joining for the second time was Sebastian Haug, who has just received his Mas- ter's degree at Oxford University and is now working for the United Nations in Beijing, China. Joining the workshop for the first time was Lucia de Ferrari, an undergraduate student at the John Cabot University (Rome). Caroline Baylon, a binational French-American graduate of Stanford University and Balliol College, University of Oxford, has been a workshop staff member for over 15 years. In Rome this year, she led the team as Staff Director and as CSDR Vice President for Operations. Anne D. Baylon, CSDR Co-Director and a University of Paris Law School and Stanford University graduate, handled the coordination of the workshop as a whole.

Workshop Publications. As head of publications, Anne D. Baylon was responsible for the editing of these *Proceedings,* as well as transcribing and translating. She appreciates the contributions of Jean Lee—who is responsible for all of the photo pages—Caroline Baylon, and Grace Wong, who provided very helpful proofreading and editorial assistance.

In preparing this year's workshop, which included the participation of nearly thirty countries, we were assisted by a great many organizations and individuals. They made important contributions to the workshop agenda, events, and other activities. Although it is impossible to adequately acknowledge their efforts, we would like to extend our very warmest thanks.

Menlo Park, California and Paris, France
November, 2012

Part One

The Global Economic Crisis, the Unpredictable Evolution of the Arab Spring, and The Complex Transition in Afghanistan

Chapter 1

Welcoming Message from the President of the Republic of Italy

Ambassador Stefano Stefanini
Diplomatic Advisor to the President of Italy

First, I would like to acknowledge Minister of Defense Giampaolo Di Paola and Finmeccanica CEO Giuseppe Orsi, our keynote speakers, as well as the amazing work carried out by Roger Weissinger-Baylon and his staff at the Center for Strategic Decision Research (CSDR). I can assure you, having been involved as well, that getting this workshop off the ground was not easy. I would also like to thank my staff, Gianluca Ansalone and Alessandro Cattaneo, who worked closely with CSDR on this.

MESSAGE FROM THE PRESIDENT OF THE REPUBLIC OF ITALY

I have three tasks and little time, so let me begin. My first task is to read you a message from the President of the Republic of Italy, which follows:

> Through my diplomatic advisor, Ambassador Stefano Stefanini, I wish to extend my warmest greetings to the organizers and participants of the 29th International Workshop on Global Security. I acknowledge with satisfaction the choice of the organizers to once again hold the symposium in Rome after the interesting 2008 edition. The themes on the agenda reflect the indivisibility of the world's security. The Arab Spring of the past two years has shown us that security cannot be separated from democracy and social justice. NATO and the European Union are guided by this principle. New technologies, the framework of contemporary societies and economies, are instruments of progress and social advancement but we must not forget that they also pose threats to states, to critical infrastructures, to the lives of citizens. With the hope that, thanks to the presence of numerous and qualified representatives of institutions and experts of international prestige, your debate will promote a fruitful exchange of ideas and proposals, I wish you every success.
>
> Signed
> Giorgio Napolitano

SOME COMMENTS ON INTERNATIONAL SECURITY AND CYBERSECURITY

As a second task, I am going to offer some very short comments to kick off the meeting. This annual event brings together a mix of diplomats, military leaders, politicians, and industry representatives from a wide range of countries, so it provides a mix of general and specialized knowledge. Having been a participant in several editions, I think we may not solve all the problems of security and international affairs, but we are forced to exchange ideas with each other, we are forced to think. This workshop is based on a principle that is quite common at NATO, that security is a common good. What does this mean? It means that we should not regard each other as threats but rather look at ourselves as being old friends. I realize that in some instances this lofty ideal might be debatable. However, in others the case is very strong and self-evident, the security of the cyberspace being one of them.

Other global threats have been around for longer and this workshop will not forget about the traditional crises around the world. But cybersecurity is one of the key challenges of the modern era. Our societies, our economies, our way of life

have come to depend heavily upon the free and legitimate use of cyberspace. And the threat to cybersecurity can come from anyone and anywhere—state and non-state actors, freelance hackers, criminal rings, and terrorists. It can be of a security nature or of a commercial and economic nature. Given the variety of threats, cybersecurity requires a unique and unprecedented degree of integrated response. We need cooperation. We need international cooperation rather than competition. We need cooperation between the public and private sector. And we need cooperation within the public sector. Defense, law enforcement, and homeland security come to mind but this affects every single area in the public administration. Cyberspace falls in the same category as navigation of the high seas, open skies, commerce routes, or the supply of energy.

INTRODUCTION OF THE MINISTER OF DEFENSE OF ITALY

I now move on to my third task, which is to introduce Admiral Giampaolo di Paola. Currently the Defense Minister of Italy, he formerly served as Chairman of the NATO Military Committee as well as as Chief of Defense of Italy. He has been a longtime advocate, nationally and internationally, of cybersecurity and cyberdefense.

Given that everybody knows Admiral Di Paola, rather than giving a presentation of his curiculum vitae, let me instead recount a few anecdotes about Giampaolo, whom I have known for approximately sixteen years. In September 2008, we had a Defense Ministerial in London. At the end of the meeting, the then Secretary General, Jan de Hoop Scheffer, gave the floor to Admiral Di Paola, who was just three months into his new role as Chairman of the NATO Military Committee. Admiral Di Paola said, "Dear Ministers, I have listened carefully to your conclusions. All is well but let me tell you that either you instruct your own bosses to do what you just agreed they should do or you have completely wasted your time." Being used to the previous—softer and gentler—Chairman, the room fell silent.

After Admiral Di Paola was appointed Defense Minister, I had the opportunity to ask my boss, President Napolitano, how Admiral Di Paola's name came up given the complex selection process. President Napolitano's answer was unequivocal: "He was by far the best choice, there was absolutely no question about it."

Il Presidente della Repubblica Italiana

MESSAGGIO DEL PRESIDENTE DELLA REPUBBLICA IN OCCASIONE DELL'INTERNATIONAL WORKSHOP ON GLOBAL SECURITY (ROMA, 16-19 LUGLIO 2012)

Roma, 16 luglio 2012

TRAMITE IL MIO CONSIGLIERE DIPLOMATICO, L'AMBASCIATORE STEFANO STEFANINI, DESIDERO FORMULARE I MIEI PIU' CORDIALI SALUTI AGLI ORGANIZZATORI E AI PARTECIPANTI AL 29MO WORKSHOP INTERNAZIONALE SULLA SICUREZZA GLOBALE. SALUTO CON SODDISFAZIONE LA SCELTA DEGLI ORGANIZZATORI DI RIPORTARE IL SIMPOSIO A ROMA, DOPO L'INTERESSANTE EDIZIONE DEL 2008.

I TEMI DEI VOSTRI LAVORI RIFLETTONO L'INDIVISIBILITA' DELLA SICUREZZA MONDIALE. NEGLI ULTIMI DUE ANNI LE PRIMAVERE ARABE HANNO DIMOSTRATO CHE ESSA NON PUO' ESSERE DISGIUNTA DA UNA CORNICE DI DEMOCRAZIA E GIUSTIZIA SOCIALE. NATO E UNIONE EUROPEA SONO GUIDATE DA QUESTA CONVINZIONE.

LE NUOVE TECNOLOGIE, AUTENTICA OSSATURA DELLE SOCIETA' E DELLE ECONOMIE CONTEMPORANEE, SONO STRUMENTI DI PROGRESSO E DI AVANZAMENTO SOCIALE MA NON DOBBIAMO DIMENTICARE CHE PONGONO ANCHE INSIDIOSE MINACCE AGLI STATI, ALLE LORO INFRASTRUTTURE CRITICHE, ALLA VITA DEI CITTADINI.

NELL'AUSPICIO CHE IL VOSTRO DIBATTITO, GRAZIE ANCHE A UNA RICCA E QUALIFICATA PRESENZA DI RAPPRESENTANTI DELLE ISTUTUZIONI ED ESPERTI DI PRESTIGIO INTERNAZIONALE, FAVORISCA UN FRUTTUOSO SCAMBIO DI IDEE E DI PROPOSTE, VI AUGURO BUON LAVORO.

Giorgio Napolitano

Chapter 2

Keynote Address of the 29th International Workshop on Global Security

His Excellency Giampaolo Di Paola
Minister of Defense of Italy

GLOBALIZATION, AUSTERITY, AND SECURITY

It is time to take a fresh approach to the issues because the reality in which we are now living requires it. Tremendous changes are happening globally in both the security and economic environments. If there is anyone who doubts the significance of globalization, he should carefully observe what is going on. We are at a moment in history when globalization is making us feel its punch. Currently, it is an economic punch: no matter how well-off we are, we are living in a time of tremendous fiscal constraint and in a time when our economies are heavily connected and completely interdependent. This is also true for emerging (or emerged) powers like China and India. In addition, there is a feeling that, if the United States has problems, everyone has them, too. So globalization is touching all of us, and sometimes hurting all of us, but if we are able to find a way out of this situation together, we will all benefit.

The observation that security and the economy are two faces of the same coin is a very common one, but that does not make it less true. Security and the economy are tied together. When we are faced with requirements for fiscal austerity and must at the same time tackle security issues, we must make trade-offs. We need to be careful since we might enjoy a short-term benefit from certain budget restrictions, but the cuts could lead to longer-term problems that will eventually affect the economy. Therefore, our countries' political leaders must assume the highest level of responsibility for their decisions: fiscal austerity requires them to carefully control how we spend money for security, but, at the same time, our leaders cannot disregard the challenges of security.

THE SHIFT TOWARDS THE ASIA-PACIFIC REGION

What is going on in the world? When we look at the comparative levels of attention to security in regions ranging from the Euro-Atlantic to the Asia-Pacific, we can clearly see a shift in emphasis toward the Asia-Pacific region. It is undeniable. This is not occurring simply because the United States has adopted it as a policy in their strategic review. Actually, it is in the U.S. strategic review because the shift is already happening. For example, the expansion of the Asian economy is fantastic in comparison with ours. Asia has become not just the economic driver but the security driver as well. Asian countries are spending more on security and investing more in defense. As a matter of fact, many of us are running toward the Asia-Pacific countries in an effort to support our floundering defense industries and exports, because our internal budgets cannot sustain our industries. This simple consideration should tell us how, even in the security area, the Asia-Pacific region is driving the future. For those of us who are fond of statistics, the aggregate defense expenditures (aside from the United States) in the Asia-Pacific region will overtake Western spending for the first time in 2013, which shows that the economy is also driving security and the defense expenditures. We have to take all this into account.

HOW TO COUNTER THIS SHIFT BY COMING TOGETHER

What can we do to counter this shift? Certainly, for the short and perhaps even medium term, we have no way of reversing this shift because, ultimately, defense expenditures are driven by the economy. If the money for the economy is not there, it will not be there for defense. This is the reality. So we have to find another way, which is to come closer together.

This is nothing new. It has been said in Chicago, in Italy, in the European Union, and in Europe. Coming closer together means having more effective defense spending, but it is also more than that. It means focusing more effectively on our real priorities, which are not only how we spend our money, but also how we can retain our technological edge—an advantage that we have always had. This is the key issue we have to resolve. If we are to come closer together, we must be ready to give up or at least limit part of our sovereignty and accept that what we make together must be used together. In the end, we might have a smaller force, but we will not have to compromise on quality. The force that we will be able to sustain together must be a usable force with leading-edge technology; it must be deployable and at the disposal of our policy; it must be fully and fundamentally interoperable and, furthermore, it must be interconnected—not only among our NATO Allies but also with our partners.

The Need to Cooperate with World Partners: Japan, Australia, Brazil, and Especially China

There is another big issue: Cooperation and coming closer together also mean coming closer together with other world partners. Recently, NATO Secretary General Anders Fogh Rasmussen made a clear and strong plea for this type of cooperative security, i.e., working with partners that are far away from us like Japan and Australia, perhaps working with countries like Brazil in the future, and possibly beginning to engage with China. Today, this remark might seem strange but it is a fact that China is a very considerable power in the Asia-Pacific region. Asia-Pacific countries pay great attention, perhaps with some concern, to what China is doing. So being ready to engage with China and being engaged by China without naïveté is probably the best way to avoid thinking of China as we did with regard to the Soviet Union in the past. This is not the time to revert to the old policy of confrontation; this is the time to engage with others; especially a country as large as China.

The Arab Awakening Calls for Political Solutions

We are surrounded by a web of challenges in the Middle East, in Northern Africa, in the so-called Arab Awakening, and in Syria. As an international community, we find it difficult to tackle the problems in Syria. We do not know how the Arab Awakening will evolve. When Secretary of State Hillary Clinton went to Egypt recently, it was very significant to see how she engaged both with Field Marshal Tantawi and with President Morsi as she tried to keep the dialogue going. This kind of cooperative approach, at least for such complex issues, is important not just in terms of traditional security; it represents a much more global political approach. Looking to the future, we will see how the Russian and Chinese positions evolve in Syria. Certainly, the Syrian issue needs to be tackled politically. At the same time, we need to carefully watch what is happening in case, under U.N. pressure, the international community is forced to take a course of action that ultimately cannot be achieved and, as a result, is forced to take a different direction. Syria's situation has a tremendous effect on the entire Middle East: it has an effect on Lebanon, on relations with Israel and on relations with Tehran. Therefore, this kind of complex crisis calls for a political solution with a really comprehensive approach. In strategic terms, this comprehensive approach is more than a classic civil-military cooperation; it requires looking at crisis management from a broader political and economic perspective and, if and when necessary, from a security perspective.

Afghanistan: We Must Stay Engaged for the Longer Run

In this big uncertain game, the issue of Afghanistan is not over yet. We have defined a path that we tend to follow with our allies, with our friends, and with the Afghan government, but when ISAF leaves at the end of 2014 there will be a new scenario in Afghanistan. The post-ISAF period, which will be a transition from the present situation to a more stable Afghanistan that will be somewhat at ease with its neighbors in the Central Asia region, will certainly not be a short-term engagement. This is why, as the Tokyo Conference on Afghanistan on 8 July reaffirmed, we need to stay engaged in Afghanistan in the longer run. This is essential if we do not want to repeat the Soviet Union's mistakes. When their forces departed, they left nothing behind—no money, no support and no soldiers—they just left. Barely two years later, Afghanistan's internal conflicts arose again. Given all our investments in Afghanistan as well as Afghanistan's central position for Asian security, we must continue to support its development if we want to prevent a similar situation from happening. Since this will be Afghanistan's own development, it will be its own choice, but we must be there to assist and provide support.

Ballistic Missile Proliferation Means We Need Missile Defenses

And then comes the new challenge and threat of the proliferation of weapons of mass destruction and of ballistic missile proliferation. If we believe that ballistic missile proliferation is a danger to us, the responses that we are developing such as missile defense, indicate that we are focusing on the proper priorities. It is not an all-encompassing response, but it is one that goes hand-in-hand with the political response and it is another example of a comprehensive approach.

Cyberspace Needs a Legal Foundation and International Rules

Finally, we are entering the world of the Global Commons, and cyberspace is the newest entry in the Global Commons. Today the cyber dimension is similar in many ways to what the maritime space was in the 14th, 15th, and 16th centuries. For our society—the way we live, the way we communicate, the way we do business—cyberspace is vital. So it is absolutely essential that cyberspace become a space for the good, a space that can be openly used like the maritime space or the air space. Therefore, this space needs some sort of legal foundation and international rules. Otherwise, there is a danger of either looking at cyberspace only in terms of openness or tightness. Some of us are focused on security and believe that cyberspace needs to be tightly controlled, but a tight control of the cyberspace would be impossible and would also be counter to the interest of our open society. Our society is based on openness, on the interchange of information and knowledge, and cyberspace is not only the fastest space for communication, it is a different way to develop knowledge and to develop business. It is a new foundation for our society.

So we must combine openness—because we need an open cyberspace—with security. This is not one versus the other. We have to find a common ground and security needs to be a space that is regulated by international law. It is not an easy task but, if you think about it, it was not easy either in the 14th or 15th centuries when discussions and negotiations started about regulating the open space of the time, which was the maritime space. It took four centuries to arrive at Montego Bay and the Law of the Seas! I hope it will not take four centuries in the case of the cyberspace, but cyberspace is an issue of extreme complexity and we need to start discussing it. And while we discuss it and try to regulate it internationally, we also need to develop a certain form of protection and security. This is what we are doing, both nationally and within the international community in NATO, in the European Union, and so forth.

INTERCONNECTION AND COOPERATION IS THE BEST RECIPE FOR FUTURE PEACE

The message I would like to leave with you today is that interconnection is fundamental to solving certain issues. More than sharing security, interconnection means cooperative security. This is key. If you look at areas of the world where crises and wars tend to develop, they are usually areas of the world that are the least connected. The more disconnected they are, the more likely they will be to be involved in future crises and wars. So expanding our connections, opening up without naïveté but opening up nonetheless, and not letting the ghosts of the past haunt us, is in my view the best recipe for solving problems for the years to come.

Chapter 3

Cybersecurity: An Industry Perspective

Mr. Giuseppe Orsi
CEO, Finmeccanica

First of all, let me thank you for the invitation to this international workshop, which is of great importance for global security. Security is a key domain and a core competence for Finmeccanica. It is part of our mission and one of our strategic objectives under business, technology, products, and service viewpoints. Our group has significant operations in Europe (Italy and the U.K.) as well as in the U.S. as part of our electronics sector.

A FEW WORDS ABOUT FINMECCANICA

Finmeccanica, with €17 billion in revenues and 70,000 employees, is today the eighth group in "aerospace and defense" worldwide and the second in Europe for "defense and security." Its total R&D spending in 2011 was just above €2 billion, of which over 40% was in the electronics sector—the main driver for technology and product innovation in Defense and Security; specifically, Finmeccanica's R&D discretionary investments in the security domain were over 25% of its total electronics sector investments. This is particularly meaningful given the current world economic crisis, which has been accompanied by a decline in infrastructure investment and in view of the persistent uncertainty regarding future market perspectives.

INDUSTRY'S VISION FOR A SECURE CYBERSPACE

This workshop is focusing attention on the emerging threats concerning the security of critical infra-structures, particularly of ICT networks. Among these, infostructures currently present the most critical challenge. My speech will therefore depict the vision and attitude of industry at large, and particularly of Finmeccanica, in addressing the requirements related to an open but safe and secure use of cyberspace. I will also address what Finmeccanica is doing to contribute to the mitigation of these fast growing and pervasive cyber threats.

In the Information Age, Information and Communication Technologies (ICT) are the most powerful engine for innovation and modernization. They represent a key factor in the progress and well-being of any society, no matter what its level of development. However, we are also increasingly aware that these technologies need to be handled with a greater degree of attention; and when I say "handled" I mean designed, implemented, and managed, taking into consideration scenarios and requirements that only a few years ago would have been neither conceivable nor required.

Our dependency on ICTs is constantly increasing and, as a matter of fact, the main networks that sustain our daily life—electricity, gas, steam, water, transportation, financial processes, telecommunications, roads, information, and media—are de facto structurally dependent upon information technologies. As such, they represent a growing critical element of vulnerability.

STATISTICS ON THE CRITICAL VULNERABILITY OF OUR NETWORKS

To provide some numbers as to the level and growth of these threats, according to international studies, the Compound Annual Growth Rate (CAGR) of reported cyber incidents was 25% for 2005-2010. However, what about non-reported incidents? During the same period, the CAGR of new malware detected was five times as large: 125%! Moreover, the level of sophistication of malware has dramatically increased since then.

A recent working group study presented to the U.K. Parliament in September 2011 found that "the worldwide cost of

economic damages from malware exceeded $13.3 billion per year," a figure which is based on 2008 data. Thus today the cost is evidently even higher. The U.K. Parliament report also found that the "total worldwide security software market is estimated at $16.5 billion. However this estimate does not include the market for hardware security appliances, which are hugely popular, expenditures on security-related staff or consultants, and other security maintenance activities." Hence, the market is much larger than this.

Global cybersecurity spending is in fact expected to reach $60 billion in 2012 and is forecast to grow by 10% every year during the next three to five years, according to a PricewaterhouseCoopers (PwC) report titled "Cyber Security M&A: Decoding Deals in the Global Cyber Security Industry." The PwC report also found that the United States accounts for more than half of all deals globally related to combating cyberthreats and describes an increasing awareness of this among both organizations and consumers. The total deal activity since 2008 has exceeded $22 billion globally. In the first half of 2011, 37 deals accounted for more than $10 billion in value, representing a 70% increase compared with all of 2010. Since 2008, total investment in global cybersecurity deals has exceeded $22 billion, an average of more than $6 billion each year.

Given that modern society depends on information technology more than ever before, these numbers are expected to grow exponentially. We must therefore invest in cybersecurity in order to guarantee open and safe Internet access and the ability to operate in a cyberspace that has become essential to our daily life, progress, and well-being.

WHAT IS BEING DONE TO COMBAT THE CYBERTHREATS

The Escalation of Malware and the Costs of a Defensive Capability

Malware has escalated in terms of both the sophistication of attacks and types of attackers. The attackers are no longer just single hackers, rebellious teenagers, or criminal organizations but also terrorists—such as Anonymous, a massive, underground hacker and para-terrorist activist group—and states. Indeed, the media has widely reported that both the Russian and Chinese governments are thought to have infiltrated electric power grid computer systems in 2009 and the U.S. government publicly recognized its recent use of cyber strategies and cyber payloads against Iran.

This escalation of malware prompted the international community to also consider the matter from a cyberdefense viewpoint. In fact, after the 2010 Lisbon Summit, NATO defined cybersecurity/cyberdefense as "all the applications of security measures to protect Communication and Information Systems (CIS) infrastructure against cyber attack," with cyber attack defined as a form of cyber war intended to disrupt an adversary's CIS. These events occurred in the international framework and the initiatives of the main international and domestic organizations led to, once and for all, the identification of the domain of cyberspace as the new "challenge" field in defense and security in addition to the traditional ones (space, air, land, and sea).

Cyberspace is a virtual, huge, pervasive arena where subtle, silent, and lethal actions may be displayed by any number of players, where the investments necessary to obtain a defensive capability are much higher than those sufficient to create an offensive capacity able to become economically disruptive, or even destructive in physical terms. While in the short/medium term R&D and procurement expenses are destined to stagnate or undergo heavy reductions, analysts designate cybersecurity/cyberdefense expenditure as anti-cyclical, in a fast growing trend along with other measures related to global security such as the special forces, the ISR (Intelligence, Surveillance, Reconnaissance) and space capabilities.

The U.S. and NATO have made cybersecurity/cyberdefense a top priority in terms of their efforts to achieve capabilities in this new frontier of common security as soon as possible. Again, a few numbers: According to the U.S. Department of Homeland Security, the U.S. budget for 2013 is set at $769 million, up from the $459 million in 2012, to support the operations of the National Cyber Security Division. On top of that, the U.S. DoD requests in the FY2013 budget for cyber at large (i.e. not just limited to computer information systems and data protection) amount to $3.4 billion. These huge investments in the U.S. show the wide disparity with Europe's cyber security / defense pace, where the level of investments is much lower.

The U.K. is more advanced than any other European country under a strong initiative from the Prime Minister's Cabinet, which led to the creation of the Government Communications Headquarters (GCHQ). In Italy several initiatives have been launched but there is still a lot to do.

Fast and Continuous Evolution of the Domain to Protect

Cyber security has an additional element of complexity since the domain to be protected is in continuous and rapid

evolution. It is worth mentioning the emerging concepts of smart city, smart grid for energy distribution, infomobility applications, and the evolution of telecommunication and transportation infrastructures. Finmeccanica has knowledge of these emerging applications and their technological implications as we are also operating in those fields. Megacities are now a reality, they are attracting flows of people that now are in larger numbers than residents in the countryside, but they also risk becoming more inefficient and vulnerable. All these infrastructures cannot stop working, even in case a cyber attack should happen.

Protection is challenging as this means guaranteeing and assuring, in case of attack, an acceptable minimum level of "business continuity" and "quality of service" for such infrastructures, while remediation must take place immediately to rapidly revert to normality. The need for protection is therefore absolutely wide, concerning both the military and governmental sectors, ranging from MoDs and Intelligence agencies to national security agencies, through critical infrastructures and public administrations and the large sector of small–medium–large business enterprises, eventually up to each single citizen.

The market is therefore wide and the investments are destined to grow. However, it is wise to look at the opportunities of this new market with attention and caution. As I have already said, today's investments in Europe in this sector lag behind those in the U.S. and have not reached yet the anticipated volumes, perhaps due to the global economic crisis which is reducing the resources available since they may be allocated to other priorities.

Finmeccanica's Response to Cybersecurity Requirements

In this scenario and with the perspectives that I have outlined, Finmeccanica companies that operate in the electronics sector have nonetheless managed to meet the rapidly-evolving cybersecurity requirements. In this respect, Finmeccanica benefited from its long engagement in the field of defense and security technologies, particularly electronic warfare, secure communications, and industrial automation systems (i.e. the SCADA systems widely used in the management and control of critical infrastructures like the electricity transmission and other distribution grids). Our offering is effectively responding to the cyberspace security demand. In the area of information assurance, the group's companies have reached full autonomy in terms of skills and competencies to develop cyber projects and/or to manage security at large.

Let me provide some details:

- *Analysis and assessment of the vulnerability of infostructures.* The group can leverage its cross-domain knowledge which encompasses several complex and critical applications from C4I through complex ATC/ATM up to railway signaling systems. A specific distinctive element is represented by MIGRA which is a proprietary methodology and product tool for risk analysis/vulnerability.
- *Design and provision of security architectures for legacy and new systems.* We have experience with a range of large-scale systems and can therefore implement interoperable architectures which assure cyber resilience and data protection for legacy and new systems.
- *Detection and analysis of cyber attacks.* We have in-depth knowledge of malware, which permits us to tailor the most appropriate and prompt response. In such a context, we manage a proprietary malware database which is constantly updated.
- *Modeling and simulation.* Both are intended to support the development of new operating concepts and also for training purposes. We have developed special techniques which complement modeling and simulation applications in other domains.
- *Proprietary products.* These include both hardware and software.

In addition, we have two security operation centers, one in the U.K. for restricted networks and one in Italy for IT security and unclassified and sensitive domains.

We have been working since the beginning of 2000 to deliver cybersecurity services to government institutions, telecommunications operators, banks, public administrations, critical national infrastructures, and many clients in the private sector. Today, we have over 2,000 customers in total. The expertise and capabilities gained by the group so far was confirmed by NATO's recent assignment of a major contract to SelexElsag, a wholly owned subsidiary, leading a Finmeccanica cybersecurity team with Northrop Grumman as a partner. The tasks under this contract concern the cyber resilience of the computer information systems of the Alliance and the protection of data, both classified and unclassified. Under this contract, the Finmeccanica cybersecurity team shall provide NATO and its more than 50 commands in 28 countries with the capability to detect and respond to cyber incidents across its data networks.

In total, the group has more than 600 specialists, including contractors, operating in information assurance and cyber,

generating an average revenue of €120 million year, with discretionary investments in the order of €20 million in 2011. Such a capability in terms of specialists and related skills is ultimately one of our major areas of development and investment. There is really no technology substitute to well-trained, experienced cyber specialists and operators, who have accumulated an in-depth understanding of the problem space. Because these skills are so difficult to develop, it difficult for most corporate or government IT network operators to internally generate the level of capability that would be required for effective protection. This is why we have been operating Cybersecurity Operations Centers (SOCs) for more than a decade and expanding our customer environment. We are now very keen to collaborate with academia, possibly in conjunction with users, to create fertile conditions for setting up jointly specialized cyber schools/courses.

Other investments underway in this sector are:

- R&D in Intelligence gathering, particularly new algorithms and advanced correlation techniques for massive search on open source data (we are talking about near real-time analysis of terabytes of data!) and dynamic risk assessment based on high performance computing.
- Definition of improved protection criteria, interoperability standards, and certification procedures.
- "Built-in" cybersecurity as embedded/native within systems and products.
- The group very actively participates in international fora and collaborates with universities and research centers.

Finmeccanica is also playing an important role through its collaboration with the key cybersecurity/cyberdefense stakeholders. We chair an international NIAG Study Group under NATO Emergency Security Division sponsorship to address proposals for better and more effective cooperation among NATO, its member states, and the private sector at large. We are cooperating with the Italian MoD in the framework of the ongoing Multinational Experiment Program 7, better known as MNE7, which deals with the new Global Commons of cyberspace. The U.K. is the custodian of the overall Cyber Space Global Common package, with Italy responsible for the legal framework package. We have recently concluded an arrangement for the FFCI (Framework for Cooperative Interaction) with NATO ACT (Allied Command Transformation Norfolk) to investigate innovative techniques for dynamic risk analysis. We also chair the Task Group TISP (Trusted Information Sharing for Partnership) within the NATO RTO (Research Technology Organization) to define requirements and the architecture for "information exchanges" between different security domains (Multi-Level Security). Finally, we are part of the "Hub and Spoke" initiative in the U.K. where we have responsibility for cybersecurity for the node of the aerospace and defense supply chain and IPR.

CONCLUSIONS

A threat developed in and disseminated throughout an open system like the Internet cannot be neutralized in isolation. It has such fine granularity, high "pervasivity," and "mutant genes," that a collaborative approach and a specialized new doctrine are not just an option—they are a must! Cyberdefense therefore requires institutional organizations to have an innovative approach to the development of unconventional concepts and "non-traditional" doctrines, as the cyber threat is more than asymmetric. The vast dimension of the net requires comprehensive Intelligence-sharing to ensure effective cyberdefense, which means that we need an improved mindset, an evolution from an individualist "need to know" approach to a collaborative "need to share" environment. Transparency and trust are essential in addressing and implementing an effective collaboration. When addressing vulnerabilities in cyberspace, we all definitely benefit from close collaboration across institutions, international organizations, academia, and the private sector. Emphasis should be progressively given to preventive measures rather than to adaptive and remedial ones only.

However, in this whole context we must work hard to arrive at a cyber ecosystem whose legal framework is, to the extent possible, acknowledged worldwide, accepted and adopted in a spirit of trust, with norms of behavior in place specifically for cyberspace. This is clearly recognized by the U.S Administration, which has recently engaged broadly with the Chinese Government on cyber issues to find common ground. The U.S. has received positive feedback from Chinese Defense Minister Liang Guanglie who said "China stands firmly against all kinds of cyber crimes." Finally, Finmeccanica will continue to contribute to and improve global security through its expertise, technologies, products, and services by engaging in proactive efforts to promote and support trusted collaboration between different stakeholders and across borders.

Chapter 4

The Middle East and the Balkans: The Perspective from Albania

His Excellency Dr. Sali Berisha, Albanian Prime Minister

First, let me thank the workshop Chairman, Dr. Roger Weissinger-Baylon, for the invitation to address this audience. I would also like to thank our friends, President Giorgio Napolitano, and Defense Minister Giampaolo di Paola, under whose auspices this international meeting on security is held, for their hospitality. This year, Albania celebrates the 100th anniversary of its independence. One hundred years ago, our nation was facing the predicament of "to be or not to be," when the great powers of that time thought it should not exist as a political concept. Yet, it is now a fully fledged NATO member; the day our flag was raised in Brussels was for me a very exciting and historic day. Furthermore, Albania is presently chairing the Council of Europe, the oldest democratic institution of our continent. We received the presidency from the oldest European democracy—the British government—something which has great symbolic significance.

Today, we live in interesting times. After the fall of the Iron Curtain, NATO demonstrated the will to forge a new dimension centered on protecting human rights. Bosnia and Herzegovina is a free and united country. Kosovo is free and independent. Last week, Libya held its first free and fair elections. All of us were deeply saddened to witness the bloodshed in Libya, but the best reward for those who fought and died for freedom were these elections and, obviously, it was worth the price paid. Otherwise, power would have passed from one heir to another, from Gaddafi to Saif, from Saif to Saif II. The United States used its power to overthrow the two most terrible dictators of our time, Mullah Omar and Saddam Hussein.

THE SITUATION IN SYRIA

Another cruel dictator is challenging the free world, and his name is Bashar al-Assad. I see no major differences with what happened in Bosnia, Kosovo, or Libya: a dictator, who had the opportunity to undo the legacy of his father, failed in embracing reforms to democratize his country. Instead, he followed in his father's footsteps and adopted the same policies of cruelty and oppression. He represented a minority in all aspects—in the population, in the regime, everywhere. Thus, the Syrian people are today calling for us to help them. Without setting a no-fly zone, the bloodshed and cruelty of the regime—which is better armed and more powerful than the opposition in many respects—makes it very difficult for the insurrection to get rid of this new Milosevic, this new Saddam, this new Gaddafi and son of Hafez al-Assad.

Albania, in its current role as chair of the Council of Europe, is trying to work with these countries and to use the chairmanship to bring these countries closer to the Council of Europe, which is an excellent institution with an extraordinary record. The Council of Europe's Venice Commission is undoubtedly the best think-tank for the drafting of constitutions, with experience ranging from South Africa to the former communist countries. Other units and departments of the Council of Europe can also be very useful for Lebanon and other Middle Eastern countries.

Albania is trying to work bilaterally through the Council of Europe as well. For decades, many Middle Eastern peoples have been told that they are not members of democratic nations because Islam is not compatible with democracy, which is a false dogma. We in Albania are a multi-religious country. We provide a strong example—which Middle Eastern countries are interested in—demonstrating that Islam is fully compatible with the rights and universal freedoms of democracy. I believe that, despite the controversies, the Muslim Brotherhood in Egypt and the liberal forces in Libya, which are beneficial for these countries, are an important step toward a democratic system.

Their path will not be easy; it will be even more difficult than our own has been. We came from a terrible darkness. Nobody can possibly imagine where we started from. Let me provide an example. According to World Bank statistics, in 1992 Albania was the third poorest country in the world, along with Angola and Uganda, with a per capita income of 204 U.S. dollars. But we were fortunate because we had models from which we could learn and which we have adopted. We were surrounded by democratic countries, by friends who helped us, and without that help, without that solidarity, without that tremendous support, our path would have been much longer and far more difficult.

These countries need models and the problem is that they have to find theirs in the Mediterranean coast. Offering models could be of great importance. I believe that the great changes which began during the Arab Spring will continue. I believe that Middle Eastern peoples will now be ready to cope with the complex and often debilitating conditions brought about by many decades of oppression prior to the Arab revolutions. Moreover, the fewer the number of dictatorships in the world, the safer it will be. Safety is a complex and multi-factorial issue, but I believe that the most consolidated path towards it is a free society, based on the rule of law and a democratic system.

THE SITUATION IN AFGHANISTAN

Albania takes part in operations in Afghanistan, with 350 troops in the country. We are there in all roles, from combat forces to the OMLT (Operational Mentoring and Liaison Teams). I visited that country and in my opinion, Taliban forces have no chance of prevailing. NATO is in control of the situation and the recent Strategic Agreement signed between the U.S. and Afghan governments is a major development in terms of ensuring the security and freedom of the country. This is extremely crucial. Moreover, the donor conference in Tokyo was a great achievement, with $60 billion in donations collected for Afghanistan.

But there is another Afghanistan, one in which terrible conditions prevail, an Afghanistan with survival statistics that are among the lowest in the world. To give just one example: Mortality in my country is 8 per 100,000 births; in Afghanistan it is 1,400 per 100,000 births. This, alongside a number of other indicators, reveals a desperate situation in which uncertainty and risk are very high on a daily basis. Thus, I hope that the funds collected at the donor conference will be used to help pull the country out of the medieval environment that persists throughout much of the country.

Engagement in Afghanistan is an engagement toward peace, stability, and security in the world. Free nations therefore have a vested interest in helping the country; I even think a global coalition would be worthwhile. There is also another factor which is drugs. Drugs are everywhere in Afghanistan; when traveling through the country, the first things that one sees are the vast drug fields under cultivation. Thus, the struggle to extricate this country from drugs is a fight for the security of our countries, a fight for the health of our children and of our societies.

I believe the world is much safer today than it was several years ago. And that is because men such as Mullah Omar and Saddam Hussein are no longer a threat to global security. Our soldiers strongly believe in their mission and its vital importance and thus are willing to face multiple risks in their work each day.

THE BALKANS

As to the Balkans, no region in Europe has changed more. From an old-fashioned region, it has metamorphosed into one where all governments are elected democratically. From a conflict-prone region, it has become one of cooperation and understanding. This progress is the result of your countries' many efforts to help our nations and our region. But some problems still remain. For those of us who live in the region, what is most important is to understand and accept that these changes are irreversible and that time cannot go backward.

Several weeks ago, the international community decided to end its supervision of the young state of Kosovo. During the 14 years since its independence, the rule of law in the country has been strengthened and Kosovo is increasingly recognized in international forums. Brussels negotiated an important agreement between Kosovo and Serbia which paves the way for intensive regional cooperation. I believe that the acceptance of existing borders is crucial to peace and stability in our region. Any attempt to revise the borders will generate tensions and even conflicts which will take many years to resolve.

There are a number of minorities in Kosovo, including the Serbs. Surprisingly, however, the majority of Serbs who live south of the Ibar River live in peace and harmony with the Albanians, while the Serbs who live in three municipalities to the north of Mitrovica—where there are very few Albanians—experience considerable unrest. Yet this comes at a time when no one is attempting to harm them or to limit their human rights. Indeed, smuggling is the main problem in these three municipalities. The smuggling also involves everyone: Albanians, Macedonians, Bosnians…This has been allowed to happen because of the government's lack of control. Clearly, the problems involving these three municipalities must be resolved in accordance with international law in order to ensure that Kosovo's borders and territorial integrity are respected.

Belgrade has a new government, and despite some of their previous unhealthy statements, we are interested in continuing our efforts toward further regional integration. Indeed, Albania has established good relations with its neighbors. We also fully support the region's integration into NATO. Furthermore, Albania is working hard to move closer to the European Union.

Chapter 5

Addressing the Urgent Regional Security Challenges in Southeast Europe and the Black Sea—The Bulgarian Perspective

His Excellency Anu Anguelov
Minister of Defense of the Republic of Bulgaria

It is a pleasure to present the Bulgarian view on the security challenges in the strategically important Southeast Europe and Black Sea regions. Both regions are of importance to the security of the Euro-Atlantic area—as explicitly mentioned in the NATO Chicago Summit Declaration—and both are a priority on the Bulgarian foreign policy agenda. By encouraging political and economic reforms, the EU and NATO are playing a constructive role for building stability and regional cooperation. But cooperation efforts can sometimes be hampered by factors such as uneven economic and political developments among countries and nationalist forces. Therefore, the regional players need to address common problems jointly and imperatively foster sound policies that will strengthen dialogue. Progress has been made so far and we firmly believe that we are moving from sharing common histories of conflict to sharing common democratic values such as the rule of law, fundamental freedoms, human rights, and good governance. The very prospect of Euro-Atlantic integration, which would eventually bring us to our common goal of well-being and prosperity for our nations, plays an important role in the region's stabilization and institution-building processes. The Chicago Summit confirmed this Euro-Atlantic perspective for four aspirant countries—Georgia, Bosnia and Herzegovina, Macedonia, and Montenegro—and, although no decisions have been made, we believe that a new wave of enlargement will take place, hopefully sooner rather than later.

FOUR KEY SECURITY ISSUES FOR OUR REGION

In this context, let me share some observations. First, there is no immediate threat of armed conflicts in Southeastern Europe and the Black Sea Region. The fact that, until recently, international military forces were needed to ensure peace and stability while today they only play a supportive role for the respective national security forces is strong evidence for this. A clear example is Bosnia and Herzegovina. Given the country's progress on the road to stability, Bulgaria is planning to withdraw its military contingent in accordance with the restructured OPLAN of the mission as of September of this year. At the same time, we will remain ready to quickly dispatch a reserve company if necessary.

However, today the national security of the states in these two regions is not solely characterized by its military dimension. Positioned at a strategic crossroads, both regions are vulnerable to residual ethnic tensions, "frozen conflicts," insufficient institutional capacity, terrorism, organized crime, cyber attacks, potential disruption of the flow of energy resources, illegal migration, etc. The diversity of risks requires a new approach to their prevention.

Secondly, problems can no longer be resolved by a single nation acting alone. Moreover, the failure to understand the necessity of cooperation will create a "security vacuum." Both regions have well-established formats of cooperation that have led to positive changes, but they were conceived in the Nineties in a different strategic environment that was dominated by ethnic strife and military conflicts and mainly played a confidence-building role.

Instead, regional cooperation should be a dynamic process that reflects the developments in the strategic environment. We must adapt the existing formats to make them more operational and better able to face the rapidly changing security environment. In some formats we could invite representatives from different ministries and agencies. Another approach could be to identify the best format to deal with new threats, such as cyber terrorism, that are not covered by the existing formats.

Given the mounting number, complexity and sophistication of cyber attacks and their potentially highly disruptive impact, we should review some of the existing formats in order to accommodate a cybersecurity function. We are already working in Bulgaria to set up a national cybersecurity center with expert and operational functions and will take advantage of the experience of our NATO Allies, in particular the Cooperative Cyber Defense Centre of Excellence in Estonia.

Another good example is our proposal to permanently host on Bulgarian territory the staff of the SEEBRIG multinational brigade within the framework of the Southeastern Europe Defense Ministerial Process (SEDM). These changes will significantly increase the operational capability of the brigade, save tremendous resources for its maintenance, and give a real impetus to its future functioning.

Thirdly, today's complex threats to the stability of the two regions require an inter-institutional approach to tackle them. Given the complexity of the challenges and the enduring financial austerity, Bulgaria has determined that more coordination and synergy among all relevant national agencies as well as intensified international cooperation is needed. Hence, in our 2011 National Security Strategy, we have developed an integrated inter-institutional approach to deal with today's multiple challenges.

Such an integrated inter-institutional approach would be very functional and helpful if applied on a regional basis too. If we are to successfully find solutions to our common challenges, interagency coordination among the national security sectors of all countries in the region is indispensable. It would save efforts, be cost-effective and provide a common viewpoint on the problems that affect all of us.

Fourth and more importantly, we must guarantee a secure and stable environment across the region in order to deal effectively with the challenges to our security. For instance, the region has the unique potential to become an area of prosperity and stability because it is a "bridge" between Europe and Asia but, due to the existing security risks, many economic, transport, political and energy projects cannot be implemented. This situation negatively affects the social-economic development and trade links in the region and, in turn, brings additional insecurity.

These challenges, which concern the states where conflicts exist, also threaten the security of neighboring states. Thus the regional conflict potential that remains runs against our efforts to ensure diversification of sources and lines of supply and reinforces our dependence on the already existing ones. These problems can only be resolved through comprehensive solutions within the framework of multifunctional formats. To guarantee uninterrupted supply, among all other measures, critical infrastructure protection must be high on our regional security agenda, among other measures. And we must also consider establishing new forms of cooperation in this sphere.

THE FINANCIAL CRISIS MUST NOT BE ALLOWED TO CREATE A SECURITY DEFICIT—THE NEED TO BUILD DEFENSE CAPABILITIES IN NEW WAYS

Another challenge is the financial crisis. It is reflected in reduced budgets and the field of defense and security is no exception. We cannot risk having the financial shortage translated into a security deficit. Therefore, we must look at building defense capabilities in a dramatically new way by combining our resources and acquiring capabilities that can be used jointly. This would cut costs for security while at the same time bringing added value to our common defense potential. For example, Bulgaria is planning to host a NATO Centre of Excellence (COE) for Crisis Management and Disaster Relief that could support our neighbors' efforts to improve their capabilities to deal with such contingencies. Our vision is that, through joint training and joint use of infrastructure and facilities, we can both enhance the level of our cooperation and improve our capabilities. In times of economic austerity, we must avoid duplications and seek multinational solutions.

Here I would like to call your attention to one more "smart" regional solution—the "air policing" agreements within the NATO Integrated Air Defense System that we have with Greece and Romania. We will soon have a similar agreement with Turkey. Such cooperation, which is based on political will, is mutually beneficial, including economically.

Another good example of a "smart" approach is the Naval Coastal Surveillance System (EKRAN) that was developed by the Bulgarian Ministry of Defense as part of the national integrated coastal surveillance system. This system is an example of the simultaneous use of one single system for guaranteeing the different dimensions of security—military, security of supply lines, counter-terrorism, fighting illegal trafficking, etc. At the same time EKRAN is becoming an example of a regional solution as well since we are ready to jointly use it with other national systems of this type.

Throughout history there have never been times of absolute peace and predictability but today, we have a chance to find together joint and effective answers to urgent challenges. Here I will refer to the last NATO Summit in Chicago in May, whose agenda serves our purpose. The decisions the Allies took regarding capability development and hence the ability to deploy in operations will permit NATO to successfully tackle all challenges irrespective of economic constraints. The Summit also emphasized the growing importance of further developing our partnerships, including those with all our Black Sea neighbors.

Turning challenges into opportunities has to become our guiding motto. I believe that together, Allies and partners, we can make it happen and the sooner, the better!

Chapter 6

Security, Prosperity, and the Internet

His Excellency Zlatko Lagumdzija
Deputy Chairman of the Council of Ministers and
Minister of Foreign Affairs of Bosnia and Herzegovina

Since I was introduced as an engineer, I will say a few words from an engineering perspective. I will also make some comments from a social perspective in my role as a Foreign Minister and, of course, from a regional perspective with a little flavor of Bosnia and Herzegovina as the heart of the region or, perhaps, the door to the region.

By education, I am a computer scientist. I have been in politics for 20 years. I was 35 years old when the Berlin Wall fell and I watched it on CNN as a research professor at an American university, with absolutely no idea that politics would change my life. As a computer scientist, I had always thought that life was essentially an engineering thing, but when I saw those bricks falling in Berlin, I realized that sooner or later those bricks were going to hit those of us who were caught in between in the former Yugoslavia, in the area of Bosnia and Herzegovina. I felt caught in between because I was born and raised in Sarajevo, my home city, and I realized that those Berlin Walls—those bricks—were going to hit us in Sarajevo sooner or later. It was sooner than expected. When I came back to Sarajevo, I joined the political arena—because I learned from systems theory that when one system is falling apart and there is no other system to take over, a vacuum is created. And, in a vacuum, a lot of things can happen, especially in a social sphere. Of course, over the last 20 years, I did not want to spend my time exclusively in politics. That is why I shifted my interests from computer science to the economy, competitiveness, and the strategic use of information technology. I realized that technology has significantly changed the world. This is why I told my students that, as engineers, they could change the world by being good engineers. Unfortunately, the world cannot be changed by good engineers alone. Much stronger forces than engineering are needed.

And now I will get to the issue of cyber crime. There are six keywords that I will be discussing from my perspective in Bosnia and Herzegovina. One cluster of words is security, prosperity, and diversity. Another cluster, which I would like to discuss from a regional perspective, is about values, beliefs and technology.

SECURITY, PROSPERITY, AND DIVERSITY

I just want to clarify one thing about cyber security. As a computer scientist, I believe that technology is useless unless you put technology in the proper context and the computer is the only machine that, at the moment it leaves the factory, has no predefined purpose. In fact, there is no other human invention I know of that is not constructed with a clear purpose. Of course, you can take a hammer and, instead of hitting a nail, you can hit a person on the head, but a hammer was not invented for this purpose. It is intended to hit a nail. For this reason, when we talk about cyber security we should talk more about security than about the cyber aspect.

We heard a very impressive speech by Prime Minister Berisha. He spoke about his country's development in an economic sense over the last 20 years, which is really impressive. By the way, Albania is the country with the largest growth rate for Internet penetration among its citizens since the year 2000. The reason is very simple, because it began with a very small base. For the same reason, Bosnia and Herzegovina is number two in the growth of Internet use. In fact, over the last 10 years, the number of our Internet users has increased by 300 times! Unfortunately, the mind-set in our country still needs improvement. Just two or three years ago, a prestigious member of our parliament, after giving an interview to a journalist, could not provide his email address, since he regarded the Internet as something used mainly by secretaries or personal assistants who would print out his email messages on a printer for him.

My point is very simple. We are a country that is obsessed with prosperity, like everyone else. But we understand that the first precondition for prosperity is security. That is why the prime target of the present government of Bosnia and Herzegovina as well as any future government is security. And that is the reason for our three major priorities, which are the tools to achieve prosperity. They are: Regional cooperation, NATO accession, and EU enlargement.

In other words, we want to close down the MAP for the countries that are now missing in southeastern Europe. So for those of us living in this part of the world, these three tools are the way to achieve our real goals—namely the social and economic cohesion of the country—in order to achieve prosperity.

Over the last 10 years, something has significantly changed among the younger population. Bosnia and Herzegovina is a country that is rich in history and rich in diversity. Some people call it a "one-two-three-four-five country," i.e., *one* state overseeing *two* entities, *three* major ethnic groups, *four* million people, and *five* levels of government between the individual citizen and the head of state.

VALUES, BELIEFS, AND TECHNOLOGY

But our diversity is something I will correlate with the growth in the penetration rate of the Internet and the penetration of social networks. The new generations are experiencing that diversity in a very different manner from their parents via the social fiber of technology. At any moment, they can be anywhere in the world with everyone that they want to be with. They realize that the differences and diversities among our four million citizens are very small, even though we were killing each other 20 years ago. Now they are experiencing and learning about diversity much differently and in a much better way.

Of course we do have one little problem on our path when it comes to different perceptions and ways of using of the Internet between generations. Perhaps I can best explain this by describing the difference between me and my 15-year-old son or my 25-year-old students. In the literature, they call them "digital natives." These "digital natives" are so accustomed to using technology that they can find everything on the Internet. Whatever the question, they feel that they can find the answer on the Internet.

And it is a little bit frightening that they are very efficient at getting the answer to anything because, the moment you give them a problem, they will Google it to find a solution. But for them, all that matters is the solution. In our generation, we are a little bit different, and maybe even old-fashioned because, when we Google a problem, we are also trying to find the reasoning behind the different solutions. We want to understand why something happened. What are the pros and cons? What are the consequences? So which generation has the better approach?

CONCLUDING REFLECTIONS ON COMPUTER TECHNOLOGIES

I will now close with one point from my favorite economist, Jeffrey Sachs. In a recent book, he suggests that we are living in a bizarre time that combines Stone Age emotions, medieval beliefs, and almost god-like technologies. And this worries me a lot. Accordingly, when we talk about cyber crime, we should be more concerned with the crime than the cyber aspect because computer technology is now so powerful that it resembles atomic energy, one of the great inventions of our time but with the potential to either create a devastating bomb or produce electrical power for a light bulb.

As a professor in a school of economics, as a retired engineer, and currently as a politician, it is appropriate for me to refer to an observation by Vaclav Havel in his Ottawa speech, when he said that we are the most complex creations on this planet, but we cannot create something more complex than ourselves. So when we strive to define democratic institutions that will make us act like civilized people, there are limits to the complexity of whatever we create. Perhaps this means that we must not seek to create the most secure technology possible, because it will lead to computers that will be of very little use—which is not the goal that we are trying to achieve.

Chapter 7

Security Challenges in Montenegro

Her Excellency Professor Milica Pejanovic-Djurisic, PhD
Minister of Defense of Montenegro

MONTENEGRO'S CURRENT SECURITY STRUCTURE

Security challenges in the present world come from different sources. Typically, they are the consequence of social, cultural, religious, economic, scientific and technological differences. From this wide range of challenges, we are particularly concerned by international terrorism; proliferation of weapons of mass destruction; unresolved border issues; religious and ethnic disputes; organized crime; natural and man-made catastrophes; economic and social problems and cyber crimes. Since these threats are transnational, no country can successfully deal with them by itself. Consequently, a global coordinated response is required, which represents a strong additional challenge.

Moreover, despite all the lessons learned and the wealth of experience that has been acquired, global security at the beginning of the 21st century is growing more complex. In democratic and organized societies, citizens' interests reflect changes in their common civilization. Responding to these interests brings numerous challenges and risks. This means that every country needs a security doctrine and operational strategy for protecting its fundamental interests and values.

Montenegro's current security system is framed in a new Montenegrin Constitution and generally matches the high international standards that are required for the process of European and Euro-Atlantic integration. In Montenegro's security system, contemporary challenges, risks, and threats arising from globalization are recognized and adapted to, which includes dealing with rapid change, complexity, and reduced geographic distances. While previously the threat to territorial integrity and sovereignty was predominant, the primary threat is now to the security of our society.

In order to be compatible with modern international security systems, Montenegro is approaching the EU and NATO and committed to following contemporary trends and democratic processes, which will raise the common level of national, international and global security.

FOUR CHALLENGES: THE GLOBAL FINANCIAL CRISIS, ILLEGAL MIGRATION AND SMUGGLING, TERRORISM, AND THREATS TO CYBER SECURITY,

At this moment, countries in our region are also faced with the global problems of the financial crisis, illegal migration and smuggling, terrorism, and threats to cyber security. These "Big Four" problems require the best possible response, so that we can create our own future in accordance with realistic possibilities, our individual capabilities, and in cooperation with our partners.

- *Dealing with the financial crisis.* As to the financial crisis and its consequences, it is our impression that, despite less than optimistic predictions, we have achieved significant results in the most recent period. Montenegro's achievements this year also include the decision to open European Union accession negotiations, receiving a message of encouragement at the last NATO Summit in Chicago, and we attained membership in the World Trade Organization. These are the best possible acknowledgments of our country's credibility on the regional and international levels. In its business environment, Montenegro has come a long way in its sixth year after regaining its independence. We are continuously working on stabilizing and maintaining economic growth while fulfilling international and national targets and goals and seeking potential foreign investors.
- *Dealing with illegal migration and smuggling.* In this context of improving our economic stability, the issue of illegal migration is serious. Illegal migration is a global problem that we cannot approach in a limited way by restricting our efforts to specific regions or groups. Accordingly, Montenegro is trying to achieve the standards that are required by our

foreign policy goals. In that context, the EU's decision three years ago on visa liberalization was a clear confirmation that we, as a country with a European prospective, have everything needed to meet the necessary criteria. At the same time, Montenegro is undertaking further steps so that we are not perceived as a transit country or one that is unable to guarantee the security of its own borders. We also undertook significant steps to prevent the expansion of smuggling, not only to meet international standards and norms, but also to permit Montenegro's own economic, social, and overall prosperity. As a responsible member of the international community, Montenegro is committed to cooperating and contributing to the fight against all different types of crime.

- *Implementation of our strategy for preventing and fighting terrorism, money laundering, and terrorism financing*. In order to prevent and fight terrorism, money laundering, and the financing of terrorism, Montenegro is developing a National Action Plan. We are upgrading this inter-institutional cooperation mechanism in parallel with the creation of a legislative framework, in order to respond to organized crime in a more functional and effective manner. These efforts have been very successful and are reflected in an overall decline in crime of almost 7% percent last year relative to 2010. Moreover, the most serious criminal offenses dropped 7.4%. In fact, Montenegro had the lowest crime rate in Europe (10 reported cases per 1,000 citizens). Nonetheless, in order to fight narcotics smuggling we are constantly conducting international investigations in cooperation with regional police services, European Union countries, and other relevant international organizations.
- *Dealing with cyber security.* At the present time, since such a large part of everyday operations relies on information technologies, security issues have become extremely important. In fact, information security surely presents one of the most challenging issues of this century. Accordingly, it is our common responsibility to strengthen the legislative framework concerning cyber security and establish institutional mechanisms to permit effective responses and coordinated action on national and international levels. In order to protect cyber space, the coordination of national security strategies, cooperation between public and private sectors, and engagement of all actors must become a high priority.

MONTENEGRO IS READY TO BE AN EQUAL PARTNER

Accordingly, we may conclude that Montenegro's current level of stability and security meets all preconditions for working effectively as an equal partner with international security structures. We have the ability to respond to all security challenges in our own country and in the international environment as well. Since finding solutions to global threats is our common priority, Montenegro is ready for further improvements in this sector, with help from the substantial cooperation and interaction that our partners are already providing.

Chapter 8

The Western Balkans: A Vision for Regional Cooperation

His Excellency Dr. Fatmir Besimi
Minister of Defense of Macedonia

It is a pleasure for me to participate in this 29th International Workshop on Global Security here in Rome since the workshop is an excellent forum for exchanging views on global security policy. I would like to take this occasion to share with you my vision for regional cooperation in the Western Balkans as a way to cope with the impact of the global financial crisis in the defense sector. Our earlier discussions about the financial crisis, illegal immigration, smuggling and cyber security, showed that there was only one single denominator, i.e., all these issues are internationally connected and interdependent and they require a global response through global cooperation.

THE SITUATION IN THE BALKANS

In the last 10 years, the Balkan region has achieved peace and stability but the challenge is to make this stability sustainable. The region has become an exporter and contributor to peace instead of an importer of peace as it used to be. Today we have seen how destructive a conflict can be, but we can also show that we can work together if we look forward to a joint future with stability and prosperity in the European Union and NATO. This is why Euro-Atlantic integration and the speed of this process are essential to the peace, stability, and development of the Balkans. It should happen as fast as possible since there are still challenges ahead—the issue of the Macedonian name and the situation in northern Kosovo and in Bosnia with the challenge of effective governance. Any delay in this integration process will affect investment and development in the region, especially during this period of financial and economic crisis, and create more space for radical political options with nationalistic agendas. I must emphasize that we have seen the epilogue of such policies in the recent past.

So, we have an opportunity to look forward and, as a region, to move towards NATO and the EU. This requires efforts in three areas—national reforms, regional cooperation, and Euro-Atlantic integration. Macedonia is an active player in these three areas and we are working towards our goal of promoting the values of freedom and democracy.

THE WESTERN BALKANS

In the Western Balkans, globalization and economic integration have let the financial crisis affect the region since all processes are interdependent, all economies are affected, and, hence, our defense budgets are affected. An analysis by the *Economist* presents some facts about the economic implications of the European economic crisis for the region. In 2009 the GDP in the region decreased by 5.2%, and in 2010 it decreased by about 0.4%, while in 2011 the GDP increased by 1.9% and the projection for 2012 is that it will increase by an additional 0.7%.

Illegal Immigration and Smuggling. We may say that the region is a transit path from the east to the EU countries. Technically, we have regional cross-border cooperation and biometric passports that help deal with this problem in the region. However, the long-term solution is to address the reasons for this immigration such as its social, economic, cultural, political, security, and demographic aspects. Therefore, Euro-Atlantic integration and the values that NATO and the EU promote for peace, stability, and prosperity should also be more effective for countries that are at the origin of this immigration.

Cyber Security. With its new technology and the world of the Internet, cyber security represents the challenge of the 21st century. It is about the balance between access and security of information. It is also about who the main player is for providing cyber security: Is it government or is it the private sector? There is a plan to open the European Cyber Crime Center in January 2013. We deeply appreciate this initiative because it will create a good base to boost cooperation between

the countries in the region and the rest of Europe. Let me share with you some information from a Eurobarometer survey about Internet use and awareness about cyber crime: 12% of those surveyed have experienced online fraud, 53% do not change their online passwords, and 89% avoid disclosing their personal information. In addition, 74% believe that the risk of cyber crime is increasing, 53% buy online, and 52% use social networks. Finally, 59% do not feel that they are well enough informed about cyber crime. According to Eurobarometer, although the Internet is used and needed, there is fear about the possibility of fraud and users are not well informed about the risks. The survey also considers that people should be better informed, and the more informed they are, the more they are ready and willing to use the Internet. If they are not informed they will simply not use the global network. So, the solution to the dilemma of increasing Internet control without reducing its openness and access may be to inform people of the risks connected to cyber crime so that they can by themselves find a way to be protected and be active players against cyber crime. Hence, fighting more effectively against cyber crime will require cooperation between government and industry and making sure that individuals are more informed about the risks from cyber crime.

CONCLUSION

In conclusion, the world is becoming more complex and the challenges are becoming bigger. Solving these challenges requires a coordinated approach and networking: The response to GLOPLEX (Global Complexity) is GLONET (Global Network). In this context of mutual challenges and joint solutions, we are fully committed to promoting the new NATO "Smart Defense" concept and the EU "Pooling and Sharing" initiative. We also intend to develop greater operational capabilities in order to achieve closer cooperation with our partner countries. Our country and the region as a whole are open to cooperation and we have managed to move forward despite the challenges of the past, proving that Euro-Atlantic integration is our best prospect. We seek to achieve this strategic goal by maintaining good neighborly relations, exchanging experiences, and providing support to the entire region by jointly promoting democratic and economic development.

Chapter 9

Cyber War and the Georgia-Russia Conflict

His Excellency Giorgi Baramidze, Vice Prime Minister of Georgia

THE GEORGIA-RUSSIA CONFLICT

The Georgia-Russia conflict illustrates both conventional and cybersecurity challenges in Europe. In August 2008, the Russian Federation invaded and occupied 20% of our territory and conducted ethnic cleansing by expelling 80% of the population from the occupied territories—Abkhazia and the Tskhinvali region. But this aggression goes far beyond the mere occupation of the two regions:

- First, Russia is trying to regain its sphere of influence in the region.
- Second, Russia is reacting to the democratization process in its vicinity. What the West celebrates as democratic progress in Georgia, Russia sees as geopolitical and ideological encirclement.
- Third, Russia wants to stop Georgia's movement towards NATO and thus impede NATO's Eastern enlargement. President Medvedev stated that, without the Russian actions of 2008, "the geopolitical arrangement would be different now; [Georgia] and a number of countries which [NATO] tried to deliberately drag into the Alliance would have most likely already been part of NATO now."

CYBER ATTACKS AS WARFARE

Russia is employing 19th century methods of great power competition for resources, spheres of influence, and territory. The August war also showcased Russia's use of new methods of warfare and created a precedent as the first cyber-kinetic war. This new element in Russia's political-military strategy combined land invasion with close coordination of an orchestrated online cyber offensive. It appears that Russia had been preparing to use asymmetric means well before the ground attack began. On July 20, 2008, a month before the actual military action, a series of cyber attacks were conducted against the website of the President of Georgia. It was a multi-pronged Distributed Denial of Service attack. (The information about this offensive was published by the Shadowserver Foundation and the U.S. Cyber Consequences Unit.)

The massive cyber attacks coincided with the Russian land invasion. The first targets for cyber attacks were the Georgian government and news media websites. After the invasion into Georgia grew in scale, the cyber attacks expanded to:

- More government websites—the presidency, ministries, court, parliament, etc.
- Media, forums and blogs—blocking not only Georgian news streams but other reliable media sources, such as the BBC and CNN. Russian information sources became predominant, which facilitated the spreading of disinformation.
- The National Bank of Georgia—cutting off its Internet connection for ten days and blocking many transactions. Accordingly, the cyber attacks caused extensive damage to Georgia's economy.

The timing and scope of the cyber assault clearly required resources and coordination on a scale that only a state sponsor could provide. The organizers had advance notice of the timing of the Russian military operations. When the cyber attacks began, they did not involve a reconnaissance stage, but jumped directly to the sort of packets that were best suited for jamming the websites under attack. Given the speed of action, the go-ahead must have been sent before the news media and general public were aware of what was happening militarily. Ninety percent of all gov.ge domain addresses and a significant fraction of .ge domain addresses were affected by these Distributed Denial of Service attacks. Investigations by the U.S. Cyber Consequences Unit provided evidence of a key role played by Russian organized crime—clues left in the registrations led to the address of the Russian Business Network (RBN) registered in St. Petersburg.

THE NEED FOR INTERNATIONAL CYBER ATTACK COOPERATION

Unfortunately Georgia is not the only target of the Russian cyber attacks. The 2007 cyber assault on the government IT

networks in Estonia, which coincided with the diplomatic spat between the Baltic state and Moscow, as well as the cyber attacks against Lithuania in 2008 and Kazakhstan in early 2009, are other vivid examples of the cyber threat. All these characteristics make the cyber campaign of the 2008 war a pattern that can be expected in an even amplified form in the future.

This experience showed that no single government is able to rely solely on its own resources in overcoming current challenges and threats to cyberspace. As cyber threats transcend borders, there is an urgent need for concerted international efforts to address them. In this respect, Georgia is determined to closely cooperate with international partners. Georgia is a member of the International Telecommunication Union (ITU) and also joined the Council of Europe Convention on Cybercrime.

I would like to underline that cybersecurity has become one of the key priorities of our relationship with NATO. On July 7-8, 2010, Georgia hosted the first NATO-led conference on emerging security challenges to discuss the nature of emerging security challenges and identify future fields of cooperation.

On a national level, Georgia has taken significant steps to actively address the challenge and to establish a comprehensive cybersecurity system:

- The Data Exchange Agency (DEA) of the Ministry of Justice was established.
- Under the DEA, the Computer Emergency Response Team was founded.
- A law on information security was initiated and became effective on July 5 of this year.
- Together with the National Security Council (NSC) and an interagency working group, the DEA takes the lead in developing Georgia's cyber defense capabilities. In June 2012, these three agencies elaborated the draft of Georgia's cybersecurity strategy.

Thus, for our part, we are intensely working on improving national capabilities for investigating cyber crimes and increasing cooperation on cybersecurity. There is a need to enhance a coordinated approach to cybersecurity that encompasses planning and capability development aspects in addition to response mechanisms in the event of a cyber attack.

GEORGIA'S ROLE IN THE EURO-ATLANTIC AREA

Georgia aims to support the principles of behavior in cyberspace and be the promoter of those principles in the region of Eastern Europe. To address the complex security challenges, Georgia's efforts are obviously essential but unfortunately not sufficient without the strong support of the international community.

In this process, a profound support of the EU and NATO, which are the central pillars of stability in the entire Euro-Atlantic area, is very important. We highly appreciate the adherence of the international community to a non-recognition policy toward Abkhazia and the Tskhinvali region. This confirms that, despite the Kremlin's efforts, the international community is unanimous with respect to the territorial integrity and sovereignty of Georgia.

However, let me remind you that Russia still avoids the full implementation of its commitments under the 2008 ceasefire agreement and we strongly advocate for more proactive measures by international institutions to oblige Russia to fulfill its obligations and to respect the fundamental principles of international law.

The president of Georgia unilaterally declared that Georgia will never use force to restore its sovereignty and territorial integrity against either occupational forces or their proxies and only retains the right of self-defense if the non-occupied part of the country comes under a new attack. Georgia has expressed its readiness for an unconditional dialogue with Russia and exercises a non-discriminatory policy towards Russian citizens: Russian businesses operate on equal conditions in Georgia and we try to facilitate good relations between the citizens of our two countries. Nonetheless, while the President of Georgia has proposed to unilaterally cancel the visa regime with Russia, the Kremlin wants to prevent Russian citizens from coming to Georgia.

Despite Russia's efforts to derail Georgia from the NATO membership path, our Euro-Atlantic aspirations are firm. Today, NATO-Georgia relations are excellent, as demonstrated at the recent NATO Summit in Chicago. Georgia is moving toward NATO membership, and we have become a reliable partner and an active contributor to Euro-Atlantic security. We have been participating in ISAF from its earliest days—around 1,000 Georgian soldiers are fighting in the south of Afghanistan, shoulder-to-shoulder with the Allied forces, without caveats. This autumn, Georgia will become the largest non-NATO troop contributor and the largest per capita contributor after the United States.

Despite the challenges, we are creating new opportunities in this part of the world. With efficient reforms across various fields, Georgia is becoming a modern, democratic state, which will benefit the entire region and have a positive impact on overall Euro-Atlantic security.

Chapter 10

Problems Never Occur One at a Time

Vice Admiral Ferdinando Sanfelice di Monteforte
Professor of Strategy, Università Cattolica (Milan)

At present, the most frequent complaint voiced by policy makers is that dynamics in international relations are accelerating; problems and crises are increasingly numerous, mostly intertwined, and therefore it is increasingly difficult to cope with such a continuous evolution. What nobody dares to add is that though this evolution was already underway during the many years of the Cold War, we did not pay attention to it, and therefore—to use a phrase from an Italian writer—"books on military strategy were left to fade on dusty shelves." Not only that, but basically too many people stopped using their own brains to look at the problems, and understand the reasons behind what was happening, which possible outcomes were in front of them, and how future contingencies could be tackled.

The "Cold War spleen"—i.e., the happy days when it was not necessary to use brains—is still lingering behind many statements about the world situation. As an old proverb says, too many policy makers end up thinking that "we fared better when we suffered from the past stringencies."

Not everybody, though, refused to consider the evolving situation in depth. In 2003, the European Security Strategy (ESS)—a most remarkable, albeit ignored document—was issued. Its title was already telling: "A Secure Europe in a Better World," and it included a thorough analysis of how the world situation was evolving. This analysis was so well-written that five years later, when an updated version was considered, it was found that there was nothing to be added, except for the scope of its "status of implementation."

The ESS included a notable phrase, most applicable to our times: "Taking these different elements together—terrorism committed to maximum violence, the availability of weapons of mass destruction, organized crime, the weakening of the state system, and the privatization of force—we could be confronted with a very radical threat indeed." It succinctly stated that no single threat is intractable and can be successfully tackled with perseverance and steadiness—a "concentration of purpose." When several of these elements are present simultaneously, thus needing to be faced at the same time, the situation can become explosive.

Lack of foresight is normally the cause of such a difficult situation, and our countries, having lived happily by forgetting the need to prevent problems, are now compelled to deal with a combination of challenges, risks, and threats. We are thus experiencing difficulties in extricating ourselves, but to overcome it we must reduce our weaknesses and increase areas of stability, development, and legality around us, in order to survive as nations in our ever-changing world.

The Balkans are a perfect example of this storm of elements: for too many years it suffered a sort of "strategic power vacuum," due to the explosion of longstanding hatreds, which were suppressed (and hidden?) under the cover of the confrontation between opposing blocs. When the blocs disappeared, what happened was just like when a coal fire is fed more oxygen, thus causing a huge burst of flames. Civil wars have always been the ideal environment for wrongdoers, and the Balkans were no exception. It took several years to cope with this emergency, and it is worth acknowledging that in these war-torn nations, statesmen have been able to slowly overcome the huge difficulties and to set up conditions for a better future for their people.

It is therefore with great pleasure that I have listened to the presentations today by statesmen, whose experience sets an example to be followed by all our policy makers on how to cope with present challenges, risks, and threats—crises, migration, smuggling, and cybersecurity—whose growth has more to do with our shortsightedness than we usually consider. They have much to say, and they can tell us a lot as to how we must improve in managing the world, which is not evolving faster than in the past: We must not deem that our ancestors were not confronted with a similar pace of events, quite to the opposite!

Chapter 11

Europe's Future Challenges: Four Areas for Concern

His Excellency Dr. Artis Pabriks
Minister of Defense of Latvia

THE NATURE OF CHALLENGES AHEAD

Let me start with two remarks on the nature of politics. First, I would like to refer to a very famous Italian, Niccolo Machiavelli, who said that "the important thing is to maintain a distance between reality and the illusion in which we live." Second, since I believe in universal values and in the universal similarity of humans, I would like to quote from a well-known Chinese thinker, Tseng Tzu, whose adage was "What is next? Before you make a step, always think of what will come next." To take an example from Afghanistan, in the public discourse we frequently hear that "when 2014 arrives and we hand over control of the country to the Afghan government, eternal peace will prevail." However, this is an illusion. The withdrawal of NATO troops from Afghanistan is not the end of the story.

There will be challenges of a different nature, of a mixed nature. I would like to describe four types of challenges that I see in the foreseeable future: (1) those driven by socio-economic hardships, (2) those of a technological nature, (3) those of a traditional or conventional nature, and (4) those connected with climate change.

THE SOCIO-ECONOMIC CHALLENGES

The European debt crisis currently at hand is directly connected with the disarmament of Europe. This, in turn, is forcing NATO and Europe to rethink their capacities—what they can and what they cannot do.

A related problem is the decline of Europe's soft power. Up until five or six years ago, we were accustomed to saying that countries like America have more hard power, but we Europeans can help dispel crises with our soft power, with our monetary involvement. (A number of other countries, notably the BRIC nations, have been increasingly using the soft power approach as of late.) Due to the economic crisis, European influence is falling globally because of the region's inability to employ soft power. And since we have also seen a decrease in hard power, this is a major challenge for security in Europe.

On a related note, if the European Union is not capable of further sustaining its integration process—which we are strongly in favor of—it is possible that we will return to the situation existent in the 1920s and 1930s where nations only looked out for their own interest. When they act out of self-interest in such regions as mine, this is of course problematic. Let us ensure that this does not happen.

Another challenge is that as of late we Europeans have tended to think that wars and conflicts happen somewhere else. But this thinking is wrong. If you look at the history of civilizations or at least the history of Western civilization over the past 2,500 years, there has not been a single period in which there were no security challenges. Although the last two or three generations of Europeans have not experienced a large-scale war on their soil, it does not mean that this is impossible.

THE TECHNOLOGICAL CHALLENGES

As far as the technological nature of the challenges, the cyber security domain is a concern. We must not only focus on defense within the cyber sphere but also on offense because—as those people who are interested in martial arts will know—defending something can only be combined with offensive capabilities. It is not possible to simply remain in defensive positions.

Cyber issues are becoming increasingly intertwined with the challenges of information warfare, which include modern media and electronic media. We have to take into account television- and media-based psychological offenses and attacks

because you do not need the war if you can change or influence people's minds: the people themselves can destroy their own societies, their states, whatever they have, if they are taken in by information warfare. We see this in the fight against terrorism. We also see in contemporary conflicts that if you lose the information war, then 50% of your war is already lost. If you add a successful cyber attack on top of this, then everything is over.

THE CHALLENGES OF CONVENTIONAL ATTITUDES

Regarding the challenges of conventional attitudes, one issue concerns the makeup of country elites. In the past decade, there has been a fundamental change in the composition of elites in the Arab world compared to those in Western countries. In the Middle East, young people—who by nature tend to be more aggressive—are dominating the political sphere. By contrast, in the Western world it is older people—who perhaps have fewer ideas and a lower capability to think in warfare terms compared to young people—who comprise the leadership. There is therefore a psychological imbalance between the two.

Concerning the Afghanistan issue, serious challenges are likely to emerge in Central Asia in the future because the region will be affected during and after the withdrawal of NATO troops from Afghanistan. This, in turn, will result in challenges for the European Union and NATO partners. Moreover, our neighbor Russia should be highly interested in cooperating with the West to tackle the challenges in the region.

The issues in Asia and the BRIC countries are also important because these countries are spending more and more money not only for soft influence, as I mentioned earlier, but also for hard defense. In fact, in these countries the psychology is very similar to the European thinking of the 19th and early 20th centuries, which considered that war is part of society (along the lines of von Clausewitz). We will likely observe this type of thinking more and more as these regions grow increasingly ambitious.

THE CHALLENGES OF CLIMATE CHANGE AND CONCLUSIONS

Lastly, the climate change issue is of course a priority. It is likely that new solutions for energy shortages, water scarcity, and other challenges may include military means. We have to be ready for this.

To conclude, we have to follow the advice of Tseng Tzu, whom I mentioned earlier, and think not only of what is next but also of what is happening, why it is happening, and how we can best handle it. This is what is sometimes missing in our approach with regards to both conventional challenges and modern ones that we cannot fully predict.

As a final remark, a practical issue we have to solve rapidly is what I would call the schizophrenic relationship between the European Union and NATO. Until they can cooperate effectively, we have an open door for a number of conflicts and issues which we cannot really tackle or do not know how to tackle among European partners. We should therefore put an emphasis on trying to resolve this issue.

Chapter 12

The Chicago Summit: Were We Faithful to the "Spirit of Lisbon"?

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

When we met in Chicago this May, the Lisbon Summit seemed a distant past. The security landscape did not change dramatically but the overall environment in which we operate changed a lot. Budgetary austerity, turbulence within the EU, and a shift in the U.S. policy towards the Far East were the "background noise" of our discussions. Yet we managed to find consensus on projects we put in motion in Lisbon and to launch quite a few important initiatives.

Unfortunately, as a result of the economic difficulties that the NATO members are facing, we look by default at capabilities and defense spending as a source of potential savings. Maintaining defense capabilities at the appropriate level during the economic crisis is a challenge. But this is an effort that has to be made.

The reality in which we are acting is marked by unpredictability. We face not only economic but also political surprises. A case in point was the Arab Spring which started as a society-led movement, and which in a short time swept away political elites and political systems in the Arab region. And it was and still is engaging many governments, including those of NATO members.

We also experience an impasse in NATO-Russia relations. I would venture an opinion that the reset button pushed in Lisbon is now stuck. We still lack an agreement on cooperation in the field of missile defense, which has recently become the central issue in our talks. Moreover Russia is planning to deploy S400 and Iskander missiles in the Kaliningrad Region—which may deepen the security gap between NATO's "interior" and "border" states.

The above examples only emphasize the fundamental premise of our strategic documents—We cannot predict all security scenarios. Therefore, apart from sound planning, the Alliance should be flexible enough to take necessary decisions fast.

THE ROOTS OF THE CHICAGO DECISIONS—THE LISBON SUMMIT AND THE NEW STRATEGIC CONCEPT

The Summit in Chicago was an important meeting but it was not a breakthrough event in the modern history of the Alliance. It was more like a point of reference to see where we stand with the implementation of tasks we agreed upon in Lisbon.

The Lisbon Summit was a milestone for the Alliance, first of all, due to the adoption of the new strategy and the opening of a deep internal reform process. NATO's Strategic Concept was a good compromise, NATO's unity being the most important issue.

In November 2010 we confirmed the centrality of collective defense and deterrence and introduced mechanisms underpinning the implementation of Article 5, such as contingency planning, exercises, and training. The measures mentioned above are a practical implementation of the Reinforcement Concept launched in Lisbon. We also pointed out the need to implement practically "visible assurance," which means that every NATO member should have access to the Allied infrastructure and tangible military presence.

We made a decision to build NATO's missile defense capabilities. Missile defense in Chicago had become an integral part of our deterrence policy. It was a very important step because it confirmed American engagement in Euro-Atlantic military cooperation. I firmly believe that the missile defense project is a unique opportunity to change the nature of NATO-Russia relations towards an atmosphere of greater trust and cooperation. We should not miss this opportunity.

The documents approved at the Lisbon Summit stimulated the Afghan authorities towards more active engagement in the process of reforming the state administration, improving governance, and developing the country. The Enduring Strategic Partnership Agreement between NATO and Afghanistan was, above all, an announcement that NATO will not take its helpful hand away, even when a military operation is over.

KEY RESULTS OF THE NATO SUMMIT 2012

Defense capabilities. One of the main Chicago deliverables was the Defense and Deterrence Posture Review, which established a balanced mix of conventional, nuclear, and missile capabilities commensurate with the role of the Alliance in our defense planning. Let us hope that we will live to see the world without nuclear weapons, but for now, the right path is to reduce arsenals carefully with the principle of reciprocity in mind.

The military structures of NATO set out to review its defense capabilities. Two sources of guidance for them were the Political Guidelines accepted by defense ministers in March 2011 and the NATO Forces 2020 declaration from the Chicago Summit.

The guidelines described the level of ambition as that of two major and six minor operations in parallel. Moreover, NATO should be able to deploy forces bigger than a corps (so-called Major Joint Operation plus, or MJO+).

Meanwhile, the NATO Forces 2020 document reconfirmed NATO's commitment to three core tasks envisaged in Lisbon. Collective defense remains the most important of them. I hope that the final result of this process will duly reflect those principles. Interoperability and the idea of Smart Defense is a brilliant response to financial vulnerability. However the target of 2% GDP spent on defense remains valid. Economizing has to be "smart" as well.

A good example of Smart Defense is NATO's Air Policing. We have agreed to its extension and just a few months ago our contingent started its fourth rotation in Air Policing. This mission is of crucial importance for the security of this region and is a visible sight of Allied cohesion and solidarity.

For the sake of a more balanced engagement of the three Baltic States, Poland would welcome diversification of airfields from where the mission is executed. The Air Policing mission was established in order to protect all three countries. Therefore, rotating the base seems logical and gives incentives for infrastructure investments. It seems that new airbases—the Ämari in Estonia and the Lielvarde in Latvia—will be operationally available for this purpose soon.

Missile Defense. The Defense and Deterrence Posture Review introduces ballistic missile defense as a component of NATO deterrence. NATO's ballistic missile defense interim capability announced at the Summit confirms our determination to develop this program multilaterally. It constitutes the first step to realize our ambition of developing a robust missile defense in Europe.

We hope that the system will gradually become fully operational. Nevertheless, there is still a lot of work to be done to solve remaining political and legal questions, including that of the debris. A clear policy should be elaborated in this regard so that every NATO member can equally enjoy the benefits and share the costs of a modern missile defense system.

With regard to the Russian negative reactions to NATO's ballistic missile defense program, the Lisbon Summit has put down real foundations for NATO-Russia cooperation. Missile defense could become an axis of NATO-Russia Council meetings and revitalize this forum after a deadlock in 2008. Regrettably, Russia does not seem ready yet to plug in. Meanwhile the atmosphere around the Kaliningrad Region and the constant perception of NATO as an enemy does not help our relationship.

Afghanistan. Decisions taken at the Summit constitute a guarantee of international support for the reconstruction of Afghanistan and dissolve any doubts regarding the future of an international presence. The Afghan security forces need to be ready for the new reality and they will not be left alone. However, we have to encourage the authorities in Kabul to become self-reliant, because only they can fully embrace the needs and expectations of their nation. The Afghan people have suffered a lot in recent decades. They deserve peace to develop their rich and complex culture.

Our withdrawal from Afghanistan will mark the beginning of a new era for the Alliance—an era without major peace operations led by NATO. This can be a good opportunity to re-establish the right balance between the core tasks: collective defense, crisis management, and cooperative security. We should use this opportunity to rebuild and reinforce our capabilities—especially the European ones—allowing us to face all possible challenges and threats, old and new.

IMPLICATIONS FOR POLAND

Let me share with you some observations from Warsaw on the Summit and related processes. The Lisbon Summit was an important compromise and success from a Polish perspective as it confirmed that NATO is still a reliable community of states sharing the same values. My country is attached to both the traditional and expeditionary roles of the Alliance—not because we are oversensitive about our security, but simply because we are aware of the difficulties that haste in solving sudden problems may imply. That is why we defended Lisbon deliverables in Chicago. That is why such issues as missile defense, MJO+, exercises, and infrastructure will stay high on our agenda. Integrity in our approach to Article 5 obligations

requires that on our side, we spend a fixed rate of 1.95% of GDP on defense, we actively participate in ISAF and other missions, and we will do our best to make Exercise Steadfast Jazz next year a success.

However, we observe a worrisome tendency to disregard the importance of greater and heavier military units. We have to remember that MJO+ is a sine qua non condition for preserving a real capability to cover Article 5-related needs. It is far easier and less expensive to retain the present capabilities than to build them from nothing when necessity arrives. But it is also a capability that we may need for the most demanding out-of-area operations.

I hope we will be able to achieve consensus on this issue with the watchful assistance of the Secretary General. The process of elaborating the Minimum Capability Requirements should be led in a spirit of compromise and watched by the Secretary General.

CONCLUSIONS

In Chicago we were able to: strengthen the transatlantic link; keep the cohesion of the Alliance; and speak frankly about needed defense expenditures. The most important message is that, despite the economic crisis, our Alliance is strong, capable, and united around shared values.

During peacetime, when war is only a distant memory, we often forget that security is a superior value. Without security there is no economic prosperity, development, or well-being for nations. And security is not always a given. We have to remember this often, as public opinion tends to forget it.

In democracies, the authorities have to respect the will of the citizens but they also owe them sincere information. We cannot determine what is impossible in a modern, unpredictable world. That is why, in moments of doubt, we should open our handbook—the new Strategic Concept—and read it carefully. The Lisbon Summit did not end in November 2010. For 18 months, we have been preparing executive documents based on the Concept and we have not finished yet. Chicago was an important, yet not the conclusive, moment in this process.

The Lisbon consensus was not a piece of cake, therefore let us respect and protect it. NATO actively engaged and concentrated on the security of its members. But also thoughtful about its partners, NATO is developing itself through constant modernization and with a strong common front. All for one and one for all—this is the spirit of Lisbon, or even the soul of Lisbon, reinvigorated in Chicago.

Chapter 13

The European and Central European Approaches To New Defense Challenges

Mr. Jiri Schneider
Czech First Deputy Minister of Foreign Affairs

I would like to touch upon two issues that do link very well with what Ambassador Winid said about the results of the recent Chicago Summit and its ramifications for European members: First, does Europe have the resources and recipes to manage the security challenges in its neighborhood? This notably applies to the post-Arab Spring situation and the crisis in Syria. Second, what is the Central European experience with defense transformation and regional cooperation? This includes such programs as smart defense, and pooling and sharing as well as defense cooperation among the Visegrad Group countries (Czech Republic, Hungary, Poland, and Slovakia) and the role that the region can play within the Alliance's wider strategic framework.

EUROPEAN RECIPES FOR THE POST-ARAB SPRING SITUATION

Judging by the recent experience, lack of resources and lowered ambitions are the prodigious thin red line running through many countries' considerations when it comes to defense and security issues. Most of us have new or updated security strategies and/or strategic concepts recognizing new threats and challenges that require smarter spending in security.

The key security considerations outlined in NATO's 2011 Strategic Concept and in the security strategies of most countries (and organizations) will not change dramatically in the near future. We will still find ourselves in a dynamic and rather unpredictable security environment, which will force us to enhance our ability to identify and swiftly react to crises—just like we did last year, when, despite several shortcomings, we acted on Libya.

And yet, defense expenditures fall year after year. Almost all European members are trimming defense budgets, which carries the risk of bringing about—as former U.S. Defense Secretary Robert Gates put it—a "collective irrelevance." This also means that the European Allies' value within the Alliance falls too. Indeed, the European Allies' share of the defense expenditures of the Alliance has fallen from 50% in 2000 to merely 25% today.

There is definitely concern over current and future crises as well as many unanswered questions. Do we really understand and know the new areas of conflict? Do we have a recipe for addressing them and a "plan B" if needed? Can we offer solutions—diplomatic or otherwise—and have the strategic patience (and resources) to see them through to the end? Do the Balkans provide a model of any use? What about the "soft power" projected by the European Union? And, can we withstand the pressure of public opinion?

Libya and now Syria are proving to be tough but valuable lessons. They are testing not only our military capabilities, but also the instruments of "soft power" and some of the EU's core policies and principles (immigration/refugees, solidarity, development, and education to name a few). Last, but not least, they are also testing the transatlantic link.

Can we even find the right recipe(s) then? The answer, given current budget constraints, may lie in finding an interface and the right balance between contingency planning and smart defense. Territorial defense and expeditionary forces are not necessarily incompatible.

THE CENTRAL EUROPEAN EXPERIENCE

Given their geographic proximity, common history, and successful re-integration into the Euro-Atlantic community, the Visigrad (V4) countries have maintained a certain degree of cooperation in the defense field. Yet, there are indeed deficien-

cies, especially in the interoperability of our armed forces, and they need to be addressed. The V4 states have been engaged in NATO operations for more than a decade, but this has not helped us to increase military interoperability, as each of us has individually focused on different tasks in different areas, with minimal overlap and joint planning.

As a result, the V4 countries have welcomed the multinational capability development initiatives that seek to contribute to achieving these goals—smart defense under the auspices of NATO and the pooling and sharing initiative of the EU—even though projects are not always easy to find and the experience so far has been mixed. At the same time, we intend to increase V4 interoperability through a more intensive training and exercise policy (e.g. helicopter training, exercise Steadfast Jazz, etc.), as well as active participation in the NATO Response Force and the EU battlegroups. In April this year, a few weeks before the NATO Summit, the V4 released the "Responsibility for a Strong NATO" Declaration capturing much of what I just described.

The robust program of joint exercises proposed within the initiative offers an excellent opportunity for deepening cooperation with the United States. The new U.S. Strategic Guidance, published earlier this year, proposes a more intensive rotation of U.S. brigades stationed in Europe for exercise purposes within the NATO framework—which coincides with the V4 plan to increase the frequency of training activities in the region.

The transatlantic partnership remains paramount for European security, but it is by no means a one-way street. It is a mutually reinforced partnership and its key message is that no matter what differences emerge, we as partners value our collaboration highly and are committed to working together because it enhances our collective security.

Chapter 14

Lessons Identified and Lessons Learned From Operation Unified Protector

General Manfred Lange
Chief of Staff, Supreme Headquarters Allied Powers Europe (SHAPE)

Our panel's task is to look at the lessons learned from the Arab Spring. In watching the news this morning, I had two observations: (a) The developments in the Arab world are absolutely topical. (b) The Arab Spring has not at all come to an end. I therefore believe it is fair and correct to say the lessons learned with respect to the Arab Spring are a challenge and to a certain extent limited but taking stock of the situation is certainly worthwhile.

The NATO-led operation in Libya, Operation Unified Protector (OUP), was conducted from 31 March through 31 October 2011. It is generally held that the Alliance successfully responded, planned, and conducted this operation despite challenging and unique circumstances. This means that—especially when measured against U.N. Security Council Resolution 1973—we can declare: Mission accomplished!

OUP ended some nine months ago, but the lessons learned process has not yet been completed. However, I will summarize the preliminary results of the lessons learned process from a strategic perspective. This summary—drawing on different strands of work done by a number of NATO bodies—includes general strategic lessons, military lessons, and political lessons.

GENERAL STRATEGIC LESSONS

There are three general strategic lessons which may appear self-evident and unspectacular, but lessons do not have to be new or exciting: They have to be valid. OUP demonstrated:

- The willingness and ability of the Alliance to quickly and effectively respond to a crisis—both politically and militarily. Moreover, OUP demonstrated that without NATO's unique military capabilities, the efforts of the wider international community to manage and resolve the crisis in Libya would have been in vain. Therefore, OUP proved—again, I should say—that NATO can be an indispensable actor in international crisis management.
- That European Allies are indeed willing and able to take the lead in a NATO-led operation, and that NATO does not always have to rely on U.S. leadership. Nevertheless, there is no denying that the U.S. had to fill important capability shortfalls and provide enablers in key areas during OUP. This imbalance in capabilities between European Allies and the U.S. must be addressed as a priority as soon as possible.
- The value of partnerships. Early and close consultation and cooperation between NATO and non-NATO actors dealing with the crisis in Libya was essential to the success of OUP. In crisis management, NATO depends as much on partnerships with the international community as the international community depends on NATO. Therefore, we should try to further enhance these partnerships, especially with the U.N. and other relevant international and regional actors.

MILITARY LESSONS

The military lessons fall into three broad categories that are critical in view of NATO's overall ability to rapidly and effectively initiate and conduct future operations. The categories are: (a) asset availability; (b) command and control, and (c) policy, doctrines, and procedures. During OUP, a wide range of assets were required in fairly large amounts—such as ISR (Intelligence, Surveillance, and Reconnaissance) and precision-guided munitions. Clearly, there were shortfalls in the availability of these critical assets. Although these shortfalls could be managed, it is important to underline that technologically advanced key assets need to be available in sufficient quantities at all times in order to effectively achieve the desired results.

Asset Availability

During OUP, it has also become apparent that NATO may still over-rely on the U.S. to provide certain key assets, such as air-to-air refueling. Overreliance on one single Ally decreases the availability of alternative sources. From a burden-sharing perspective, and in view of the global trend towards further cuts in defense spending, pooling and sharing of assets and capabilities amongst several or even all Allies may be required to ensure the availability of key assets and capabilities in sufficient quantities at all times. The AGS Program, the JISR Concept, and other initiatives are intended to provide solutions for some of the shortfalls observed during OUP. The assured availability of key assets and capabilities is key as the Alliance's ability to effectively respond to future crises depends on it.

Command and Control

A properly manned command and control structure ensures efficient use of available assets and capabilities. During OUP, deficiencies in the availability of specialized personnel within the military structure in the areas of targeting, ISR, StratCom (Strategic Communications), and legal affairs were noted.

The "new" Alliance structures—e.g. the new command structure and new Air Command and Control System—are designed to mitigate most of the shortfalls experienced during OUP. However, some doubts remain as the new structures will be much "leaner," yet these new structures will still have to be filled by Allies who all will be facing cuts in defense spending.

Policy, Doctrine, and Procedures

Shortfalls in the policy, doctrine, and procedures category are undesirable, but can be mitigated with sufficient improvisation—as proven during OUP. Due to planning constraints—such as time, and the incremental approach to the arms embargo and the no-fly zone—the conduct of OUP led to somewhat segregated maritime and air operations executed under separate OPLANs (Operation Plans in Complete Format). A more combined approach with a single OPLAN may have been the preferred approach, but we decided on the pragmatic approach of single OPLANs due to the timelines given to us by the political leadership.

POLITICAL LESSONS

Relations with Other International Actors

The political lessons fall into two broad categories: (a) relations with other international actors, and (b) partner involvement. From the outset of the Libya crisis, political consultation and liaison with other international and regional organizations—such as the U.N., the League of Arab States, the Gulf Cooperation Council, the EU, and the African Union—helped ensure robust international and regional support, and facilitated—if not enabled—NATO's contribution to the international effort, in accordance with the Comprehensive Approach. Contacts and consultations with the different actors were initiated at appropriate levels from the very early stages of the crisis, continued through the planning phase, and were enhanced during the operation itself. The initial request from the Gulf Cooperation Council, and subsequently from the League of Arab States, for the imposition of a no-fly zone over Libya proved instrumental for subsequent decisions at the U.N. Security Council. Strong international and regional support, both politically and operationally, paved the way for NATO's operational involvement.

Throughout the crisis, NATO participated in the different meetings of the Contact Group on Libya. The presence of the NATO Secretary General in the main sessions of the Contact Group's meeting of foreign ministers was important in highlighting that the NATO operation was conducted at the behest of the wider international community. NATO staff contacts and extensive but discreet coordination between SHAPE and humanitarian actors such as the International Committee of the Red Cross and the U.N. Office of the Coordinator for Humanitarian Assistance were instrumental in ensuring effective deconfliction of OUP with humanitarian efforts. At a more technical level, NATO was able to interact effectively with civil aviation authorities to ensure safe civilian air traffic and military air operations.

In sum, NATO's interface with other international organizations during the Libya crisis proved to be very successful

and, in many respects, more robust than during previous crises. We should aim to intensify NATO's interface with international actors.

Partner Involvement

The participation of non-NATO actors in OUP, notably by countries from the region, proved to be a key factor for the success of the operation, both from a political and operational perspective. Building on this positive experience, pragmatic initiatives could be explored to enhance cooperation with non-NATO actors. These are the preliminary results of the lessons learned process at NATO.

CONCLUSIONS

On a personal basis, I would like to add a few personal lessons learned:

- *Improving situational awareness.* As NATO is determined to contribute to international crisis management beyond its borders, even at a strategic distance, there is an urgent need to improve NATO's capabilities for situational awareness, as stated in the new Strategic Concept. As a step in that direction, SHAPE has, in the meantime, established its Comprehensive Crisis Operations and Management Centre, which will considerably enhance NATO's situational awareness.
- *Avoiding operational overstretches.* During the run-up to OUP, I was slightly worried that NATO was running the risk of operational overstretches. NATO was already conducting four operations (ISAF, KFOR, OOS, and OAE). However, NATO's workload was well within its level of ambition, and OUP turned out to be a success. It remains to be seen whether we can achieve this again with a significantly smaller NATO command structure of about 6,600 PE (Peacetime Establishment).
- *Each situation is unique.* NATO is taking a realistic and pragmatic view of what it can—and should—do in this complex 21st century. We are taking lessons from OUP, but each situation is unique and we must be clear in our understanding of the benefits of lessons from OUP and the limits of these very same lessons.
- *Guarding against further budget cuts.* In terms of NATO's command structure, OUP has clearly shown how important a standing NATO structure is in order to react to a crisis swiftly. We must recognize and accept that after 20 years, NATO's military operational command is approximately 30% of the size it was in 1993. At the same time, national military structures are being reduced. I am sure there is a floor and I believe we have reached it. Further cuts will not solve problems but simply make them worse and undercut the most fundamental element of the Alliance—its glue.

Chapter 15

Lessons Learned from the Arab Spring

Ambassador Maurizio Massari
Italian Special Envoy for the Mediterranean and the Middle East

FIVE KEY POINTS

When we talk about lessons learned from the Arab Spring, we have a very complex and difficult picture. I would like to make five points.

- *There are many kinds of Arab Springs.* The first point is that there is not just one kind of Arab Spring, but many different situations: Tunisia, Egypt, Libya, Syria, Yemen, and Morocco are very different from each other. We have at least three typologies: the popular uprising, the armed struggle, and the evolution—as is the case of Morocco. So in different countries the transition has been conducted in different ways. This of course has clear implications for our policies and this will be our first lesson. Sensible policies have to be country-based. Ambitious regional programs and blueprints are not realistic at this point and, let us be honest, the West does not have the political and economic resources to implement them. This is what makes the Arab Spring and our response different from the post-communist transitions. Post-communist transitions took place at a moment when the West was at the peak of its political and economic strength. The West was willing and able to engage on a large-scale. The Arab Spring is taking place during a period of economic difficulties for the West and for Europe in particular. So the first lesson is a very realistic approach with country-based policies. Of course this requires the best possible coordination among Western countries in terms of implementing assistance and aid to these countries. And it also requires coordination among the various international organizations. By and large, the "more for more" approach that Europe and the EU in particular have adopted is the right one. In any case, it is the correct one provided that incentives are very clearly defined and the relative resources are also allocated.
- *Arab Spring countries have no "model" of reference.* The second lesson is that 2011 is not 1989, as I indicated above. This is true not only for us in the West, but it is also true for the countries of the region. Countries in the post-communist period beginning in1989 had a very clear vision of returning to Europe. For Arab Spring countries, there is no real model of reference. There is no family to return to, which is a point I have heard in all the countries to which I have been traveling in recent months. Each country will follow its own path of development. There is no Turkish model and, fortunately, there is no Iranian model. I mention Turkey and Iran because there has been so much speculation as to whether countries would follow either the Turkish model or the Iranian model, and I think that is a misleading approach.
- *Arab Spring countries have common challenges of governance, the relationship between Islam and politics, and inclusivity.* A third point is that, despite some special circumstances, there are three common challenges that all these countries must face. The first one is governance. After all, the crises were caused by a deficit of governance in all of the states. So the fight against corruption, for transparency, social justice or the reduction in social inequalities—all these issues which fall under the hat of governance are a common challenge for all of these countries. The second common challenge is the relationship between Islam and politics, which also has to do with the writing of the new constitutions—whether sharia will be the exclusive or primary source of law. As you know in Tunisia, the issue has been resolved in a positive way according to our perspective. It is still open, however, in many other countries like Egypt. And the third common challenge is inclusivity, which has many different dimensions, certainly including the treatment of minorities. We tend to focus on the rights of Christians, but this issue is important for all minorities in these countries. Inclusivity also has a geographic dimension. Consider Libya for instance and the treatment of the different regions of the country. It is the same in Tunisia, where coastal regions have been developed whereas the internal regions have been much more neglected. In addition to this geographic dimension, there is also the struggle between old and new which will be

resolved through the transitional justice. The challenge is to have justice and to sanction crimes that are linked to the old regime but to do so in a framework that is not one of vengeance but, on the contrary, of national reconciliation.

- *A realistic country-based approach is necessary.* I now go to the fourth point. What do we need to do to have a realistic country-based approach? First of all, we need to adapt and reset ourselves psychologically, because what we are seeing with the Arab Spring is neither the end of history nor the clash of civilizations. The euphoria that existed at the beginning of the process is now replaced by a transition, which sometimes leads to outright skepticism or even nostalgia for the old order. I believe this is exactly the wrong way to think about it. We should look at the development of the Spring in a realistic way. We cannot expect convergence with the West, but at the same time we should not fear any irreconcilable divergence with us. We should accept that we have to deal with these countries differently from the way we did in the past. Whether this will be better or worse will be judged by the people of these countries. We also need patience. Since these transitions are going to take a long time, we need to be realistic, while at the same time respecting their sovereignty and treating these countries as equals.
- *Implications for regional security.* My fifth and final point concerns the implications for regional security. The good thing is that—as we know in international relations—democracies usually do not go to war against each other. So in theory we should have a better chance of constructing a regional order. Of course this principle will take time to be validated, because the transition has to be consolidated. In any case, we already see some good signs in the form of mutual relations among the countries of the Maghreb, the Arab Maghreb Union, the relationship between Tunisia and Egypt, and that between Egypt and Libya. As to the relationship between the new Egypt and Saudi Arabia, everybody thought it would be very tense. Yet, in his first trip abroad, President Morsi went to Riyadh. At the same time, we have witnessed over this year and a half a revitalization of regional organizations: the Arab League, which has been playing an active role in the Libyan and also in the Syrian crisis, and the GCC, the Gulf Cooperation Council. So there are some positive signs of a possible regional order.

CONCLUDING REMARKS

Of course, three major challenges for regional stability will remain with Syria (and we do not know how this crisis will unfold), Iran, and the Palestinian issue (which provides a reason for resentment in the region). I believe that if democracies consolidate, we will have the conditions to create a bottom-up security dialogue in the region, engaging all the regional actors, the regional institutions, NATO, the European Union, the Arab League, and the GCC. Let us hope this will consolidate mutual trust with other countries of the region.

Chapter 16

What Lessons Have We Learned From the Arab Spring?

Lieutenant General Claudio Graziano
Chief of General Staff, Italian Army

The events of the Arab Spring will represent, no doubt, a turning point in the social and political developments on the southern shore of the Mediterranean and in the Middle East. I will first offer you some personal thoughts before focusing on some of the lessons we have learned from the Arab Spring.

REFLECTIONS

It is important to note that the Arab Spring has arisen in what has long been a critical region. The Middle East has a history of being on the front line of crises, an area where profound geo-strategic changes frequently take place and future conflicts are likely to erupt. The area stretching from the Maghreb to Suez and eastwards along the Mediterranean Basin encompasses countries and populations characterized by strong contrasts and dissimilarities. For the most part, these countries have large stocks of natural resources—notably oil and gas—whose revenues are not redistributed equally, thus creating a widening gap between the wealthy ruling classes and the poor masses, who are increasingly pessimistic about the future. It is no coincidence that the earliest uprisings were due to economic causes: In Egypt, for example, the rising price of broad beans, the main food for the less well-to-do classes, was the triggering factor.

Moreover, we cannot forget that this region is engaged in an enduring crisis given its close proximity to Israel and the unresolved Palestinian issue. This can be easily manipulated and exploited by actors who can derive economic or geopolitical advantages from the persistence of conflicts in the region.

The key role played by the armed forces in almost all countries which participated in the Arab Spring should not be underestimated. Often, the armed forces proved themselves to be the true bulwarks of national unity as well as reliable partners for the population and the local community.

The Meaning of Democracy in the Middle East

Despite knowing that we were dealing with a potentially unstable area, we, the West—and particularly Europe—did make a serious mistake: We did not predict what would happen at our very doorstep. We thought a democratic political system could be established in these countries overnight. We did not consider what the meaning of democracy is in countries that are inspired by strong theocratic feelings. For example, in February of last year, when I was the Chief of Cabinet of the Italian Minister of Defence, I landed in Benghazi, in Libya, with the Chief of Cabinet of the Minister of Foreign Affairs to talk with the revolutionary governing body, but they were not ready to begin planning for a fully democratic government. A wave of demonstrations against Gaddafi subsequently broke out and his regime collapsed several months later. The revolutionary governing body was still not ready, however, and moreover it is probable that without NATO's intervention Gaddafi's ouster would have taken much longer. In many cases, for the first time the political forces in the countries participating in the Arab Spring have had to consider the true meaning of the word 'democracy' in an Islamic context and how to act accordingly in order to strike the right balance between Islam and democracy.

Different Forms of the Arab Spring

The Arab Spring has taken a number of different forms, so we must first look at a snapshot of the situation: In some cases, uprisings did not turn into riots, as in Algeria, Morocco, and Jordan, where constitutional measures and new parliamentary elections sufficed to contain revolutionary anger. These cases, however—and Morocco's in particular—are indeed peculiar: Protests cannot involve the king, as he is considered a direct descendant of Prophet Mohammed. In other cases, regimes fell

before a civil war started. This was the case in Tunisia, where 2011 elections sanctioned the victory of the Islamic moderate movement and where, under the fourth cabinet in one year, the works of the Constituent Assembly are almost finalized. In still other instances, however, the fall of regimes came at the end a violent confrontation, as in Egypt. Here the military, which have held power since President Mubarak was overthrown, had to call legislative and presidential elections given the bloody street battles. Last, but not least, there are also extreme cases where protests degenerated into real civil wars, as in Libya and Syria.

In Libya, despite the recent elections—which were the first free democratic elections in more than 40 years—the overall security picture is a cause for concern given the large number of clashes between rival militias as well as attacks aimed at institutional or international targets in several parts of the country, especially Cyrenaica. Let me emphasize that Western military intervention in support of the National Transitional Council—although in the form of a coalition of the willing in its early phases rather than of an action shared by the entire international community—has managed to avoid a Syria-like scenario. The transition has just begun in Libya and—while the country is much less complex than Lebanon, where it took 16 years of civil war and confrontation to reach a democratic phase due to the large number of ethnic groups dividing the country—it will still require some time to complete the process.

The gravest crisis is taking place in Syria, both from a humanitarian viewpoint and in terms of its outward destabilizing potential, especially since it appears the revolution still has not reached its most violent phase. The situation in Syria is much more complex than in Libya. Democratic aspirations suffer from the religious conflict between Shia and Sunni Muslims, which inevitably affects all Arab States, albeit indirectly. I do not think we can deploy an alien military force to Syria like we did in Libya, especially if we consider the profound economic and sectorial interests that have prevented concrete actions by the U.N. Security Council so far. The Syrian crisis, in my opinion, is highlighting the need for a major overhaul of U.N. decision-making mechanisms. Since I do not think such a solution can be implemented in the short term, I think the only possible form of military deployment to Syria relies on a Russia-led coalition of the willing.

LESSONS LEARNED

- *Each crisis is unique, and we must be prepared to adapt*. In the first place, the West has learned that each and every crisis is unique and we must therefore be prepared to adapt our forces, both during the crisis itself and after, during the rebuilding phase. Hence, we must tailor our approaches to capability development and reconstruction to each specific instance. Revolutionary events may take place at different speeds in different countries but we can be sure of one thing: On the domestic front, the fall of an authoritarian regime does not automatically fulfill the expectations of the revolutionaries. And from an international perspective, it generates a climate of uncertainty that could undermine stability in the entire Southern Mediterranean and Middle Eastern regions.
- *The importance of a roadmap for transition.* The second lesson is the importance of defining a roadmap for transition; It is essential to evaluate all possible ways to handle revolutionary movements in order to establish the most suitable political, military, and business tools to assist in the transition process. There are a large number of variables that affect transition times. In fact, even in situations where transition has taken place more quickly and less violently than expected, the leaders of the revolution have often struggled with critical or tense local management situations due to the absence of a 'leader' to whom to hand over the responsibility of the country to. Furthermore, the complete annihilation of potential opposition movements (as in Egypt) or the total absence of an existing institutional fabric (as in Libya) frustrate the transition process. Of course, the election of a new government or the ratification of a new constitution does not bring transition to completion (as the Egyptian example demonstrates). Only when the post-Arab Spring states have found concrete answers to the challenges they face, both on the domestic front and with regards to the international community, can we say that transition is complete.
- *The dichotomy between the democratic motivations at the root of the uprisings and the Arab Spring's evolution toward radicalism.* The third lesson concerns the dichotomy between the motivations at the root of the uprisings, such as improving living conditions, increasing individual freedoms, and establishing democratic governments—which are widely shared among the international community—and the Islamist evolution toward radicalism, which has affected almost all the states in the post-dictatorship phase, i.e. Tunisia, Libya, and Egypt.
- *The need for new ways to prevent and manage crises, including tackling root causes such as poverty.* The fourth lesson is the need to find new ways to prevent crises as well as manage existing ones. Conflicts generate immense human suffering, disrupt economic development, and hinder the protection of human rights, thus undermining the fragile transition process towards democracy. Conflicts and poverty are closely linked: While conflicts are a major cause of social exclusion

and poverty, there is no doubt that poverty increases the risk of violent conflicts.

Linking poverty reduction, development cooperation, and the protection of the rights of man to peace-building strategies coincides with what has been an objective of the international community since the 1990s: developing civilian instruments to prevent and transform violent conflicts. The success of this new approach, which goes beyond traditional international politics, was instrumental in pushing European civil society towards planning prevention, management, and the transformation of conflicts.

Conflict Prevention: Operational and Structural Methods

Conflict prevention comprises a set of strategies and provisions aimed at preventing the violent escalation of political disputes within states or among states. Typically, two different areas of action exist: (1) operational prevention, which concerns the potential crisis itself, and (2) structural prevention, which addresses the underlying political, economic, and social causes at the root of the conflict. Operational prevention is directly focused on the possible outbreak of violence and has immediate and short-term effects. In contrast, structural prevention is associated with social and economic development strategies and the creation of structures for political integration in the medium and long term.

The Role of International Organizations in Prevention: The U.N., EU, and NATO

In terms of the involvement of the international organizations, preventive diplomacy institutions and initiatives have developed rapidly over the past decade. Despite these new approaches and methods, however, the Arab Spring and its different facets have shown that the international community was unable to ensure adequate prevention in either of the two phases described above. Nonetheless, international and regional organizations play an essential role, not just in terms of intervention but especially in terms of prevention.

In 1992, the United Nation's An Agenda for Peace drafted by Secretary-General Boutros-Ghali cited prevention instruments as key measures to increase confidence. These include the monitoring of arms, fact-finding missions, timely reporting of conflict situations, and preventive deployment of peacekeeping operations. The U.N. has also established its own early detection system in the humanitarian sector. Like the EU, however, it suffers from decision-making mechanisms and procedures that have proven ineffective, thus requiring a major overhaul. However, the U.N. remains the essential organization to legitimate and to mandate civil and military interventions.

The European Union is another major international stakeholder with a range of policies, both military and civilian, that also encompass trade, development, and security-related matters. They all have real significance in the world. However, the EU itself has not spoken with a single voice during either the Libyan or Syrian crises. Reviewing the procedures and methods for European political and military intervention outside European borders is therefore a necessity.

Since the end of the Cold War, NATO has had to adapt considerably: It took years for the Alliance to take action in order to bring the conflicts in the Balkans to an end. From this experience, we learned that early detection is crucial to prevent crises, and NATO rapidly moved along this path. First, it expanded the range of what it considers possible hazards, which now goes well beyond the mere threat of direct aggression to Allied territory and encompassing non-military and unconventional threats such as terrorism. Moreover, it has developed a new, powerful intelligence warning system, the NIWS.

No matter how well designed a system of early detection is, however, its success depends above all on assessment and political will. Ultimately, the political will to act and—if necessary—to intervene individually and collectively is more important than any other early detection instrument. Political will is clearly influenced by a host of other issues, including elections, conflicting internal priorities and, above all, public opinion.

CONCLUSIONS

In conclusion, the Arab Spring has been, almost from its very inception, a controversial topic among Western and other observers. Many scholars have noted that the events demonstrated the inadequacy of the previous instruments and categories of analysis, as they were unable to predict the events or suggest future developments. However, foreseeing a turning point in history is quite difficult and probably a definite time placement will never be possible.

In any case, the Arab Spring has taken the West by surprise, which was probably not fully aware of the importance of the link between information/communication and revolution in these countries. Indeed, history has shown that streets

filled with demonstrators and rapid news dissemination are no guarantee that uprisings will turn into revolutions, nor that they will transform democratic ambitions into institutional provisions. The rapid flight of President Ben Ali from Tunisia and the relatively quick overthrow of President Mubarak in Egypt only a month later provided a taste of optimism to both the Arab and the Western worlds. A domino effect was consequently triggered and the Middle East as a whole took fire—a fire which continues to simmer—in its quest for freedom. For different reasons and in different ways, the protests have not stopped in any country in the region. Unfortunately, Western public opinion is only focusing on a few countries, especially Libya, while the Jasmine and Lotus Revolutions in Tunisia and Egypt respectively seem like distant and forgotten events. It is as if the delicate process of transition that Egypt and Tunisia are experiencing were not as important and crucial.

We have certainly learned that increasing pressure on a specific regime or assisting those clamoring for change may lead to a true turning point, although we cannot predict when or by what it will be triggered. Tunisia, the country where it all started, is a good case in point: A man reached the limit of his endurance, set himself on fire, and the images of his death triggered popular revolts. As a consequence, others came to believe that success and change, which some optimistically called democracy, were achievable.

Bahrain and Syria, however, prove that events can unfold rather differently. Making autarkic dictators or quasi-dictators fall does not guarantee an open door to truly free political systems based on popular will. The evolution of the Syrian crisis, and the gradual Islamist drift of the Arab Spring in particular, put to the test and perhaps question the strategy that the West has adopted so far. Although the uprisings over the past year have been sparked by liberal and libertarian movements, the overthrow of old regimes has witnessed the emergence of Islamic groups which can only partially and euphemistically be considered moderate.

Chapter 17

Personal Views on the Afghanistan Situation

Lieutenant General Jürgen Bornemann
Director General, NATO International Military Staff

NATO'S KEY PRIORITIES

When trying to identify today's challenges for NATO, we need to explore the key priorities for the NATO HQ within the next two to three years, which could possibly include the run-up to the next summit. I believe there are six topics which are very high on the NATO HQ's agenda in Brussels. I will only briefly touch on them and then concentrate on Afghanistan.

- *Afghanistan.* Afghanistan remains our first priority, which should not be surprising to you and, right now, the key issue is to complete the transition of the security responsibility to the Afghan authorities.
- *Defense package.* Our next priority is the defense package, and we touched on this during the workshop when we talked about future capabilities. How can we guarantee that NATO will have the necessary capabilities available in the next decade taking into account our limited resources?
- *Enlargement.* Enlargement is a priority—and this means maintaining the existing "open door" policy in NATO, particularly with regard to the Western Balkans. This was also an issue that was addressed in this workshop.
- *Russia.* As to Russia, I believe we have to look seriously into the question of how we can revitalize the NATO-Russia Council and in this context also how can we deal together with our Russian colleagues in order to come to a compromise on the missile defense issue.
- *Partnership.* NATO is an organization that is looking for global partnerships and, as General Lange mentioned, this is particularly relevant in NATO-led operations; this is also true in Afghanistan. If you look at the NATO summit in Chicago, 60 nations and organizations sat around the table—the biggest gathering in NATO's history. So the importance of partnership is becoming more and more relevant with regard to NATO's operations and we have to look into the question of how we can implement the partnership tools, agreed to in the Berlin package of 2011, and make it more attractive for partners to deal with NATO.
- *Transnational threats.* And finally, how should we deal with transnational threats? In this context, the main challenges for us are cyber—this was one of the key issues of this workshop—but also energy security, counter-terrorism, non-proliferation, civil protection, and disaster management.

I believe these are the six key issues that will be high on the agenda of NATO HQ in Brussels in the years ahead, and as such, I was pleased to see that in this workshop most of these new challenges have been addressed over the last couple of days.

VIEW ON THE AFGHANISTAN SITUATION

Let me now concentrate on Afghanistan. As I said in the beginning, Afghanistan remains the No. 1 priority for NATO from an operational point of view. The operation in Afghanistan is still NATO's largest operation. I will not bother you with a lot of facts and figures and will only give a few numbers: I already said 50 nations are contributing to the operation in Afghanistan. Twenty-eight are NATO nations, but there are nearly the same number of non-NATO troop contributing nations. In total, 130,000 troops are serving under the banner of NATO ISAF in Afghanistan.

At the same time, we are seeing the build-up of the Afghan National Security Forces to a final strength of approximately 350,000, made up of the Afghan National Army (roughly 200,000) and Afghan National Police (150,000) by the end of October 2012. So in a couple of months we will see this successfully completed.

What is the security situation as we see it at the moment? We see considerable progress has been made in the area of security, but also in the area of governance and development. If you only look at the media, you might have the impression that this is a very optimistic view, but I can tell you that the reports we receive in Brussels from COM ISAF and from the representative of the Secretary General indicate real progress, which has not always been reported by the media. I would only mention in this context the legitimate and transparent presidential and provincial elections in 2014 and the completion of the security transition process, which would constitute a positive indicator of the sustainability of the gains made so far. So 2014 will not only be a decisive year for the NATO and troop contributing nations, but also for the Afghans themselves.

However, challenges will remain beyond 2014. The government of Afghanistan's authority and the ability to govern will be impacted by sub-national government structures in the country that are still emerging and by competition posed by power brokers. In terms of security, the insurgency bolstered by sanctuary in Pakistan will still pose a threat to Afghan stability and present challenges to the Afghan security forces with the Afghan National Army still engaged in conducting stabilization operations.

The Afghan national security forces will have achieved significant progress by the end of 2014 in terms of both capacity and competency. However, operational and training capability gaps will still exist and we cannot ignore this. Therefore, the ISAF meeting during the Chicago Summit a couple of weeks ago addressed those challenges that are lying ahead of us.

As the ISAF mission draws down, the NATO Summit delivered a clear decision to establish a post-2014 NATO-led mission to train, advise, and assist at the invitation of the Afghans themselves. This decision was made clear in the joint declaration issued by the ISAF nations and Afghanistan. It is still under discussion whether this NATO follow-on operation after the end of ISAF in 2015 will require a further U.N. Security Council mandate as this is not completely clear at the moment. But there are three key points that were agreed during the Summit in Chicago:

- *Completion of the transition process in mid-2013.* First, an agreement on the next stage of our current engagement. It is a clear understanding of all contributing countries to complete the transition process in the course of 2013. We expect the Afghan forces to be in the lead for combat operations across the country. With Tranche 3 of the handover of provinces this summer, already three-quarters of the Afghan population will be living in areas where the Afghan national security forces are taking the lead for security and in mid-2013 the last province will be handed over to the Afghan national security forces which means the transition train is rolling—we cannot stop it.
- *Completion of ISAF's mission in 2014.* As the Afghan forces step up, the NATO ISAF forces will step back into a supporting role. This will allow us, gradually and responsively, to draw down our troops, but we will remain combat ready until we have completed the ISAF mission at the end of 2014. This requires a successful closure of the ISAF through an ordinary transition and redeployment of our forces—not a rush to an exit, and not as an element to an exit strategy—and without leaving the country in chaos. Therefore, redeployment of our forces will be a major operational challenge that lies ahead of us; it is not only a logistical task, it requires close coordination and cooperation between all contributing nations. Open transit routes and ground lines of communication are vital. Special transit arrangements have been signed with some of the Central Asian countries and with Russia. Pakistan has recently reopened the transit route south through Pakistan.
- *The vital need for communication with the Afghan people.* One of the most important tasks which lies ahead of us is getting the communication right and this is vital. This is true with regard to the Afghan people because they believe NATO will leave them alone at the end of 2014 but at the same time it is true with regard to our own societies. We have to convince our people that an ongoing engagement in Afghanistan is important for our own security. Therefore it is also important that we now start the planning for the role of NATO after 2014. The decision of the heads of state and government in Chicago was the new guideline for training, advising, and assisting the Afghan national forces who have responsibility over the whole country.

We have achieved a lot to prevent Afghanistan from once again becoming a safe haven for terrorists, but there is still a lot to do to sustain the gains made so far.

Chapter 18

The Arab Spring: An Ongoing Political Process

Ambassador Michel Foucher
Institut des hautes études de défense nationale (IHEDN)

I will start with a quotation attributed to K'ung-tzu, Confucius in Latin: "If I were in charge of government affairs, I would start by restoring the meaning of words because when words lose their meaning, people lose their freedom." So let us have a look at the so-called Arab Spring, which by the way started on 17 December 2010, during the winter time in economically depressed central Tunisia.

TEN KEY WORDS TO A CLOSER ASSESSMENT OF THE ONGOING POLITICAL PROCESS

In order to better assess the ongoing political process, I will discuss the following ten key words.

- *Al-alam Al-arabi,* i.e., the Arab world, is not a geopolitical set but a basin of interpretation, a resonance chamber with a popular language, social networks, television such as Al-Arabia and Al-Jazira, and it is going through a kind of synchronous situation.
- *Nahda,* a rebirth or "renaissance" is a motto in Tunisia by reference to what happened there already in the late 19th century.
- *Tahrir* means freedom.
- *Karama* means dignity. It is a key word because dignity comes before democracy.
- *Min Al-moukhit ila Al-khali*j translates into "from the ocean to the Gulf states." This is a tricky association because you can easily imagine that, after President Ben Ali had to leave and take refuge in Saudi Arabia, there were day and night meetings in many capitals to decide on how to adapt to the new situation. In Morocco, it was decided at the top to open up the game to political forces towards a kind of constitutional monarchy, but in Damascus there was a three-day-long meeting to get ready to crush even the first peaceful, unarmed demonstration.
- *Nations.* Nations are the frameworks of these political movements, which are not about Pan-Arabism, Arab nationalism like in the past. They are not about restoring the Arab nation.
- *Revolution, revolt or coup d'etat*? The qualification of these political movements depends upon national situations. In Egypt, it was a coup d'Etat by the military against Mubarak's decision to give power to his son who was not a military man.
- *Democratization.* Is this democracy? It is not yet about democracy but about democratization. Democracy is an internal process in which elections are only the first step. The best proof of democracy is when five years after the first turn, the winner of the first turn accepts to lose the second turn.
- *Overthrow of autocratic powers.* It is an overthrow of autocratic powers but it is also a tricky issue which is very well known in every kind of revolution. The unorganized forces that started the movement were not organized enough to win the first elections. This is the case in Egypt or Tunisia.
- *Articles.* In Tunisia, the Constitution, which was promulgated by Bourguiba, establishes in its Article 1 that Tunisia's religion is Islam and its language is Arabic. However, several contradictory articles are now under discussion such as Article 8, which does not allow religious parties, or Article 6 about the equality between men and women. In Egypt, Article 2 establishes Islam as the state religion, shari'a as the source of the laws, and the Arab language as the official language. What is at stake is where to put the curser between the public and private spheres, between the state and religion. This is nothing new. Europe was confronted with this problem in the past. Of course, in the Maghreb, the Muslim Brotherhood and their affiliates seem to be the winners.

THE DIVERSITY OF TRAJECTORIES TOWARD TRANSITION

Ambassador Massari pointed out earlier the diversity of these trajectories toward transition. Three regional sets can be identified:

The Maghreb. In the Maghreb, the Arab West has initiated a transition towards democratic regimes, with the exception of Algeria, which is rich enough to avoid any change. Morocco tends toward a more constitutional monarchy. Tunisia is the real place for democracy. In Libya, there is a kind of paradoxical heritage from Kadhafi where clerical parties seem to lead. Egypt is a central country, the beacon country in the Arab world, but we have to watch how the curser itself will be drawn between the Muslim Brotherhood and the Supreme Council of Armed Forces.

The Arabic Peninsula. Monarchies have the possibility to adapt themselves. The monarchy was tough in Bahrain because Shia and security issues prevail. In the long run, Paul D. Miller from the National Defense University foresees a "Fading Arab oil empire," where "rising prices and production costs, declining reserves, and the availability of alternate fuels and unconventional sources of oil will decisively undermine the defining role of the Middle East in the global energy market." So the strategic importance of the Arabic Peninsula in the long term will be decreasing.

The Near East. The Near East is a grey area in the evolution of the Arab world. It is a nebula with its societies in the shape of tribal and community mosaics, with the permanent Israel-Palestinian problem and its impact on neighboring countries.

GEOPOLITICAL AND STRATEGIC CONSEQUENCES

We are facing a very diverse landscape. At least in France, this new diverse landscape was presented as the "second death of Bin Laden," but very active affiliates are on the rise, such as AQIM and AQAP in Yemen.

There are new intra-regional struggles between Egypt, Saudi Arabia, and Iran; between Sunnis and Shiites; between lay, theocratic and conservative regimes; there is activism in Qatar and prudence in the United Arab Emirates; there are concerns about Iran regarding Syria, Lebanon, and the U.S. military build-up; and also about the impact on the Israel-Palestinian conflict and the status of Israel, which is feeling isolated today.

Admiral Betermier mentioned earlier the destabilization of the Sahel-Sahara zone, which is serious and is linked to the regime change in Libya. Syria is a very complex issue because it is a multi-layer conflict and when a minority, a clan, is in power, it is not in a position to negotiate and there is no possible compromise.

In the West, the U.S. and Europe are basically bystanders, except in Libya, which was a unique case, and maybe in Syria. What the European Union has to do, and I agree with Maurizio Massari on this, is to try to meet the demands coming from the region to help the transition. As to the policy of the U.S., it is changing and the U.S. may be more comfortable than Europe with accepting a growing role of religion in politics, provided that the Muslim Brotherhood are open to a market economy, which is the case.

Chapter 19

Lessons Learned from the Arab Spring

Ambassador Mariot Leslie
Permanent Representative of the United Kingdom on the North Atlantic Council

The lessons learned from the Arab Spring were very well covered earlier by General Lange, Ambassador Massari and General Graziano. One point I would like to insist on is that whatever we call the Arab Spring—the Arab Awakening or the Arab Four Seasons—it is not a single phenomenon. Each country has its own reality and its own politics. There are some common themes, but there are also many things that arise from the particularity of each different country.

- *Economic challenges.* We can see some commonalities in the economic challenges many of these countries face but not in all of them. For instance, you see across the Maghreb real demographic tensions, particularly young male unemployment, difficulties in economics, difficulties for families and households in making ends meet, but some of the hot spots of this phenomenon have not been in places where those were the most difficult issues.
- *Political tensions.* There has also been across the region some commonality in the political tensions. I think that we would be quite wrong to say that this phenomenon was underpinned by religion but we would also be wrong to completely turn our eyes away from the fifteen years or so of a narrative that was built up not only by Al-Qaeda but also by Arab political movements in the region. This narrative is one of opposition to many of the existing leaders, opposition to interference from values coming from outside the region, and a confusion and contestation in the minds of individuals as to where they want to go in their own circumstances.

AN ARAB PHENOMENON?

So this region was perhaps ripe for something to happen, some big political movement, but that is also true elsewhere. We need to ask ourselves whether there are links between what was happening in the Arab world and perhaps what happened in Iran in the June uprisings, whether it is similar to what is happening in Burma, and whether we can say that there is an Arab phenomenon. I would hesitate to say that there is a pan-Arab phenomenon but it would also be clearly wrong to say that this is not an Arab phenomenon.

Against all of this really quite complicated background politics, the Western international community, the non-Arab community, has been very cautious about how to analyze it, how to intervene, what to do, and yet very troubled by the images it has seen, which had a big effect on our public opinion in many of our countries. And so there is a tussle in people's minds in capitals like mine between principles like human rights, the responsibility to protect, and some of the issues embedded in the U.N. Charter on the one hand, and a reluctance to become involved in something where we may make things worse rather than better, on the other. So, that was by way of a start.

Second, is to say self evidently that it is not over. This phenomenon, whatever it is, is in a very different state in different places: in Morocco, as Michel Foucher and other people were saying, you see a king leading a process of reform that so far looks set to be peaceful. In places like Bahrain, you have perhaps stasis. It is not clear to me whether that is over or whether it will go in some other direction. In places like Syria, we have the most atrocious bloodshed as we speak. In Libya, we had last week elections with perhaps a clearer result than anyone might have predicted; and if you had said to me a year ago that the poster boys of what is happening would turn out today to be Yemen and Libya, I do not think I would have believed you. So we are in the middle of something that has not yet seen its end. Let's be a bit cautious about drawing lessons.

THE LIBYA CAMPAIGN

I did want to talk a little bit about Libya because it is what I know best, it is what I was most heavily involved in myself on the North Atlantic Council last year and I entirely agree with the lessons that General Lange was drawing for NATO and where we go from here at NATO. Particularly, I agree with him in the gaps he pointed to in some of NATO's military

capabilities. They are not the only gaps, incidentally, but they were the ones thrown into relief by the Libya campaign, which stretched us. It was a very small operation, it was small, it was limited, it was quick, it is over.

I do not think NATO has ever done an operation of that size so quickly from start to finish and ending so cleanly with exactly what we said we would do, no more, no less. So in that sense, it looked unchallenging but actually it stretched to the limits an Alliance that already had 160,000 military personnel under arms elsewhere in other operations.

I think that there are some lessons from Libya that we should not draw, though people are very inclined to do so, including in the media.

- Firstly, I think it is premature to draw lessons about U.S. leadership. There is a line that goes, "This demonstrated that the U.S. had ceded leadership to the Europeans, they led from behind," or various variants on this story. Actually that is not so. The U.S. did not regard this as a priority; it had other priorities elsewhere in the world. It had other priorities actually in the region including Iran, including Gulf security, including its concern about Israel and its security, and an operation in Libya was not a priority. But once the U.S. had decided—and for France and the United Kingdom it was a priority—once the U.S. had decided that there would be an operation, U.S. leadership came in in the mighty way that U.S. leadership tends to. It is worth remembering that the U.S. was in the coalition that started the operation. It was in there from day one, it was U.S. military power on day one that made a decisive difference to Libyan air defenses, it was U.S. leadership in the United Nations alongside that of countries like mine and France. And I cannot say that I noticed an absence of U.S. voices in NATO as the operation proceeded. So does this mean that the U.S. is increasingly going to look to Europeans to carry out operations in Europe when they are of interest to Europe? I do not know. I think that it is unproven with this particular instance, with this particular U.S. Administration, with this particular conjuncture, and I think we need to wait and see what happens next. But what I do take very seriously is the U.S. challenge to the Europeans to make sure they can play their part with their own capabilities in operations in which they want to be involved.
- Secondly, there is a narrative about the Alliance being divided and not all contributing. Well, of course there are different views in the Alliance. We are an Alliance of 28 democracies, we all have our own politics, our own differing views inside each of our capitals and parliaments. But it was an extraordinary quick movement from the 17th of February when a Tunisian vendor triggered unexpectedly an uprising to the point where NATO had completely taken over a full-scale military operation at the end of March.

I have never known the North Atlantic Council to move quite so quickly. People had differing motives, differing degrees of enthusiasm, but it was not a divided Council and it was not a divided Council as we went through the operation. It is true that not every country contributed its national armed forces but no country made difficulties about its personnel inside NATO's common command structures. Many countries who did not contribute forces themselves did things elsewhere in theaters like Afghanistan to release the forces that could then be used for the Libyan operation, and there were many countries that simply could not have contributed because, for instance, if you are a landlocked country without a navy, it is quite hard to see how you are going to contribute to a maritime operation. There are countries who had agreed with NATO when they joined that they would not have fast jets because we would do the air policing—hard to see how they could have contributed to that part of the operation. So I think that narrative needs to be buried because it did not actually reflect the political reality as I lived it.

LESSONS FOR NATO

I think that there are some lessons that we do need to learn in NATO. They are beyond the ones that we discussed yesterday. We have a sort of illusion in NATO that what we are doing in Afghanistan is a major expeditionary operation and when that is all over, we need to get back to learning different types of lessons that we have unlearned. Actually, paradoxically Afghanistan is not an expeditionary operation. It is a very static land-based campaign that is now a very mature one with huge bases, huge supply lines. It is not what you would do if you were doing a quick contingency response in which you had to scramble together logistics from the start and do it in a joint way, in a challenging way on short notice with difficult supply lines. We have actually unlearned how to do some of those types of operations, which are not necessarily land heavy. They might be amphibious, they might be quick, they might be joint and we are going to have to practice that in NATO again after 2014.

Then I think there were some other lessons we learned, which was the importance of some principles that we adopted in NATO, principles when we looked at the dilemma that was Libya. We said that we would not operate unless there was a demonstrable need for us to do so, unless there was a clear legal base for doing so and unless there was strong regional support. Now all of those things came together in what was happening, the massacres in Libya, the U.N. Security Council

Resolutions, and the role being played by the Gulf Cooperation Council and then the Arab League, so those three things did come together. NATO has taken this, I have to say, as a sort of litmus test for what we might do in the future. I hope that will prove useful rather than a straitjacket.

But we also discovered some other principles like how important for political solidarity it was not to have civilian casualties. I think that this was the first major air campaign in which precision weapons were used to the extent and in the way in which they were, and the absence of significant civilian casualties (of course there were some) and certainly absence of any that we were conscious that we were likely to create because we took great care to avoid civilian casualties, that was a very important political binding point inside the Alliance and among allies. Then, there were also things we have been aware of in many other areas but that were very clear in Libya, such as the speed of the media, and the fact that people on the ground with their mobile phones have ground truth that was difficult for us to have in a campaign in which we did not have ground forces.

CONCLUDING REMARKS

And here I would just leave the thought with those of you who come from the IT and cyber community that we are tussling as diplomatic practitioners and perhaps as military practitioners with some of the same issues and principles that you are tussling with. So there is a tension between a much greater demand for transparency, for accountability, for openness in what you are doing, and how you combine that with the requirements for security, for privacy, for working out solutions and how you create effect under the glare of publicity.

And as a diplomatic practitioner, I would just say to those of you who are practitioners of other trades that one of the biggest professional dilemmas that we face at the moment is how to allow time for quiet, behind-the-scenes diplomacy, which brings together NATO (which was a very small player in the Libyan campaign), alongside diplomacy, contact groups, the United Nations, and regional diplomacy; how to bring together the space for finding solutions while at the same time accounting for what you are doing almost minute by minute in the public forum.

Chapter 20

Lessons Learned from the Arab Spring

Ambassador Haydar Berk
Permanent Representative of Turkey on the North Atlantic Council

Over the past year and a half, we have witnessed an unprecedented democratic awakening in the Arab world. The Arab Spring was no less than a paradigmatic shift that altered the political landscape of an entire region. It was a delayed process. Over the years, the Middle East had unfortunately become a reference point for conflicts, turmoil and bloodshed. This perception needed to change and we believe that the Middle East region has reached a defining and irreversible turning point that will make change and democratic transformation inevitable.

TURKEY'S APPROACH TO REGIONAL SECURITY

The main principles of our approach to regional security are the following: (a) security for all, without discrimination; (b) enhanced political dialogue; (c) economic interdependence; and (d) multicultural coexistence. In order to achieve security, we firmly believe that:

- Security and stability can only be sustained if the legitimate aspirations of the people are met.
- Countries in the region should be encouraged to implement comprehensive reforms.
- Violence and the use of force are unacceptable.
- The sovereignty, territorial integrity and political unity of each country must be preserved and respected.
- Transformation should be led and owned by the peoples themselves.
- These processes should not be hijacked by radical marginal groups seeking to foment sectarian, ethnic or ideological strife across the region.

THE ARAB SPRING: ACHIEVING A SUCCESSFUL AND SUSTAINABLE TRANSITION

With elections in Tunisia, Egypt and Libya, the region is now at the critical juncture of a process that will take at least a decade. Free elections are the cornerstone. Therefore, the region is just at the starting point since the transition to democracy requires building a wide range of robust social, economic and political institutions. And these institutions need to be built upon a premise of inclusiveness: sections of societies in the Arab world that were formerly disenfranchised now need to find a voice.

Common Features of the Arab Spring Uprisings

In order for this historic transition to be truly successful and sustainable, there must be a strong commitment to institutionalize the change in a way that will realize the democratic and socio-economic aspirations of the masses that initiated this change. In fact, what are the common features of the Arab Spring?

- At the forefront, we see mainly young people; they are well connected to the outside world through social media.
- Slogans are very similar: democracy, freedom of speech, fair share of economic wealth, etc.
- However, crowds are not organized; participants come from diverse walks of life.

Basic Principles for Successful Transition toward Democracy of the Arab Spring Countries

Therefore, there is no single recipe that could guide transition in all of these countries. Each one of the countries will have to work its way towards democracy according to its own set of circumstances. Each country's social structures, estab-

lished institutions, traditions and historical past will shape transition. However, certain basic rules and conditions will have to be met:

- First, as I already mentioned, the new regimes need to be inclusive. The concentration and perpetuation of power and opportunity in the hands of a few caused this cataclysmic rupture. The new institutions need to include and engage all sections of society regardless of their faith and political affiliation.
- Secondly, this process of inclusiveness will have to be enshrined in and guided by a new constitution that will be prepared and adopted with the participation of the entire society to guarantee a truly pluralistic and participatory system based on the rule of law.
- Thirdly, to ensure that change comes through ballots rather than bullets, transparency and accountability will be of paramount importance. In this context, a robust civil society organized through free associations will determine the strength and resilience of these budding democracies in the longer run.
- Fourth, given the multi-cultural, multi-ethnic and multi-religious composition of the Middle East and North African (MENA) nations, respect for minority rights and freedom of faith will be fundamental for a successful transition.

The Need for Comprehensive Economic Reforms

Democracy without economic participation is not sustainable. It leaves the newly created electorate vulnerable and susceptible to manipulation by extreme elements. This means that comprehensive economic reforms are necessary. The entire system of generating and distributing wealth will need to be revised to make it more responsive and relevant to the expectations and aspirations of the people.

State control and ownership of the means of production confer to governments excessive economic leverage beyond fiscal instruments and make it difficult and costly to relinquish power due to the perceived loss of economic benefits they entail. Achieving such change is not an easy task. Squares like Tahrir in Cairo have successfully served as the seats of change but they cannot be the seats of government.

The Arab Spring Will Blossom—But Not Overnight

This process also requires constructive international assistance as much as domestic leadership and ownership. In fact, the events of the Arab Spring have shown us that the peoples of the region are more globalized and connected across borders than the regimes in power. They follow, share and react to the fate and suffering of others beyond their borders with far more empathy and solidarity than their governments could demonstrate. Sovereignty does not give states an absolute right to mismanage their citizens. We all share a moral responsibility to help those demanding a better future from their oppressive rulers. There are valuable lessons from Tunisia, Yemen, Egypt and Libya. Now, Syria is a case in point.

The developments in Syria have entered into a critical phase, which is prone to creating serious risks for regional and international peace and security. The humanitarian situation is getting increasingly alarming. In addition to the ongoing bloodshed, there are millions of internally displaced persons (IDPs) and the flow of refugees to neighboring countries, including my country, already exceeds tens of thousands. It is the collective responsibility of the international community to act swiftly to prevent further bloodshed and to ensure the initiation of a political transition process without delay leading to a democratic and plural political system in accordance with the will of the Syrian people.

From the beginning, Turkey has followed a principled stand. We want to see the Arab Spring blossom in order for the region to be free, democratic, modern and stable. It will not happen overnight. But it can happen.

Chapter 21

Lessons from the Arab Spring: A Russian Perspective

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

The events unfolding in North Africa and the Middle East are often referred to nowadays as the most remarkable phenomenon in global affairs of the 21st century, although the 21st century has just begun. The transformation processes that shook the region reflected quite a natural desire of people there to live in a better social environment, have more opportunities for self-expression, participate in political life, and enjoy economic welfare—an aspiration that they should not be deprived of, and which we, the international community, should strongly support.

Experts have long ago started pointing to the fragility of authoritarian regimes in a number of Arab countries and a high probability of social and political turmoil. In fact, Russian diplomacy was highlighting that prospect as early as the beginning of 2010. But it was indeed hardly possible to predict the scale and rapidness of the wave of change that hit the region. In my view, the lesson is clear: today, no state in the region or beyond is immune to social perturbations unless it modernizes itself, addresses acute social, economic, and political problems left unresolved for decades, and satisfies the basic needs of the population.

These processes are far from being completed, and it seems rather difficult to assess their further evolution since they are often accompanied by painful civilizational, ethnic, and confessional as well as economic and political fractures, putting regional stability at risk. In this regard, it is yet too early to make a final judgment on the lessons of the Arab Spring. It is not easy to mentally put aside specific aspects and see the picture as a whole—in other words, to see the forest behind the trees. For that, we need to wait for constitutional transformations and planned democratic elections and see the path political forces that are coming to power will choose.

ROLE OF THE INTERNATIONAL COMMUNITY

The role of the international community, to put it briefly, is to help the transformation period bring the world more gains than losses. Russia—maybe better than any other country—knows the true price of revolutions. We are aware of the fact that revolutionary changes inevitably mean not only a rollback in social and economic development, but also human suffering and sacrifices. That is why we stand for a gradual and peaceful transformation in the region of North Africa and the Middle East.

Surprisingly, this is not obvious for everybody. As mass popular movements were growing in the region, two major approaches came to dominate: first, the expert discussions on which course of action external players and the international community as a whole should choose, and, later, the practical steps of states as well—either helping the people in the region define their future on their own or, making use of the softening or *de facto* collapse of regimes that were previously too rigid, trying to shape a new political reality to their liking.

Recent events have made it obvious once more that attempts to impose democracy from the outside can—and often do—produce an exactly opposite result. It wakes up underground forces, including religious extremists, who try to change the vector of a certain country's development and challenge its secular system.

Examples are abundant: take the complicated situation in Iraq and the still unresolved crisis in Afghanistan. There is more than enough evidence that things have not been running smoothly in Libya since the overthrow of Muammar Gaddafi. The wave of instability has reached countries further down in the Sahel-Sahara region. I may only mention the situation in Mali. Egypt, the historic leader of the Arab world and for decades the linchpin of whatever fragile stability in the Middle East, a country where the actual transition of power was not accompanied by large outbreaks of violence, is still far from calm waters. The recent political turmoil over the parliamentary and subsequent presidential elections has minimized Egypt's regional standing. Besides, reports of a growing number of ethnic clashes and violations of rights of the Christian

community cannot but cause concern.

Perhaps I should also refer to events that have been unfolding in Bahrain in the last several days that are notably almost totally ignored by the Western media, with police violently cracking down on peaceful demonstrators.

THE SYRIAN CRISIS

There are more than enough reasons to adopt a balanced and moderate approach towards today's most acute situation in the region—the Syrian crisis. Naturally, after what happened in Libya, it has become impossible to follow the pattern of vague decisions in the U.N. Security Council which leave free space for arbitrary interpretation. The Libyan people still feel the consequences of irresponsible actions by our partners. It is also a lesson, in a way.

That is why it is important to understand what is really going on in Syria and what can be done to overcome the current painful stage in its history. Unfortunately, there is still a lack of qualified and fair analysis of the events in Syria and their possible implications. Instead, we often have to deal with black-and-white propaganda clichés. At the same time, one should ask oneself—how does the government that has allegedly lost popular support manage to stay in power for more than a year despite far-reaching sanctions adopted by its main economic partners? If fear were the only reason, why did it not help the other authoritarian rulers?

Obviously, the Syrian leadership bears the main responsibility for the crisis that hit the country. It had not embarked on the road to reform in time and had not drawn the lessons from the deepest changes affecting the region. That is correct. However, another factor is true as well. Syria is a multi-confessional state where Sunni and Shia Muslims live side by side with Alawis, Orthodox and other Christians, Druses, and Kurds. And undisputedly, over the last decades freedom of worship has de facto existed in Syria. Today, however, representatives of religious minorities fear that this tradition can be broken if the regime is overthrown. Indeed, historically, Syria was never at the bottom of the list in any rating of human rights and basic freedoms. In fact, its place was much higher than that of some countries whose leaders today try to give Damascus a lesson in democracy.

So without the slightest reason or inclination to act as an advocate of the Syrian president, I would challenge those who see that the only way to settle the crisis is forcing Bashar al Assad out of power immediately despite the will of quite a large part of the Syrian population who associate their welfare and security with the current regime and claim that the most probable outcome of this course of events would be Syria sinking into the chaos of a protracted and bloody civil war with unpredictable consequences for the broader Middle East. The role of responsible external actors should be that of helping the Syrian people avoid this and ensure that a Syrian-led political process leads to a transition that meets the legitimate aspirations of the Syrian people and enables them independently and democratically to determine their own future.

RUSSIA'S POSITION ON SYRIA

It is obvious that a continued and perhaps numerically expanded presence of U.N. observers is essential. That is precisely why Russia has submitted a draft U.N. Security Council resolution to that effect. And this view was fully supported by the special envoy Kofi Annan during his talks in Moscow over the last two days.

In the real conditions of today's Syria, orientation towards unilateral support of the opposition, and particularly of its most militant part, will not lead to a rapid establishment of peace in that country and hence is contrary to the goal of protecting its civilian population. It seems as if elements of a big regional geopolitical game dominate here. The latest piece of evidence confirming that conclusion has been the attempt to turn the U.N. observer mission into a bargaining chip, coupled with blackmailing Russia and China over a possible U.N. Security Council resolution.

Instead of rushing towards further sanctions and insisting on engaging Chapter 7 of the U.N. Charter, thus opening the road to armed intervention, Western countries should live up to their commitments taken at the Geneva meeting of the Action Group on Syria on June 30th, namely and I quote, to "apply joint and sustained pressure on the parties in Syria" in order to secure full implementation of Kofi Annan's six-point plan and Security Council Resolutions 2042 and 2043.

Without that, I dare say, bloodshed such as what we have been seeing in Damascus these last few days will go on. If we wish above all to stop the bloodshed, and that is exactly what we should focus on, we should notably seek a durable ceasefire first of all and contribute to launching an inclusive pan-Syrian dialogue to enable the Syrians themselves to elaborate a formula for a peaceful resolution of the crisis. That explains the Russian position on Syria.

SETTLING CRISIS SITUATIONS

In this regard, Yemen is a glaring example of how crisis situations can be settled. There, the parties directly involved managed to reach a compromise following long and strenuous efforts and thanks to the important role of the Gulf Cooperation Council. Yemen's example has proved that: to settle an internal conflict, all parties directly involved should be confident that the international community will act on the basis of firm principles, speaking with one voice and seeking to stop the violence and ensure the conflict settlement through comprehensive dialogue.

Only thus can the Middle East region be prevented from descending into bloody wars and anarchy and stay, as some like to say now, on the right side of history. We are confident that other scenarios implying outside interference in Syria—from blocking undesirable TV channels to piling sanctions upon restrictions to scaling up arms supplies to the opposition forces and air strikes—none of that will bring peace, neither to Syria, nor to the region as a whole.

We also cannot afford to forget the remaining protracted conflicts in the region, first and foremost the Israeli-Palestinian one. Clearly the ongoing large-scale transformation of the Arab world does not contribute to their resolution. True, everyone is preoccupied today with acute domestic problems. At the same time, it seems like certain international actors are so much engaged in the Libyan and Syrian conflicts that they have no time left to address chronic regional conflicts. Meanwhile, progress in settling the Palestinian problem could improve the general atmosphere in the Middle East, ease confrontation and calm down extremist sentiments.

And another, more general observation: The Arab revolutions show a clear tendency in those countries towards going back to the historic roots of their civilization. At this stage, it is reflected in broad public support for parties and movements acting under the banner of Islam. Actually, this phenomenon goes beyond the Arab world: suffice to mention Turkey which increasingly tends to position itself as a self-standing center of power and a prominent actor in the Muslim world and in the broader Middle East region. In the context of a multi-dimensional geopolitical reality where no single system is able to dominate economics, politics, and ideology on a global scale, we can expect still higher weight of the factor of civilizational identity in global affairs.

With regard to practical politics, it can only mean one thing: attempts to impose one's own system of values upon others have absolutely no chance of success. It can only result in a dangerous increase in intercivilizational frictions. Of course, this is not to say that we should fully abandon exercising influence upon each other. But this should be done in a fair and open manner through enhancing the export of one's own culture, education and research while fully respecting civilizational values of other nations as a prerequisite for maintaining the world's diversity.

CONCLUSION

I would like to conclude on an optimistic note, expressing the hope that the changes taking place today in many countries of the region of North Africa and the Middle East will have a positive effect and will ultimately let us see these countries get stronger and enter a qualitatively new stage of political, social, and economic development. I am confident that it is in the interest of all the international community.

Part Two

The Rapid Growth of Cyber Threats, the Possible Contributions of the Defense Industry and The Way Ahead for Global Security

Chapter 22

Welcoming Remarks for the U.S. Deputy Secretary of Homeland Security

Rear Admiral Nicola De Felice
Director, Centro Innovazione Difesa (CID)
Department of Plans and Policy, III, Italian Defense General Staff

Today I have the honor and pleasure to introduce to this audience the second in command of the mighty battleship called the U.S. Department of Homeland Security: the Honorable Jane Holl Lute, Deputy Secretary of the DHS. Deputy Secretary Lute is not only the Executive Officer (XO) of the Secretary, Ms. Janet Napolitano, she is also Chief Operating Officer, responsible for the day-to-day business and management of this kind of aircraft carrier's fleet with a crew of 240,800 people. Among the many operations for which Ms. Lute is responsible, her department is always prepared to face any kind of disaster and fight against threats of any type.

Talking about global security, and especially about cyber security, the U.S. Department of Homeland Security plays an important role in countering these cyber threats, and Ms. Lute, due to her more than 30 years of military and senior executive experience in the U.S. government and in the United Nations, is the best placed to prevent and deal with "torpedoes" launched by the fleets of her country's cyber adversaries.

She is building one of the best teams anywhere to keep U.S. federal civilian networks secure, and secure cyberspace and the critical infrastructure on which the U.S. depends. That means working across the federal government, partnering with the private sector, and promoting cyber security knowledge and innovation.

We thank Deputy Secretary Lute for being here in Italy and for sharing her experience with us.

Chapter 23

Cybersecurity Keynote Address

The Honorable Jane Holl Lute
U.S. Deputy Secretary of Homeland Security

This morning, I would like to discuss how we are viewing the problem and challenge of cybersecurity within the U.S. Department of Homeland Security. There are two things to note: Everybody is talking about cybersecurity today, but—we can be frank—not everybody understands what cybersecurity means; moreover, not everybody understands what Homeland Security means for us in the United States. For those of us in Homeland Security, it is true that we have extraordinary brand name recognition. Everybody has heard of Homeland Security and it is true that we have 210,000 federal and military employees; we also have about 200,000 contractors who now work in Homeland Security. We are the third largest U.S. government department.

Although everyone has heard of us, not everybody understands what we do and not everybody understands how cybersecurity fits in with what we do. I would like to talk about that. Beyond this, I would like to discuss how what we do in cybersecurity is deeply affected by the very significant changes that are going on around the world with respect to the Internet, some of the challenges that we face, and offer some ideas about how we are trying to address the challenge of ensuring cybersecurity in the United States.

WHAT IS HOMELAND SECURITY?

What are we trying to do in Homeland Security? We say that we are trying to create a safe, secure, resilient place where the American way of life can thrive. In order to do that, we think that we need to do five things:

- Prevent terrorism,
- Secure our borders,
- Enforce and administer our immigration laws,
- Ensure our cybersecurity, and
- Build national resilience.

You may have heard of the United States Coast Guard, FEMA (Federal Emergency Management Agency), the Transportation Security Administration, Customs and Border Protection, our Citizenship and Immigration Services and our Transportation Security Agency. All of their activities relate to these five missions. And we call cybersecurity a critical mission of Homeland Security because it is impossible to imagine a safe, secure, resilient place where our way of life can thrive without a safe, secure, resilient, cyberspace. At the heart of a secure cyberspace are two challenges, which constitute the irreducible minimum with which we must be concerned: confidence in the integrity of our information and in the security of our identity. The rest is commentary.

As we look at the mission of cybersecurity, we can see a certain duality with respect to all our other missions in Homeland Security. For example, keeping our borders secure means being on guard to keep out people or things that might be dangerous. On the other hand, we want to expedite legitimate trade and travel. As a result of this duality of intention, tension exists in almost all of the missions that we confront in Homeland Security.

WHAT IS THE ROLE OF GOVERNMENT IN CYBERSECURITY?

Just as it is for our other missions, whether it is border security or immigration, the challenge is "What is the role of government?" In cybersecurity, this is not a settled question by any means. None of us who represent governments in this room have the corner on the market in providing cybersecurity. So we are present at a moment when we have to verbalize

and articulate the role of government on this question.

Why is this question even interesting? It is interesting in part because, typically, security is the role of government. When it comes to cybersecurity, however, government does not have this role exclusively. While I recognize that what I am saying to this audience is perhaps is a little provocative, let me go ahead anyway and say that when we speak about power, for example air power or sea power, you cannot talk about cyber power in the same way. There is no corner on the cyber power market. In fact, governments are not even the dominant player when it comes to cyber power. They are one among others, and this reality is only slowly seeping into the minds of governments as they wrestle with the challenges of what to do about the security of cyberspace. And this also means that there is a bit of a tension here as well. On the one hand, governments are typically given responsibility for ensuring the security of their populations and the security of their enterprises; on the other hand, it is not yet the case in cybersecurity.

In this way, it is possible to see the difference between what we call in the United States national security and Homeland Security. Homeland Security is of course an aspect of national security but it is not the same thing. National security is strategic, centralized, and top-driven. Homeland Security is operational, distributed, and bottom-driven. It is driven by communities, states, and municipalities in the United States. National security has a predominant culture of the military, of the Intelligence community, and, you might say, of Washington. Homeland Security's culture is law enforcement, emergency response, and the homeland. It is a very different culture. It is not unity of command. It is unity of effort. It is not "need to know for information," it is "duty to share." So, when we talk about cybersecurity, it is very important to understand that this is a very different environment.

THE CYBERSECURITY BACKDROP

As I lay out the problem and think about what my department should do, I would like to make two other observations, since our department has been given the principal responsibility for leading the U.S. federal government efforts on cybersecurity. I think there are two significant trends that are worth talking about.

Technology is an actor. My first observation is that technology is an actor in the question of cybersecurity. Once again, this is unusual because the security actors are typically governments, nation states, and some non-nation state actors that figure prominently in today's world. With cybersecurity, however, technology is an actor with standing, power, and influence. Moreover, technology is way out in front of all of us. This is a little ironic because in English, technology is precisely the word we use to describe tools that come into our grasp. Yet today, technology is the word we use to describe things we do not understand. It is technology. And we are not just leaving it to the experts. We are leaving it to the next generation. Our kids know more about technology than we do and ever will. So technology is a wave that is way out in front and it is animating everything we do every day in modern society. It is being trailed by the social wave, since all of our societies are trailing technology, and trying to keep up. Lagging further behind is the law. The law is always the lagging indicator, but this situation is even more pronounced in the case of modern technology and challenges like cybersecurity.

A change in public expectations. The second observation I would make is that the public is changing, and with these changes come changing expectations of their governments. What do we expect from our government? Typically in the United States and anywhere around the world where I have been—and I spent a long time in the United Nations—I can tell you that people do not interact with their governments unless they have to. People are changing though. Increasingly, we see powerful public expectations of inclusivity: "Nothing about us without us." There are very powerful expectations of transparency: "What is going on? I have a right to know." There are powerful expectations of reciprocity: "How come she gets that and I do not?" And there are very powerful expectations of accountability.

So how are governments doing? When you talk to your citizens and ask, "What do you expect from your government?," you find that they expect a clear value proposition and they expect us to deliver on that value proposition in three key areas: security, well-being, and justice. Our societies expect threshold conditions for security, well-being, and justice and beyond threshold conditions, they expect their governments to provide clear value in these areas.

Social anger, anxiety, and loss of trust. But what is happening? A growing number of people around the world are finding these things on the Internet. They find an opportunity for expression, they find common travelers and common causes, they find an opportunity for well-being and some version of justice. Who interacts with their government 14 hours a day? It is those of us who work for the government. Others do not. Yet people will spend 14 hours a day, 12 hours a day, eight, six, or pick a number, on Facebook. In fact, there are only five things I can think of in the world that claim the active affiliation of a billion or more people: being Indian, being Chinese, being Catholic, being Muslim, and being on Facebook—a billion people. People are changing and their expectations of government are changing. People are also angry. My col-

leagues and I spent the last two years in a negotiation with the EU on something called Passenger Name Records (PNR). I was the lead U.S. negotiator and it was an extreme pleasure. We traveled everywhere throughout Europe, my colleagues and I, and we saw the social anger that you know exists there. There are angry people in the United States as well; people are angry in many places around the world. I have seen a lot of social anger over the course of my career. I have seen purpose-driven social anger and people kill each other with that kind of anger. This is not that. This is an anxiety-based anger. People are deeply anxious and I wonder if that anger or that anxiety stems from the fact that we feel like we have lost the ability to institutionalize trust. We cannot trust the media, we cannot trust the market, some say we cannot trust the government, we cannot trust big institutions; they have let us down and failed us. It is not only that we do not trust these institutions, we do not know how to "architect" trusted institutions, some say. That will matter a lot in the Internet age. That matters a lot in cyberspace and we have to find ways to answer these questions.

ATTEMPTING TO DEFINE THE GOVERNMENT'S CYBERSECURITY ROLE

So this is the backdrop against which we look at the challenge of playing our role in cybersecurity. As we confront the increasing need for the Internet, we confront an increasing need for cybersecurity. So we look at the three questions that lie at the heart of every policy maker's day; What is the problem? What can we do about this problem? And who should do the work?

What is the Problem?

What is the problem? The problem is that we have a comprehensive reliance on the Internet. Cyberspace is the endo-skeleton of modern life. We cannot imagine our modern societies without the Internet today. Combined with that, there is also rampant exploitation, theft, and other malicious activity going on. And third, there are no clear assignments of responsibility for ensuring the safety and security of all of us in cyberspace. So we have comprehensive reliance in an environment where there is rampant exploitation and no clear assignments of responsibility to keep us safe. That is the problem.

But the Internet itself is characterized by distributed ownership, dynamic connectivity, very diverse systems that are nevertheless connected, and instantaneous but organic growth patterns. Yes, it relies on machines that are located somewhere, connected by the global telecommunication system that spans the globe. Yet the Internet is a place where geography and borders matter differently than they do ordinarily. It is not that they do not matter; it is that they matter differently than in physical space, since the reach of national law is incomplete and since the role of governments in security is an open question. That is what we face today.

What Should Be Done?

So what should be done about it? I will offer what we are doing in the United States and what we are doing in Homeland Security. We are doing three things: We are securing dot.gov (i.e. government networks); we are helping to build a healthy cyber ecosystem; and we are looking increasingly for more international collaboration. Let me briefly discuss each of those.

In securing dot.gov, there are again three parts. In the first instance, we are putting in place policies, practices, and procedures to deal with access, database management, workforce cyber skills, supply chain management, removable media, secure database storage facilities, cloud computing, etc. All of this has to be mapped and we are doing that. Secondly, as we are developing and implementing these policies and procedures, we are requiring people to know more about the state of their cybersecurity and their relationship to it: Who is on your networks? What data are you holding? What software, what hardware, what kind of configurations do you have? I am not a technologist and I am not likely to become one in the remaining years of my professional career, but we rely increasingly on technologists and those technologists have to come together with policy makers and with the programmatic community to create a world that we can live in—because not everybody works on cyber but everybody works in cyber. So these policies, practices, and procedures have to be pragmatic and workable from an operational and policy point of view. That becomes complicated, but it is not impossible.

The second thing we are doing is implementing what we and the technical community increasingly call critical controls. There is a list called the 20 critical controls. Twenty is a big number when you are in government looking for policies to put in place and we are beginning with five that are the most critical: hardware asset management, software asset management, vulnerability management, configuration settings and controls, and then antivirus as well. So we are putting in place a broad foundation of policies, practices and procedures. We are implementing these 20 critical controls and establishing a

framework for continuous diagnostics so that we can know from an automated sense all the time what is going on, what is on our networks, what should be on our networks, what does not belong on our networks, and how to take remedial steps to ensure that they remain healthy.

In securing dot.gov, we are also establishing a perimeter intrusion defense strategy that works in real time on the basis of information sharing of all of those on the network. So the first thing that we are doing in dealing with all of these problems is securing dot.gov. When you sit on an airplane and they walk you through the safety measures, they say, the air mask will drop, please affix your own air mask before attempting to help the person standing next to you. So this is a little bit of affixing our own air mask when we work on securing dot.gov.

The second thing that we are trying to do, and we are doing it at the same time, is to architect and help create. We are only one among a number of players in a healthy cyber ecosystem, in which we have smart machines and smart users. They have access to real time threat and vulnerability information and can move and share that information quickly. We know we cannot do this alone, but we consider it to be a process of education, helping to identify and baseline security measures and standards and figuring out how to incentivize improvements.

The third thing that we are trying to do in this ecosystem is work with industry on innovation, commercializing promising technologies, while sharing information and lessons learned. Also, while we are working on securing dot.gov and building a healthy cyber ecosystem, we are trying to work collaboratively on the international scale. It is an important dialogue in which we are participating this year; it has been going on for some time now and we are actively a part of it.

Who Should Do the Work?

I have already discussed how we think about the problem and what can be done about it. Let me turn now to who should do it. Let me assert that, from our perspective, cyberspace is civilian space. There is a lot of exploitation going on in cyberspace right now, but we cannot manage it. It is not in our view a war zone, so we cannot manage it as a war zone. It is a contended space to be sure, but—nonetheless—it is civilian space.

Having said that, the status quo is not acceptable because there is rampant exploitation and other malicious activity going on. So governments must act but governments cannot do all that needs doing. The current debate in fact is very polarized: on the one hand are those who say, "Let the market handle this." We do not ask the market to handle anything exclusively and it certainly cannot handle the challenge of cybersecurity alone. On the other hand, there are those who say, "This is too dangerous; the problems of cybersecurity are too extensive; governments must come in and impose rules and regulations and retake ownership of the Internet."

We do not agree with that either. It is not feasible, nor is it desirable. Governments cannot do all that needs doing here and we also know that all that needs doing cannot be done alone. So our position is in support of the multi-state model to ensure an open, accessible, reliable and secure Internet. It is vital to have international cooperation to achieve this. Among governments and other stakeholders, it is equally vital to have that cooperation with the private sector. We have to find ways to jointly support research and innovation, entrepreneurship, economic growth, and the development of critical cyber skills because this is a highly technical world.

Over the past three and a half years when I have been in the Department of Homeland Security, I have thought a lot about this. Prior to that, I spent my entire career in international affairs, foreign policy, and in national security. One thing struck me about the coincidence of these two experiences: For seventy years, it has been the shadow of our most destructive technology that has given us the clearest evidence of our shared humanity; today, it is our most promising technology that does so. We are in this together, but we cannot sacrifice security simply for the sake of maintaining an open Internet and we certainly will not sacrifice openness for the sake of security. Can we find a way to bridge this gap? Yes, together, I am confident that we can.

Chapter 24

Planning for the Future Cyber Security Environment

Mr. Steve Grobman
Chief Technology Officer, McAfee|Intel Technologies

In my presentation I would like to provide some insight into what the world is going to become and, at the same time, offer some thoughts about understanding today's cyber threat. Understanding it is critical, but it is not sufficient. Cyber is somewhat different from other challenges because of the speed of its change. For example, if we work successfully on achieving an understanding of today's cyber threats and reconvene, let us say, in 2015, we might arrive at a situation of complete failure, because the world will have changed. Therefore, it is critical to focus on where the world is going and how it is evolving so that we can deal with today's threats but also make sure that we are prepared for the tools that cyber threats will utilize tomorrow.

Earlier panels discussed the important point that there is no clear delineation between consumers, private sector, public sector, and defense, although we would often like to convince ourselves that these areas are separate. As I go through my presentation, you will see that they are interrelated, that they will become even more interrelated and that, in many cases, this is intentional. So, if we are to succeed, securing all of those realms is absolutely critical. Finally, several speakers have expressed great concern over budget reductions that might not make it possible to solve some of the big problems that we have in the world. In these areas, technology is a very helpful tool and we need to enable it so that it can successfully assist with the critical challenges that every country's population deals with. Cyber security must not be an impediment to those areas.

So, when we think about the future, I would like us to think about some big trends that are occurring right now and which will have a profound impact on our way to deal with the world's computing environment: What are the technological evolutions that we see around us? What will the world look like in 2015-2016 based on some of the things that are in early incubation today? What does the Cloud really mean to cyber security? How does the change in the devices that we all use impact cyber security? All these changes will lead to new threats, new challenges, and require new approaches to address their cyber security implications.

THE NEW APPLICATION LANDSCAPE

Let us start with what I call the new application landscape. In the past few years, something truly phenomenal has happened, which is about to get another big push. It is a fundamental change in the way applications are developed, distributed and sold. Take for example your own computer that you have at work or at home. Either you or your IT department probably installed a handful of applications over the last year. Typically, these applications are coming from well-understood and well-regarded companies that you know and trust. Now, compare and contrast this to your experience with devices like iPhones, android devices, or the upcoming Windows 8 architecture where every developer on the planet has the opportunity to create and sell software to every other user on the planet. That is a profound change in the way software is being developed and delivered. Finally, compound that with the rate and pace of development in this new environment compared to what we are used to. Instead of installing three applications a year—a TurboTax if you are in the U.S., or Microsoft Office, or other very well understood applications—you are installing applications that will make you most productive in your job regardless of who developed them. Of course, the breadth of software that is becoming available is phenomenal in its ability to provide solutions to some big challenges. At the same time, this new situation changes the security paradigm and we need to figure out how to address it. We need to understand how to deal with the rate and pace of those applications and how to secure systems when anybody can develop software that ultimately lands on a platform.

THE CONSUMERIZATION OF IT

When we link this new applications landscape to the next big trend, which is the very rapid move to the consumerization of IT, this means that someone in a company can bring home a device that is being used in many of these enterprise environments and give it to his/her kids. The kids are installing applications on this device and the company's IT department allows the employee to use that device for knowledge-based work in the office. According to a recent study, 95% of private knowledge workers are using personally-owned devices in the workplace and this brings a major improvement to productivity. At the same time, when we think about some of the goals that groups like ours have traditionally established for cyber security, these goals are about isolating environments, separating consumer life from the enterprise, and separating the enterprise from the public sector and defense. Then we start to see that devices will go home, get applications installed in consumer environments, and then go into suppliers that are directly involved in the supply chain for all of the critical infrastructure components that our various countries depend on. So, we want to figure out the right technologies that will enable IT to facilitate this paradigm where workers who are under very tight controls can be more productive, versus simply using policy to prevent those sorts of actions from moving forward.

THE NUMBER AND COMPLEXITY OF DEVICES

Another big challenge is complexity. If we look at the number of devices that exist, they cover not only consumer mobile devices that are becoming very prevalent but also all the connected embedded devices that we see in every aspect of our future world. These embedded devices are part of industry regardless of whether they are part of critical infrastructure, energy, or even for marketing, such as digital signage. The number of connected devices is exploding and we expect to see nearly 50 billion connected devices in the coming years. Very often there will be no human interacting with these devices. In order to secure this new environment, industry will therefore need solutions that will have a level of resiliency, recoverability and automation that will not require human intervention. There are not enough humans on the planet to stand in front of 50 billion connected devices and get them back in business when a major cyber incident happens. So, planning for that future environment will require a very different thinking.

THE SHIFT TO THE CLOUD

The final big trend that will have a major impact on the world is the shift to the Cloud. There are two elements to the Cloud that we need to consider from a cyber security perspective: the private Cloud and the public Cloud.

The Private Cloud. In the private Cloud environment, we see the existing private sector and, potentially, some government entities, taking advantage of the cost efficiencies, inherent elasticity, and agility that the Cloud offers. Yet, we need to give these private sector users the same level of assurance that they had when they were running infrastructure in a private data center. In a private data center scenario, IT has a very good sense of what is running, where it is running, and who is the operations team behind those assets. In a private Cloud environment, however, at least some of those factors are going to be potentially delegated to other individuals where the inherent level of trust is degraded. So, this is where we are looking at technical solutions to help solve those problems.

The Public Cloud. In my view, the public Cloud does for the infrastructure what the new applications landscape has done for the endpoints. In my opening remarks, I mentioned that this new applications landscape enables anyone on the planet to become a software developer and to sell his product to anyone else. The public Cloud does the exact same thing but from an infrastructure perspective. What this means is that anyone can create a worldwide data center presence with immense computing and network bandwidth in a very short amount of time and extremely cheaply. What will this lead to? There will be an explosion in the quantity of dynamic content living in the public Cloud. So, given that the barrier to entry has been substantially lowered in order to achieve a worldwide data center presence with this very capable computing environment, there will be all sorts of new dynamic capabilities but, in general, those capabilities will not have the same level of rigor and management that we have seen in a classic publicly-facing data center-managed environment. There will be unpatched servers and unmanaged servers. There will also be dynamic content written in ways that are not put through the scrutiny that is customary in the traditional private software environment. We need to know how to react to that very quickly because the underlying infrastructure is very powerful and the next wave of cyber threats is likely to target this new environment in the public Cloud and use it as a launching point to attack public infrastructure, critical infrastructure, and the private sector. So we must give a lot of thought to the implications of the public Cloud.

ACQUIRING INFORMATION TO UNDERSTAND THE NEW ENVIRONMENT

Putting all these together, the threat landscape will change but in the end, the equation describing that landscape will remain somewhat the same. There will still be techniques but they will be different, taking advantage of the old tried and true methods as well as of new things based on the new trends that I have mentioned. The targets will change. We will not only see traditional targets, we will also see combined attacks; attacks simultaneously on phones, PCs, and infrastructure. Motivations will change. In addition to what we see today, more groups will have the ability, either directly or through others, to exploit this new environment. Although this new environment does add new levels of complexity, it is a solvable problem but the tools and techniques will need to change. The way that the security industry has looked at protecting cyber over the past 20 years is still necessary but it is insufficient. We can try to compile a list of known "bad" issues but we also need to comprehend this new world in which a lot of dynamic content can be good or bad—we do not know. We need to focus on things like isolation all the way down to a very micro level on individual devices. We need to comprehend vast amounts of information on what is going on in an environment.

If we look at cyber today from an attacker's perspective, it is very much like a rat in a maze where the rat can go down the wrong turn and hit a wall without penalty: he still has the full ability to get to his goal. Attackers today will keep probing. We may have done a good job patching all sorts of areas in our environment but if attackers can find just one area that is still vulnerable and exposed, they will get through. We need to change that paradigm and move from a rat in a maze type of thinking to one where the attackers need to be on their guard. For example, if they trip a single alarm, we can catch them, lock them out, and prevent them from achieving their ultimate goal. The way to do this is to acquire vast amounts of information, to correlate that information, and provide new solutions based on this big data problem. It will also require taking advantage of technology at many levels of the stack. So, we need to rely on the Cloud, on capabilities on the endpoints, and on a new hardware foundation to facilitate these goals.

LOOKING AT CYBER SECURITY TO ENRICH OUR LIVES

Finally, I want to mention how McAfee and Intel fit together in all of this. Intel has a vision to create computing technologies that will connect and enrich the lives of every person on earth in this decade. If you think about why we are here talking about cyber, it is because the world has seen that this technology has the ability to enrich all lives. We need to look at cyber security as an enabler to enrichment, not as a problem. Going back to manual systems, or systems that are highly inefficient or cost ineffective, is not the right direction. I hope that, by working together, we can put the right controls in place and provide the right technology so that Intel can really achieve its goal of using technology for this purpose.

Chapter 25

Cyber Security in an Age of E-Diplomacy

Ambassador David Thorne
United States Ambassador to Italy

THE AGE OF E-DIPLOMACY

We have entered the age of e-diplomacy. From 2000 to 2010, global Internet usage increased from 360 million to over 2 billion people. Twitter and Facebook users have now topped 1 billion. Political decision-makers cannot ignore the powerful influence of social media in shaping opinions and attitudes. In some cases, the impact has overthrown autocratic governments as you know and as we saw during the events of the Arab Spring in Tunisia, Egypt, and Libya. The State Department, as the main U.S. foreign policy agency, has taken the lead for the rest of the U.S. government in this area and has created the office of e-diplomacy which uses the Internet to advance our foreign policy initiatives. Here in Rome, we engage in e-diplomacy of our own, tweeting and updating our embassy Facebook page for which we have now reached nearly 7,000 fans. It is not a whole lot compared to Facebook, but it is a big improvement compared to what the U.S. Embassy was doing before. Protecting our ability to engage in e-diplomacy is part of a larger cyber diplomacy effort encompassing a wide range of U.S. interests in cyberspace. These include not only cyber security and Internet freedom but also Internet governance, military uses of the Internet, innovation, and economic growth. Cyberspace has also become a foreign policy issue in multilateral fora, in our bilateral relationships, and in our relationships with industry and civil society.

BUILDING INTERNATIONAL NORMS OF STATE BEHAVIOR IN CYBERSPACE

In May 2011, the U.S. Administration released an international strategy for cyberspace that lays out our foreign policy in this area. In partnership with other countries, the State Department is leading the U.S. government's effort to build consensus around voluntary international norms of state behavior in cyberspace. To more effectively advance the full range of U.S. interests in cyberspace, Secretary Clinton established the Office of the Coordinator for Cyber Issues in February 2011. In addition to the State Department's efforts, the U.S. government is taking a comprehensive approach to maintaining cyber security both internally and externally. State Department employees are continually educated on cyber threats and State Department employees (including myself and I did pass the first time around) have to pass a cyber security exam in order to access our computer system.

ENCOURAGING BUSINESSES TO USE TECHNOLOGY FOR GROWTH

Another critical initiative is the 2010 memorandum of agreement signed by the Secretary of Defense and the Secretary of Homeland Security. This memorandum enhances cyber security collaboration between the two agencies. Any discussion of government activity in this room should not be allowed to distract from the core element of this issue. In short, a secure Internet is the virtual bloodstream of all our Internet activity today. Having come to e-diplomacy from the private sector, I can attest to this from my own experience. In a May 2011 McKinsey and Company study, which looked at 13 countries that account for 70% of the world's GDP, they found that the Internet accounted for 3.4% of global GDP growth. Even more importantly, however, was the key conclusion that the Internet is a critical element of future growth. Protecting this rapid growth at a time when economies face acute challenges is vital to economic security. We must protect small businesses as we must protect big businesses. Over the last few years, I have been encouraging the use of the Internet for commerce here in Italy. Through various digital economy forums held throughout this country, we hope to encourage businesses here

to use technology to grow. You want to catalyze innovation, entrepreneurship, and job creation, particularly for the small and midsize enterprises.

CYBER THREATS TO INTELLECTUAL PROPERTY AND CREDIT CARD INFORMATION

The cyber threats to Internet commerce and finance from hacker attacks seeking to obtain credit card information or steal intellectual property can have a very damaging effect on small and big businesses. While the threat to intellectual property is often less visible than other threats, it is probably the most pervasive cyber threat today. Every year, an amount of intellectual property larger than that contained in the Library of Congress is stolen from networks maintained by U.S. businesses, universities, and government departments and agencies. Sustained intellectual property losses erode any country's national competitiveness in the global economy. But stealing is cheap and profits are easy.

According to Symantec statistics in 2010, stolen credit card numbers retail for between $.07 and $100 on the underground market and the more you buy the cheaper it is. The data breaches are not only problematic for the individuals whose information is compromised but they cost companies billions of dollars. The private sector is working hard and spending money to protect its infrastructure. According to a report published by the Ponemon Institute in August 2011, the median cost for fighting cyber crime in the 50 organizations they studied is $5.9 million per year with a range of $1.5 million to $36.5 million each year per company. This cost has increased from the previous year's study.

Our governments need to catch up and provide sufficient protection at the national level. The U.S. Defense Department has requested $2.3 billion for the U.S. cyber command in 2013. Of course, private security investment is a much higher number. Congressional funding for the U.S. government request will establish and institutionalize the importance of cyber security for the U.S. government.

COLLABORATING FOR BETTER CYBERSECURITY

Our internal cyber security can only go so far. The Internet is global and countries need to collaborate to protect critical infrastructure. This does not necessitate a global centrally-governed structure to impose rules and regulations on the Internet. But we should build closer ties for our cybersecurity architecture. Our methods and counter-methods need to be more sophisticated and we need to strike a balance between protecting data and sharing information to combat a common enemy. We are on the right path for better cybersecurity, but we need to accelerate the process to avoid what Secretary Panetta has called a Cyber Pearl Harbor. This is not only to protect critical infrastructure and banking systems but also to protect intellectual property and private industries that are fueling economic growth globally—and even more importantly to keep the Internet available to everyone. In so doing, we will also preserve the ability of peaceful protest movements promoting democracy to reach a global network.

Chapter 26

Key Dinner Address: Italy's Views on Cybersecurity

Senator Francesco Rutelli
Member of the Italian Senate; former Mayor of Rome

As the only Italian politician speaking here, which is a bit scary, I will try to approach the topic of cybersecurity from an Italian perspective and less as a politician and more as a representative of the institutions. That is what I did a couple of years ago when, as the chairman of the Parliamentary Committee of Intelligence Overview, I presented a report to the Parliament on the risks of cyberspace for national security. Still today, it is the only official document on this topic in Italy and the main reference for the necessary implementation that my country needs to do at all levels to prevent any disruption coming from cyberspace. It brings together the best efforts from the private and public sectors—including the Intelligence services—to prevent any potential attack to our vital networks. I believe that the ideal mix of this audience, made up of representatives from governments and the private sector, can really appreciate this effort that we are leading.

One of the main features of the international arena in this 21st century is the diffusion of power. It is a structural revolution that we have been experiencing, at least since 1648, when in Westphalia the principle of national sovereignty was established. The Internet, since its debut in 1989, has revolutionized commerce, communication, governance, and even military action. Much of the modern world is simply inconceivable without it. The revolution, however, has not come without a price. The annual cost of cybercrime has now climbed to more than $1 trillion, while coordinated cyberattacks have crippled Estonia, Georgia, and Kyrgyzstan in recent years. There is an escalating number of attacks between two uncomfortable neighbors like India and Pakistan and the news of a computer virus like Stuxnet slowing at least the process of uranium enrichment in Iran has disclosed a new dimension for strategy and international security. The central features of this cyberworld are the interconnections of global communications, information and economic infrastructures, and the dependence upon these infrastructures in order to govern, to do business, or simply to live.

OBSERVATIONS CONCERNING THIS NEW CYBERWORLD

Growing dependency. First, the new cyberworld is still evolving. Economically developed societies are becoming even more connected within themselves and with others, and all are becoming dependent upon the rapid and reliable transmission of ideas, data, and information. Second, when dependency is not governed, then this global network becomes vulnerable to information theft, electronic crime, malicious attack, or even asymmetric offense. In this sense, along with land, sea, air and space, the cyberworld can be used as a strategic tool. Cyberpower can be used in peace and war, because it is stealthy and covert, relatively cheap, and its use both favors the offense and the defense.

Instrument of military power. Cyberspace is the latest collection of technologies in the history of information. The printing press, telegraph, telephone, and wireless communication technologies—such as radio or TV—have each revolutionized societies, economies and military affairs. Cyberspace, however, is different from its technological predecessors because it is not just a means of communication but also a means to create, store, and exploit information. The increasing reliance of state systems on cyberspace is part of the mosaic of the shifting geopolitical and economic global environment that provides the strategic context for the use of cyberpower.

This strategic context is challenging for policymakers, strategists, and scholars to understand. Cyberpower is technically and tactically distinct from the other instruments of military power, but it is not beyond strategy. It enlarges the spectrum of strategic vulnerabilities and strategic actors. This spectrum starts from the individual presence in cyberspace. For centuries, individual reputation has been the cornerstone for public and civil coexistence. It has passed from domestic walls to the public square when politics has become the most significant public activity. This reputation now floats in cyberspace and is constantly submitted to the dangers of manipulation, offense, and discredit.

Crime and espionage. Crime and espionage also form a dark underworld of cyberspace. The criminal world is usually the first to seek out new opportunities and methods, and espionage usually follows, exploiting techniques and opportunities. They take advantage of the cracks and fissures that open up in the transformation of our technological world. Crime and espionage have also emerged because of poor security practices of users, from individuals to large organizations. Data today is transferred from laptops to USB sticks, over wireless networks at café hotspots, and stored on the Cloud (networks of computers whose servers are located who knows where). These new modalities of communicating disperse the targets and multiply the points of exposure. Paradoxically, documents and data are probably safer today in a file cabinet, behind the watch of bureaucrats, than they are on a PC.

Militarization of cyberspace. States are starting to militarize cyberspace. They find their opportunities for a strategic posture much less expensive than conventional weapons but as effective as conventional strikes. The creation of a 9,000-man strong cybercommand at the Pentagon is the most relevant index of this new trend. Countries such as Iran or North Korea are training armies of cyberwarriors. The fact that cyberspace knows no borders implies that cybersecurity is only as good as its weakest link, and that something must be done to prevent cyber anarchy, the militarization of cyberspace, state-sponsored espionage, and the rise of unregulated countries that can offer a haven for cybercriminals.

Internet governance. While no fewer than six U.N. bodies and multiple regional and national forums have sought to build a consensus on the future of Internet governance, there has been little progress so far. Most Western countries believe that freedom of access to the Internet is a basic human right and that the right to privacy and security should be protected by laws. Unesco argues that the right to assemble in cyberspace comes under Article 19 of the Declaration of Human Rights. At the other end of this spectrum are those countries that favor a global treaty but nevertheless believe that access to the Internet should be limited if it threatens regime stability and that information can also be a cyber threat. For these countries, any state has the right to control content within its sovereign Internet space.

The two sides are far from willing to reach an agreement; and national states are not the only actors in the global arena. Political movements, opinion groups, and shadow entities like Anonymous are playing an active game on the Internet and their opinion—or action—will count when trying to establish a common set of rules for use of the Internet.

But we certainly need to promote a framework agreement to regulate the global Net and its use.

A MULTILATERAL APPROACH

One of the main causes for the global turmoil we are experiencing today in the world of economy and finance is the lack of a global governance mechanism. Problems and threats are common; thus we need a common response. We affirm the need for a governance mechanism to make globalization a win-win game and not a zero-sum game. It is the same for information technology. During the Cold War, on the verge of the frightening scenario of an ultimate nuclear Holocaust, the United States and the U.S.S.R. convened for a mutual strategic arms limitation treaty. Today we need something similar to prevent a chaotic militarization of cyberspace and the proliferation of strategic cyber weapons. In this sense, a multilateral approach shall be considered as the best way to reach this goal.

This conference is one that is highly "NATO-influenced." And that is very good news when analyzing the issue of cyberspace and its implications for national and international security. NATO has devoted a large part of its recent summits to the issue of cyberspace. In Lisbon and especially in Chicago, NATO has showed how effective it can be in a highly volatile and changing world. It is not a relic of the past. It is a vital forum to discuss and to act, to prevent new and disruptive threats. That is particularly valuable for Italy and Europe. The transatlantic relationship is crucial for a variety of reasons, also in cyberspace. Close cooperation between the two shores of the Atlantic in intelligence and military matters has extended into cyberspace, enabling both parts to influence the domain in a way that is difficult, if not impossible, for any other alliance to match. On both sides of the Atlantic there should nevertheless be a discussion regarding the precise nature of cyber warfare. This discussion should take into account the complexity of cyberspace, the challenges posed to traditional notions of warfare based on attack and defense, and the speed of change in the medium term. There is, however, no need to reinvent the wheel and to devise new techniques and procedures related to cyber warfare. There are lessons regarding the management of complex problems to be learned from the existing defense environment, government, and the commercial sector. But for the moment, cyberspace still remains terra nullius, beyond the reach of a mature political discourse.

It is precisely the absence of a constraining political framework around cyber warfare that makes cyberspace so attractive as a place in which to aggressively pursue cultural, religious, economic, social, and even political goals. I believe that occasions like this conference, which bring together the various stakeholders, are ideal forums to advance the awareness of the threats and opportunities emerging from cyberspace.

Chapter 27

Dealing with Threats to Broadband Networks

Mr. Franco Bernabè
Chairman and CEO, Telecom Italia

Broadband Internet networks are the backbone of digital economies. Any threat to their smooth functioning is rightly considered a threat to the heart of modern societies. Coping with these threats is an issue that involves both the private and public sectors and it is the responsibility of Telecom Italia—which owns, manages and continuously invests in the upgrade of the main Italian fixed broadband network—to ensure to our customers the highest standard in terms of quality and continuity of Internet access services. Our goal is to allow our customers to fully benefit from the Internet services without incurring the risks of being harmed by ill-minded individuals.

Two phenomena have lately gained a growing importance from a security standpoint: the threats to the security of DNS and the DDOS. DNS stands for Domain Name System while DDOS stands for Distributed Denial of Service. Both may endanger and undermine the Internet reliability and security.

DNS, i.e. the system that allows Internet users to reach their desired destinations, has increasingly become a battered cyber attack target. DNS resolves domain names into IP addresses used by the Internet routing equipment to identify and locate computers and servers connected to the Internet.

CYBER ATTACKS TARGETING DNS FUNCTIONING TAKE TWO MAIN FORMS

Cyber criminals may violate DNS servers and alter the association between "site name" and "IP address." Through this practice cyber criminals redirect computer browsers towards malicious and counterfeit websites. Then the cyber offenders that run the counterfeit websites are in the position to steal precious information such as credit card details or bank account coordinates of unwitting Internet users.

Ill-minded individuals willing to exploit DNS weaknesses may alternatively rely on the viral spreading of malware code capable of modifying browser settings. Notably DNS-aimed viruses instruct browsers to replace the DNS it normally uses with "new" DNS controlled by the cyber offenders who can then resolve Internet queries to fulfill their illegitimate goals. Manipulated DNS are like a GPS that purposely drive Internet users to wrong destinations controlled by cyber criminals.

Manipulating a specific DNS server affects simultaneously all Internet users that rely on the manipulated DNS server. Conversely viruses changing DNS settings can either step in as the virus spreads or can alternatively be programmed to begin to work at a predetermined moment in time. These scenarios may sound far-fetched or unrealistic. Unfortunately evidence suggests they are not. To see this, it suffices to read the latest cybercrime news.

Let's first look at the case of the malware virus known as DNS changer. The criminal organization behind this malware was shut down last year by the FBI, Estonian Police and other law enforcement agencies after the virus infected some four million computers worldwide. To avoid major service disruptions a consortium of private companies led by the FBI set up DNS servers that acted as temporary hosts for users infected by the "DNS changer malware." The 9th of July was expected to be the "Internet doomsday" since, that day, the Internet System Consortium tasked by the FBI to operate the DNS replacement took down their infrastructure. Despite estimates of nearly 300,000 still-infected computers, the DNS infrastructure shutdown did not cause major problems. Security firms reported no significant outages on the 9th of July as Internet service providers took steps to provide their customers with the necessary information and tools to clean their computers.

The initiatives carried out by the major Internet service providers certainly contributed to rein in the consequences of the DNS changer virus. Nonetheless, 300,000 computers that were potentially unable to use the Internet cannot be seen as a reassuring outcome.

This time was a matter of addressing the aftermath of a criminal operation dismantled by the FBI more than 6 months

before. Facing and coping with ongoing cyberattacks may lead to riskier outcomes.

The DNS Changer working task force gathered the best professionals and competences available at the international level. Indeed they took timely and accurate steps to address the situation in the most appropriate way. Nonetheless, uncoordinated action and the spread of disorderly panic was prevented more by the shortage of media coverage rather than by a real understanding of the risks involved.

Telecom Italia implemented specific websites enabling its customers to check their computer health. The best way to deal with threats like the DNS Changer virus is to provide customers with their own means of defense. The implementation of the website www.dns.ok.it, along with an adequate public information campaign, has proved extremely effective. The high number of customers that used the sanity check provided by the www.dns.ok.it website is in itself the best acknowledgement and reward for the efforts made by the Telecom Italia's security experts.

The scope of Telecom Italia's involvement in this initiative was twofold: the protection of our customers' interest came along with the willingness to take proactive steps to actively contribute to the security and trustworthiness of the Internet as a whole. It is indeed our opinion that securing a trustworthy record of neutralized cyber attacks is pivotal for further developments of the digital services delivered through the Internet. Improving Internet security and trustworthiness is to be considered one of the top priorities.

DISTRIBUTED DENIAL OF SERVICE

The second major phenomenon that has been lately undermining the reliability and the robustness of targeted Internet sites is the so-called DDOS, i.e. distributed denial of service. DDOS has been in use for quite some time: DDOS impairs the Internet's smooth functioning by saturating the resources needed to gain access to the targeted websites. This traffic overload used to be generated by a large number of Internet users attempting to gain access to the same website. The inability to gather a sufficient number of people or resources upgrade by the targeted websites has led to new strategies involving more sophisticated cyber crime tools. To strengthen DDOS attack effectiveness and enhance its impact, cyber criminals have developed malicious programming code that spreads through the Internet and infects unwitting unprotected PCs and servers. This malicious code works like bacteriological weapons that take control of PCs and instruct them what to do. Viruses and Trojan horses spread very quickly. Infected PCs soon turn into "zombies" poised to fight alongside the other resources employed by the attackers. The outsized army and its worldwide geographic footprint make it more difficult to filter out aggressors on the basis of their geographic identity.

Attackers have often succeeded in circumventing the Maginot line created to protect websites. The Italian DDOS war toll has been recently quite high. In the first half of 2012, DDOS-hit websites included CartaSi, Ministero dell'Interno, Governo, Vaticano, Trenitalia, Equitalia, Enel, BCE, Polizia di Stato, Carabinieri and Ministero della Difesa. By way of example, DDOS attacks on Telecom Italia's network have almost quadrupled in the first half of 2012 compared with the same period of the previous year. The technical measures implemented by Telecom Italia have limited the impact and the consequences of the DDOS attacks. This proves that a good preemptive defense strategy is essential.

The ability to adequately address risks and to cope with emergency circumstances surely relies on the availability of robust infrastructures and sufficient means, but it is also heavily dependent on the cultural flexibility of the involved organizations. The cybercriminal's competitive advantage typically lies in his skill and cutting edge technology. A cybercrime offender that succeeds in his criminal intent relies either on better knowledge or better motivation. Often the targeted outfit is neither aware of its cyber vulnerabilities nor is it able to identify a rescuer or the tools needed to address the risk it faces.

Given the scenario depicted in the previous paragraphs, major disruptions do not seems unrealistic. To avoid them, firms and organizations need to plan carefully the resources and skills needed to address the foreseeable cyber threats.

The first gap that must be addressed is the scarcity of awareness and the clear underestimation of the risks at stake. Many firms and outfits do not seem to care or be prepared to take the necessary steps to mitigate the risks associated with cyber crime.

Indeed there are some exceptions to the scarce consideration devoted to the cyber crime threats. Few firms and organizations have already worked out credible action plans. Telecom Italia fixed broadband and data network is the digital backbone that allows Italian firms to enhance their competitiveness and effectiveness. Coherently Telecom Italia's IT experts have long been preparing to identify the best measures and solutions needed to protect our clients' IT infrastructures while ensuring and enhancing the highest security standards for our core business.

A reactive approach where firms take the necessary steps once they have fallen prey to a cyber attack is no longer a viable strategy. Firms need to engage in a proactive and preemptive manner. This is all the more true in the highly globalized cyber

crime scenario that stretches ahead of us. Political and organizational complexities often lead to government-led action that is not able to cope with a fast-paced cybercrime environment. Overlapping competences may further delay a timely and effective reorganization of cybercrime units and bodies.

The lack of clear mandates and responsibilities among the various public bodies that deal with cyber crime from various angles has so far held back the creation of an operational task force entitled to cope with the risks associated with cyber attacks aimed at Italian strategic targets or infrastructures. Working groups set up within the Prime Minister's cabinet are not necessarily the right way forward because such groups may lack the stability and the empowerment to cope with these threats.

Cyber offenders do not have to deal with diplomatic issues. They do not have to cope with conflicting cyber crime agendas or other hierarchical and organizational issues. Cyber criminals take immediate action to achieve their aims. Cyber crime activities are driven by economic rewards and recognition while the threat of criminal charges often work as an incentive to devise better, untraceable and undetectable strategies.

These imbalances between the motivation and effectiveness of the cyber criminals and the organizations set up to counteract their actions apply to both Italian and European Union institutions. Two examples of ineffective European Union decisions come immediately to mind:

- The creation of the CERT (i.e. the Computer Emergency Response Team), whose establishment and financial resources were agreed upon on June 2, 2011, has surely come too late.
- Placing the ENISA (European Network and Information Security Agency) headquarters on the island of Crete has not been the most effective choice either. The European Security Agency in fact needed an easy to reach location and a geographic environment where the Agency could have immediately set up collaborations and partnerships with private sector and academic research labs. Indeed the very establishment of the Computer Emergency Response Team in Brussels clashes with the fact that a very similar body already existed at ENISA.

The ambitious task of counteracting cyber security threats calls for a close examination of the effectiveness of the initiatives envisaged over the last few years. Organizations that have fallen short of their expected outcomes should be dismantled or merged into more effective ones. Cyber defense initiatives should be redesigned to meet the needs of cyber war management.

Reorganizing public bodies that deal with cybersecurity issues to make them more effective and nimble is surely a step forward. Nonetheless, this may not be enough to tame current cyber threats.

The challenges that the Internet is now facing hint at the complexity and diversity of a system that has grown from a system designed to interconnect a few highly trusted supercomputers to interconnecting the world. As it stands today, the Internet's functioning and architecture are not in the best position to take advantage of the opportunities that lie ahead.

Further development of services like financial and health services need security and inviolability standards that go far beyond the level that can be provided by the current Internet infrastructure.

Taking on the next decade's opportunities might thus entail some rethinking of the "Internet functioning." These ideas, known as the clean slate approach, have been the subject of academic research for quite some time. It is now time to take them to the next level. It is now time for industry to bridge the gap between theory and practice.

This does not imply a shutdown of the current Internet infrastructure. It simply means that the current Internet should develop towards a more comprehensive tool capable of accommodating "standard service delivery" alongside a service delivery characterized by a strengthened security emphasis.

Chapter 28

Towards International Cyber Stability through Confidence- and Security-Building Measures

Ambassador Rolf Nikel
Federal Government Commissioner for Disarmament and Arms Control

Cyber threats to our vital interests are growing from states, international terrorists, and organized crime networks. Our societies depend on functioning IT systems, but our networks are vulnerable and our critical infrastructure is at risk. The good news is that states, international organizations, as well as private businesses have taken up this new security challenge. We all need to develop common approaches to stem the growing risks. Time is of the essence.

Our economies heavily depend on cyberspace. Information technology provides tremendous new opportunities. However, many, if not most, cyberattacks directly harm the business sector. Data theft and violations of intellectual property rights occur on a massive scale, resulting in losses of millions of euros. The threat to global financial markets is very real. Attacks do occur, even though the very perpetrators should have an interest in safeguarding the integrity of the system. So "deterrence by interdependence" does not necessarily work.

Cyber content can be a powerful tool in advancing political freedom. The Internet and new social media have demonstrated their influence in the Arab Spring. Authoritarian regimes all over the world therefore try to block, over-regulate, or misuse the Internet for suppression and indoctrination. Any attempt to protect or regulate cyberspace against whatever kind of attack must therefore safeguard freedom of opinion and information.

Cyber challenges require the involvement of many actors, national and international. Information must be shared, data must be analyzed, and relevant institutions must act in a coordinated manner. In Germany we have therefore created a Cyber Security Council with ministries and industry plus a cyberdefense center which unites the analytical capacity of national ministries and agencies. To address and coordinate all the dimensions of a coherent cyber foreign policy, Foreign Minister Westerwelle has established a cyber coordination unit in the Federal Foreign Office.

WHAT SHOULD OUR STRATEGY BE?

Robust protective measures are the priority. The dependency of modern armies on information and communication technologies is reflected in an increasing digitization of warfare. Industrialized countries are worst affected by security gaps in cyberspace. Critical infrastructure protection is paramount. Accordingly, Germany has enhanced its resilience measures, especially for critical infrastructure. With its new strategic concept, NATO has begun to strengthen the cyberdefense capabilities of its critical infrastructure. An EU cybersecurity strategy is also needed, encompassing all three elements of cybersecurity: information systems security, cyberdefense, and the fight against cyber crime. Protecting these systems is expensive and a shared responsibility. We must analyze our vulnerabilities more systematically in order to increase their robustness and resilience. The higher the wall, the more likely a pre-emptive attacker will not even try. Thus, defensive measures can deter attackers by robbing them of any hope of success (deterrence by denial).

Non-state actors, and especially state actors, can carry out cyber attacks easily. Instruments for cyber attacks are inexpensive and available. Cyber mercenaries can be enlisted as well. In cyberspace, it is difficult to legally attribute an act of cyber aggression to a presumptive attacker. All that is needed for a devastating attack is a room with computers and Internet access; geographical proximity is not necessary. Against this background, "deterrence by retaliation" does not make much sense. States should rather define the framework for lawful state conduct in cyberspace. International rules, principles, and norms will help to enhance transparency and predictability of responsible state behavior in cyberspace. Practical transparency and confidence-building measures (TCBMs) will help to avoid the risk of misperception and escalation.

Without such minimum rules—I commend the endeavors made to draft the "Tallinn Manual on the International Law

Applicable to Cyber Warfare"—states can continue to shirk responsibility for cyber attacks by blaming private hackers. We need a discussion of state responsibility for cyber attacks launched from their territory, if states do not act to end such attacks when informed about them. In any case, we should be very careful about cyber offense. You have to know offense in order to devise a sensible defensive strategy. However, engaging in large scale cyber attacks of the Stuxnet or the Flame kind is a double-edged sword.

WHAT IS REQUIRED FOR IMPLEMENTATION?

Traditional arms control and disarmament instruments are not applicable to cyberspace. Currently, limitations or a ban of certain cyber activities cannot be verified. There is no recognized definition of cyber weapons. Technical capabilities in cyberspace cannot be classified using traditional categories of "civilian" and "military," and they cannot easily be limited. Most proposals for arms control in cyberspace therefore concern confidence- and security-building measures, not restrictions of technical capabilities. In order to implement such a strategy to build international rules and apply practical CSBMs, we need to be proactive. In its National Cyber Security Strategy, the German government identified the basic principles for an international cyber policy from our perspective.

In this context, we reaffirmed our belief that a code for state conduct in cyberspace (cyber code) should be established, which is signed by as many countries as possible and includes confidence-building security measures. In 2011, Germany worked out proposals for a set of CBMs. We support several projects in this field, including the elaboration of an annual cybersecurity index as a transparency measure. It would provide a survey of military cyber capabilities, organization, and structures, as well as possible postures worldwide. Germany has also prepared a set of papers on the application of general principles of international law and of humanitarian international law to the cyber realm.

States must agree as soon as possible on the best ways for recognizing and affirming the application of the relevant international law principles with regard to state behavior in cyberspace. This includes in particular those derived from the U.N. Charter and international humanitarian law, as well as relevant international human rights law. In our view, recourse to military self-defense requires an armed attack. Even massive cyber intrusions do not fulfill this precondition. However, in the case of cyber attacks, international law provides a set of rules for (non-forcible) counter-measures below that threshold. States should also endeavor to outlaw cyber attacks on critical infrastructure. In December 2011, the Berlin Cyber Security Conference provided the forum for an extensive multi-stakeholder debate with EU, U.S., Chinese, and Russian participation on such an approach.

Germany has played an active role in promoting a cyber TCBM agenda. Two important regional organizations, namely the OSCE and the ASEAN Regional Forum (ARF), have started work on it.

This work will certainly help the efforts of the U.N. to find common ground on global rules for cybersecurity. For this purpose, the U.N. Secretary-General has convened for the third time a Group of Governmental Experts on Cybersecurity (GGEs). It will have its first meeting this coming August.

The Group should focus on the mandate it has been given by the U.N. General Assembly, namely to study possible cooperative measures to address existing and potential threats in the sphere of information security, "including through norms, rules or principles of responsible behavior of states, and confidence-building measures in information space." Germany will appeal to other GGE members to avoid the temptation to discuss Internet content or control.

Our contribution will focus on the application of international law in cyberspace as well as specific TCBM elements drawing on the work of previous Groups of Government Experts and the OSCE. These include: Early warning mechanisms, inter alia among CERTs (Computer Emergency Response Teams); Exchange of information and best practices on national cybersecurity strategies and national views; Cooperation on fostering the development of technical recommendations for robust and secure cyber-infrastructures; Establishment and notification of national focal points; Establishment and/or improvement of existing crisis communication channels for use in case of cyber incidents; Support for capacity-building in cybersecurity in developing countries; Establishment of awareness/training programs.

Developing international rules and confidence- and security-building measures can be a first step, focusing on the regulation, restriction and, perhaps, prohibition of hostile activities in cyberspace. Limitations of cyber capabilities itself would be difficult. A comprehensive approach will consider not only security but also the economic, humanitarian, and cultural aspects, while preserving and expanding the freedom-promoting effects of cyber media. Given the multitude of bodies involved and the many challenges, effective international policy requires a coherent approach. Germany will actively contribute to the work in order to ensure that they can fulfill their respective roles in achieving global cybersecurity.

Chapter 29

What Shapes Our View of the Internet?

Mr. John N. Stewart
Senior Vice President and Chief Security Officer, Cisco Systems

A VERY YOUNG INTERNET

In order to introduce our panel on cyber security, the first observation I want to make is that, when we speak about international security—whether physical, electronic, social, civilian, military, or in the international domain—it has had a significant amount of experience to build on versus what the Internet is trying to learn and achieve in just a short period of time. If you consider this history in terms of years of maturity, the Internet as we know it today is probably at best 20 years old. Remember when all of us were 20 years old? When I was 20 years old, I believed that I knew it all. Of course I did not, but I was very convinced that I did, and I had an endless amount of energy to the point where I would take some of the silliest ideas and pursue them purely because I thought they were right. The Internet has now reached that age and it is doing approximately the same thing: there are good ideas, there are bad ones, but there is an endless amount of energy and it seems to know it all. I also thought about this conference, which is 29 years old. I am 29 years old—I just happen to have 14 years of experience being 29 years old—and I will never turn 30 nor will this conference, despite the fact that next year might be its 30th year.

HOW EXPERIENCE, GOALS, AND WORK SHAPE OUR VIEWS

Looking at my notes from last year, I said at the time that we needed trust, speed, and clarity. Then I wondered what we needed to think about this year. My thoughts turned to something called "perspectives." The human race created aqueducts, survived the black plague, cured polio, and got to the moon. It even acquired the ability to fly, which—when I am entering an aircraft—does not seem possible in any way, shape, or form; and yet here we are doing it. We learn from our failures, we build upon our successes, and it is typically because of patience and dedication that requires way beyond those 20 years. So my perspectives turned to the following: We need to look at and think about things differently because each of us is in a different spot.

The first difference might be experience. I would imagine that absolutely none of us in this room grew up with the Internet from day one and yet, there are all kinds of communities of people, students and children that are living in a world where this is commonplace. This can be to the point that, as Jane Lute described it, it is the endoskeleton of their lives. It can be so much so that, like electricity for us when it goes out, if the Internet goes down, they think that the world has come to an end. There are some of us who might be called immigrants to the Internet—they joined it as it began, or they joined it in flight and are only now beginning to understand it, or they may never fully understand what the Internet truly is. And finally, there are the inventors if you will, those of us that dabbled at the very beginning and have brought it from its very shaky starts to something that might never have been imagined 20 or 30 years ago. But it is that experience that has made this conversation difficult because one might say that my iPad is the Internet and another might say that IPv4 or TCP/IP stacks are the Internet and, yet, both would be right.

The second perspective I thought about are goals, including for this conference and for all of us here. Are we trying to solve problems or just contain problems? I would argue it is probably the latter, not the former. Are we fixing problems faster than we are creating them (something which I worry about on a regular basis including in my role as an executive at Cisco)? Do we need norms or do we just need majority agreements? Do we have enough consequences and accountability to deal with those who like losing money or are doing things for wrong versus for right?

And then there is a third point, which is very *à propos* to me for this panel if you think about your experience as one

perspective, and your goals as a second perspective, and the place you sit in the world as a third perspective. As we talk to each other, we do not all sit in the same spots. I am sitting in a private sector position in a corporation that is multinational. And yet, there are government, military, partnership development, and most assuredly, international representatives on my panel. We should keep all this in mind during our discussions.

Chapter 30

Building an Understanding of the Cyber Security Situation

His Excellency Jaak Aaviksoo
Minister of Education and Research of Estonia

INTRODUCTION

When we last met here in Rome in 2008, it was the year after the 2007 cyber attacks on Estonia that brought cyber security to the attention of the international community as a potential national security concern. Where do we stand today five years later? Is our cyber security situation improving? Are our defenses better? Do we have means and measures in place to defend our soils, to feel secure? Or has the situation worsened? Have we failed or worse? I believe that we have neither succeeded nor failed. We are building an understanding and broad awareness of where we are.

Why do I think that way? First, when you ask whether the chronological, organizational, and infrastructure development of cyber space has produced more opportunities or threats, the general understanding is that there are many more opportunities than threats. People do not perceive threats as a major problem. They are still much more engaged in using the opportunities and making new opportunities available through technological development. Of course, this in turn leads us to focus on increasing the security of cyberspace and so, where we are today is understandable. I do not think that we have failed in the sense that we have not been able to address the challenges that we have confronted during the last ten or 15 years. We have had many meetings and many different strategies and concerns. We have also come to the conclusion that, in addition to fighting cyber crime, we should also focus on the protection of the critical information infrastructure. More broadly, we have developed different operational capabilities, even within the European Union or NATO. Some countries have developed rather extensive defensive and offensive capabilities but, as was pointed out by Deputy Secretary Lute, we have not been able to agree on the role of government or the international community and for different historic, cultural, or other reasons, we often have a very different understanding of what cyber, privacy, and security really mean.

USING BASIC FUNDAMENTAL PRINCIPLES

Somehow the basic concepts are not very well in place. Maybe we should not concentrate on trying to come up with solutions by putting concepts in place first and then gradually building a defensive edifice. The nature of cyberspace is fundamentally different. We have to accept high levels of threat as a matter of fact. Just as in physics where there are two fundamentally different types of equilibrium, a static one and a dynamic one, I believe that the same framework should be applied to cyber security. It would be a "mission impossible" to formulate a cyber security concept that is stable and static, even within a period of months, not to mention decades as some of our military doctrines have required. I do not believe that this is a solution. Instead, we have to develop different ways and means to handle ,the cyber security and defense program.

If we want to survive in this turbulent environment, there are some fundamental principles that we should use. One principle, which is very useful and convenient, is to avoid over-mystifying cyber. If we want to understand what is good and bad in cyber, a rational approach is to view it in exactly the same way as we view what is right and wrong or good and bad in real life. If something is undesirable or unacceptable in the real physical world, it will be unacceptable as well in cyberspace. This simple principle is worthwhile when we address the very complicated and sophisticated problems we may encounter as we deal with cyber threats or cyber opportunities. In this respect, I disagree with those who say that cyber will remain cyber and that the cyber threat must be addressed as a cyber event. If a cyber event has real consequences in the real world, a real world response is fine. This is also the case in terms of defense. For example, if the consequences that might require using Article 5 are bad enough, then it is right to respond in an appropriate way using all the ways and means at hand. So, one should not over-mystify cyber. On the one hand, it is complicated, it is different, it is dynamic and it is everywhere. On the other hand, it is about people, it is about our interests, our lives. We should not think that it has been imposed on

us with different rules that somebody other than our own selves has established. This is important.

Favoring Internet Freedom Over Security?

There are three major tensions when we address issues of cyber security. The most important one is the balance between the Internet and full security. Perhaps the Internet was born in the wrong way because it was born as a community instrument when trust was not a problem but now, we have developed it into a global environment where trust has almost disappeared. Since there are two billion people on the Internet, we cannot trust all of them. Perhaps there are some fundamental problems with the Internet's architecture and we need a more robust infrastructure. I do not believe that we can walk in that direction. An example is the history of efforts to protect intellectual property rights on the Internet. We have to somehow live with this tension: a free Internet as a human right versus a fully secured environment as some of us may wish. It is a political question in the classic sense, the liberal versus conservative division, but it is also a political question on an international level since some governments believe in freedom more than in security or vice versa. I said earlier that we should make more efforts to understand the free Internet's opportunities because it is most probably going to prevail. Finding a balance that tends a little towards favoring freedom over security seems to be a global trend that will be hard to fight.

Building Trust among Partners

My second point concerns trust—and confidence—building. Most believe that there are a huge number of cyber attacks given the many reported incidents. Yet, when we look at what, where, when, and against whom these cyber attacks occured, little information is available. This is understandable because it involves sharing cyber security and cyber defense information. This situation is similar to sharing Intelligence information, which is considered highly sensitive. I do not know why it is like that, but it is like that. I confronted that problem when we discussed what kind of cyber exercises we could organize in the NATO framework. Moving forward was slower than expected because of insufficient trust. Again, it is easy to say that we should improve, but it is equally important to understand why that happens. Is this specific to cyber or are there other reasons behind it? Perhaps we might share information by creating a center that will gather anonymous information on cyber incidents and share it without names attached so that it can be used for training, educational purposes, or for other ends.

Internet and Identity

My third point deals with Internet and identity. Whether my email is a personal or government one, it always contains my full name. My son, who is in the IT and security business, thinks that this is not very wise. When I asked him how many identities he has, he said that he did not know but that it was very likely more than three. I personally think that this is not a proper code of conduct and if I were to write a code of conduct, I would say that using different identities is not a good idea. Yet if people who live in that environment follow that kind of behavior, there must be some justification for it. So there may be something to learn from such practices. I do not know, but I still keep only one identity, one name.

CONCLUSION

Last but not least, I believe that having had this kind of debate for several years now has been very useful and has helped efforts to increase cyber security and build national and international defenses against cyber threats. Let me also invite everyone to be even more open to these debates by asking that a broader stakeholder community be involved in them. In this way, we will avoid ending up with agreements that do not have the community's support in the broadest possible sense. Secondly, building trust in the Internet community, trying to learn from the Internet community's experience, making this experience part of government practice and taking these ideas into account when devising and agreeing on policy is a good way forward. Despite all our efforts, I still fear that even the most liberal governments tend to believe in rules and regulations that are hierarchical, static, and not always enforceable. But despite all these threats, I will end by saying that cyberspace is a nice thing to have.

Chapter 31

Finland's Approach to Cyber Security: Principles and Strategy

Lieutenant General Arto Räty
Permanent Secretary, Ministry of Defense of Finland

Cyber security—the topic for this morning—is very close to my heart as Permanent Secretary of the Finnish Ministry of Defense and also as Chairman of the National Security and Defence Committee, which has been tasked by the government to write Finland's first National Cyber Security Strategy by the end of this year. The work started 1.5 years ago. In today's world, filled with economic and other crises, it seems that sometimes politicians forget that in all sovereign nations one of the fundamental tasks of the state leadership is to guarantee security. This includes cyber security. That is why I very much appreciated Deputy Secretary Lute's words. My short discourse will address the security aspects from the perspective of a small but well-developed nation. I will briefly introduce Finnish national security principles as well as discuss the ongoing development of our National Cyber Security Strategy.

FINNISH NATIONAL SECURITY PRINCIPLES

An Inter-Societal Approach

Our national approach is firmly built on the comprehensive security approach, which is based on close cooperation between all relevant authorities, the business community, and organizations. Our model in fact can be described much more broadly than just a "whole government" or "inter-agency" model. It is better described as an "inter-societal approach." The government's National Security Strategy from 2010 outlines the principles of our national comprehensive security approach. The strategy has been compiled from the viewpoint of safeguarding those functions that are vital for society in all situations. Those functions are: management of government affairs; international activities: Finland's national defense capability; internal security; functioning of the economy and infrastructure; security of the population's income and vital services; and psychological resilience to crisis. The Finnish cooperation model has a strong national tradition and is supported by all sectors of society. It is a natural solution for a small nation where resources are limited. The aim is to create straightforward and uncomplicated systems that are at the same time cost-effective.

Interdependency between the critical functions in our society, as well as in all modern societies, has grown considerably. Serious disturbances in one sector such as the transmission of electricity or telecommunications services lead quickly to serious failures in other sectors such as financial transactions or transport and logistics. When extensive cyber threats occur, they can cause a chain reaction that seriously affects the vital functions of the country.

Cyberspace is nowadays an integral part of modern life. People around the world interact, cooperate, and compete through a series of networked linkages that span the globe. However, as we have heard many times, the international community in reality still has a very limited ability to govern the cyber common. Users, whether organizations or individuals, must typically take care of their own security. Much of cyberspace operates outside the controls of any official organization. Internet traffic is routed through peer arrangements between Internet service providers without real central authority or real-time control. The physical infrastructure of the cyber common is also largely owned and controlled by the private sector. There are myriad providers of devices, connectivity, and services in loosely woven networks with open standards.

The Need for Increased Coordination

Finland is at the moment one of the most developed countries in the area of cyber security. However, even in Finland, competencies, knowledge, and responsibilities of cyber security are scattered between many organizations and stakehold-

ers. The development and decision-making processes related to cyber security have been conducted relatively separately in different parts of the administration and society. This has even hindered the creation of common cyber security objectives.

As the vulnerability of our societies has increased, it is indispensable that the management of a cyber disturbance can begin without delay. Currently in Finland, the procedures and responsibilities in managing and solving a nationwide cyber crisis are not defined clearly enough. The requirement for an authority that comprehensively coordinates and directs the prevention and management of cyber threats will be studied as part of the strategy work. Only by creating a comprehensive cyber situation picture is it possible to improve the capability of society and the state leadership to deal with an extensive disturbance or cyber security threat against several vital functions at the same time.

Strong Cooperation with the Private Sector

In Finland, the public and private sectors have traditionally prepared for exceptional circumstances in full cooperation and secured the vital functions of society by working together. This national approach is a result of decades of development and is a key element of Finland's national security. A practical example of our comprehensive approach is an "information exercise" organized every second year. It focuses on preparedness of the network and information systems and of information and communication technology (ICT). The exercise gathers a broad group of private enterprises (for example, operators and service providers) and is entirely based on the voluntary participation of the private sector.

As mentioned many times during this seminar, the private sector holds a key position in securing the functioning of the economy and infrastructure in particular. ICT services, transportation, and office ownership and management are amongst the service entities where outsourcing is typical. It can easily be stated that one cannot ensure reliable cyber security without tight involvement of the private sector and other relevant stakeholders.

Quite often when we do speak about cyber security we only address the threat. From the point of view of civil society and the development of business activities, the cyber operating environment is not only a threat but also a huge opportunity. A secure and reliable information network with a wide range of electronic services makes e-inclusion, participation, development of democracy, administrative efficiency, and new business activities possible.

THE DEVELOPMENT OF FINLAND'S NATIONAL CYBER SECURITY STRATEGY

As I mentioned, we are in the process of writing a National Cyber Security Strategy. The work is currently conducted by a Working Group involving all relevant actors nationally and internationally. To facilitate free thinking and new ideas, the chairman comes from outside the administration.

As part of the internal roadmap/work program, the Working Group delivered a preliminary study report which included a very broad and comprehensive mapping of the current national situation related to cyber security. One of the conclusions was that we have to convince the political leadership that the global cyber domain is a growing challenge for Finnish national security. This naturally means that Finland has to be fully capable of protecting the vital functions of the country against cyber threats in all circumstances. The government also agreed on a very ambitious goal: By the year 2016 Finland should be one of the global forerunners in the field of preparedness against cyber threats and in managing serious failures and disturbances caused by cyber threats.

Finland does cooperate continuously with many actors within this context. We are actively contributing to the developments in cyber security within the EU framework as well as within the NATO partnership program. We also work together with the United States and our Nordic partners to develop cyber security. In addition, we participate in international exercises (MNE7).

Nine Areas for Action

Key observations in the preparatory report for the National Cyber Security Strategy define amongst several others the following nine actions to be taken as part of the strategy:

- Agree on the central national definitions related to cyber security.
- Decide which authorities implement and lead the operational functions of cyber security.
- Define a process to identify how the threats, risks, and vulnerabilities in the cyber environment endanger the vital functions of our society.
- Foster our national processes through which a comprehensive cyber situational awareness is compiled on the basis of

the various existing situation pictures. This includes analyses, cooperation between the administration and the business community, providing information to citizens, and the exchange of information at the international level.

- Clarify the needed amendments to national legislation, norms, and agreements.
- Define competencies, actions, and responsibilities to proactively protect the critical infrastructure of the country.
- Define activities and responsibilities to govern R&D, education, and know-how.
- Ensure a common view of the opportunities offered by the secure and reliable cyber operating environment for the development of civil society and new business activities that benefit the national economy.
- Define national goals in promoting cyber security and critical infrastructure protection in the international operating environment.

CONCLUSIONS

I am a believer when it comes to strategic planning. There is no way to achieve success without having a clear vision and a wide enough road planned to get there. For governments, this is even more crucial since political leaders come and go, while strategy gives you continuity and the possibility of long-term planning and execution.

I also strongly believe that a comprehensive security approach is the way to create security in the cyber domain. A small nation like Finland cannot afford to build an expensive centralized cyber command and that is why we have selected a network-based system encompassing all sectors of society through coordination provided by the government. In this way we can in a cost-effective way utilize all existing capabilities in our society.

Chapter 32

Perspectives on the Current State of Cyber Security, Key Issues, And Work Being Done to Close the Gaps

Mr. Kent Schneider
President and CEO, AFCEA International

Based on the workshop presentations and discussions of the past two days, one thing that we can clearly agree on is that the global cyber threat is real, that it is multi-dimensional, and that it ranges from recreational hackers to hacktivists (who have been particularly active in the last couple years), to cyber criminals, terrorists, and state actors. Those categories are not necessarily mutually exclusive since people can sometimes be in more than one category. We also heard about the complicating factors that exist, some having to do with technology; the challenges introduced by greater mobility, and by social networking; all the issues associated with big data, whether the data are in transit, at rest, or in processing; and of course Cloud Computing, which has introduced a whole new set of issues with regard to security.

Some of the more interesting and profound complicating factors concern the political issues, the debate about security versus privacy, and certainly budget issues because cyber security is not cheap. So, at the very time when we need to give cyber security our best attention, global economic challenges limit the amount of resources that we can put into it. Industry is developing security solutions across that broad range of threats but, as was discussed earlier, cyber is a very dynamic area. Aggressors are innovators and, unlike us, they have the advantage of not being challenged by acquisition process issues, so they can move very quickly and be very agile.

THE PROTECTION OF GOVERNMENT NETWORKS

There has been considerable discussion about the appropriate role of governments and international bodies in this area. This is where I would like to direct my comments because we have a tendency to look at the issues associated with the Internet and cyber security as being somewhat homogeneous, but we are starting to realize that this is not the case at all. At the risk of oversimplifying, let me talk about three categories: The first category is government networks, systems, and data, and you can subdivide those if you wish into defense and security or into defense and civil government, but there is no doubt that government has a responsibility to protect those assets. Whether classified or simply sensitive, there is an absolute requirement for control in that space and a lot of resources are directed towards that. In the United States, this category has been further divided into two parts: the Department of Defense worries about the dot.mil environment, the defense environment, and as Secretary Lute said, we spent a good deal of money creating the U.S. Cyber Command to coordinate the activities around that part. And then, the Department of Homeland Security has the responsibility for the dot.gov environment, that part which is connected to civil government.

THE PARTNERSHIP BETWEEN GOVERNMENTS AND INDUSTRY IN PROTECTING CRITICAL INFRASTRUTURE

The second category concerns the critical infrastructure, which has to be a cooperative endeavor because most of the critical infrastructure is not owned by the government but by private industry. Government regulates it often or, at least, government works very closely with the critical infrastructure providers to ensure that they have the threat information they need and to share information about protective measures. Of course, we cannot afford to lose any of those critical infrastructure assets. Whether we are talking about finance or transportation or telecommunications or energy or the health community, these are all critical to the welfare of any nation and therefore government has to play a role there.

THE IDENTITY ISSUE IN THE PUBLIC AND PRIVATE SECTORS

The third category is public information and this is where we generally encounter the most debate, primarily because of issues around identity. A lot of people would like to remain anonymous on the Internet for various reasons, some simply because they do not want their information known, others because they use the anonymity to do something negative on the Internet and obviously want to hide that. This is the classic case of government versus non-government. I worked for a while in the U.S. with the Senate High Technology Task Force and one issue that they were dealing with was this identity issue. It became clear that no issue ever created more negative feedback in the U.S. than the idea of implementing a national ID card. Right after 9/11, there was some sentiment in favor of a national ID card but it never got even close to reality because there was so much negative feedback. In Europe, a few countries have successfully implemented national ID cards but most got the same kind of pushback as in the United States. The U.K. is a great example. In the mid 2000s, there was some leaning toward the development of a national ID card and, in 2006, legislation was passed to enable the creation of the Identity Repository, which was a proposal to collect information and biometrics on every citizen and non-citizen resident in the U.K. and then use this information to anchor a credential. The program died under its own weight, partially because of a pushback by individual citizens and partly because the departments and government could not decide who should be in charge.

In the private sector, progress is being made in terms of identity. At the enterprise level, companies have identity systems that work. Industries have created identity where it is necessary, for example, within the transportation community, for example, and globally we are beginning to see identity embedded in credentials used in commercial transactions. Credit cards with embedded identity are emerging. For example, Mastercard and Visa have announced that in 2014, they will start introducing credit cards with embedded identity. Banks are already using strong identity systems for online banking. But what characterizes all of these systems is that they are opt-in systems, in other words, it is the choice of the user to sign up for that system. So in this privacy versus security issue, if you want the additional security, you have to compromise on your identity and it is your choice. You can do it or not, and I believe that we will see more progress on the public side than through government activity. The problem is simply that government cannot be as agile as it needs to be to keep up with the pace of technological change.

GOVERNMENTS AS EDUCATORS OF INTERNET USERS

So, as we think about the role of government, I would suggest that we think about it within those three categories. Even then, we may not have all the answers but it is easier to think about what the appropriate government role is if we think of it with respect to government systems and government data; with respect to the critical infrastructure environment where government clearly needs to play a role, but in partnership with industry that provides most of that critical infrastructure; and with respect to public information where government should play a minimal role in terms of law enforcement, emergency response, and certainly education. One of our biggest issues with public information is simply the large number of poorly informed users. John Stewart talked about the 20-year-olds who think they know everything but really do not. When you ask the average person, "Do you have a firewall on your home computer? Do you use antivirus software?" the response you get is, "What is that?" If that is the case, there are an awful lot of unprotected systems out there. I think that one key role that government can play is helping with that education process and perhaps even making the tools readily available. For example, it would make sense if government had online links to free open source software for virus protection. Some people might not be willing to spend the $100 that it takes to buy commercial antivirus software but will get the free software if it is readily available. Not only could we make it known to users that they need it but we could also make it easy by providing a link to the free software so that people would not have to pay when they feel that they cannot afford to buy the commercial one.

Chapter 33

Dealing with the Exponential Growth of Cyber Threats

Mr. David Pollington
Director of International Security Relations, Microsoft

Thanks to Microsoft, I have the chance to work with governments and international organizations around the world and it is great to be here in this workshop with such high level representation from international organizations. Our challenge in this particular panel is to discuss how to deal with the exponential growth of cyber threats. So, first let me ask a question about the exponential growth: is that really happening? I have been working in cyber security for ten years now and to me, because I work for Microsoft, the bad days were actually in 2003 and 2004.

EARLY EXPERIENCE WITH SLAMMER, BLASTER, AND SASSER

This is when events named Slammer, Blaster, and Sasser actually destroyed the data and work of so many of our customers by clogging up their networks and slowing them down. No money was stolen, no information was exfiltrated through espionage, but business ground to a halt.

When I think about the number of vulnerabilities, I think about MITRE and the other organizations that we work with in terms of recording the vulnerabilities in software. Five years ago, there were on average about 3,500 vulnerabilities reported in all the different types of software. Last year, it was only 1,600, so the vulnerabilities appear to be coming down. But I know as well as anyone else that botnets appeared in 2004 and since they started to appear, we have been looking at an exponential growth in a new type of crime, which is the rate at which credit cards are being stolen. In 2006, when we first saw evidence of espionage working through our Office programs, causing corrupted versions of Word or Excel or something similar, we saw that they were single instances, individual cases. Three years later in 2009, when we looked for the same vulnerability in Office 2000, we found that it was all over Southeast Asia. The important thing here is that the malware does not go away. Every single month, we clean and update 600 million machines. We collect the information from updating those machines and incorporate it into a security intelligence report. There are lots of statistics there, and this is where I am pulling some of my information from. You can download a copy of this report and if you look back to 2009, this is where you would find the report on the espionage attacks that were done in that particular area.

LESSONS FROM DEALING WITH CONFICKER

But if you look at the latest report which came from the last half of last year, what you will notice is that we did a piece on Conficker. Conficker is simply a piece of exploitation software that tries to steal credit cards. It was patched in October 2008. We patched it out-of-band every second Tuesday and we patched 420 million machines in six days. None of them were in an enterprise; every one of those machines was a domestic machine or a small business machine. Well, six months ago, when we checked our latest stack of statistics, 1.7 million machines were still infected with Conficker. These machines are still infected with Conficker because they are inside enterprises. Enterprises and governments with enterprises are the slowest to patch. So that threat is changing for us.

In a world where we really worry about advanced persistent threats, the persistence may not always be in the event's threat. We have to take out some of the language that we use and understand how these things work. When I think about what solutions we would come up with, I am thinking about cyber crime in terms of stealing things, I am thinking about protecting children online and other things that can be done there, I am thinking about critical infrastructure and how we address that, and I am thinking also about espionage and exfiltration. These are the things that we need to be able to address.

Chapter 34

How to Deal with the Exponential Growth of Cyber Threats

Major General Salvatore Farina
Director of Military Policy and Planning, Italian Defense General Staff

OVERVIEW

This presentation will deal with both the cyber dimension's general framework and the approach of the Italian Defense Ministry to the subject. As underlined during the panels this morning and yesterday, security in cyberspace is a matter of concern in almost every sector of today's society and, in the future, security and defense will increasingly deal with this growing phenomenon. Actors in this field range from states to terrorist groups, criminal organizations, hacktivists, and hackers who can use technologies and means easily available on the "off the shelf" market. In addition, due to difficulties in clearly identifying the originators of an attack, they can act with little fear of retaliation. This means that deterrence cannot work in the same way it worked with the nuclear threat in the past. However, dissuasion—through resilience and advanced capabilities to identify the nature and source of an attack—can discourage, at least partially, potential attackers.

We need to consider two fundamental issues: First, to accurately predict, as much as possible, all opportunities and applications offered by new and emerging technologies, and second, to imagine and evaluate all possible evolutions of cyber threats. An analysis based on this data will give us a clearer picture of the measures and projects that we should promote for the next two decades. Of course, these two fundamental issues can only be achieved in a synergic interdepartmental effort and in cooperation with industry—particularly given that in the case of an attack on economic or financial assets, public or private companies and services, or critical infrastructures, the possible effects could easily become relevant at the strategic level or influence behavior, actions, and news related to ongoing military operations.

NATO'S CYBERDEFENSE POLICIES

This is also one of the reasons why the NATO Strategic Concept (which led to the development of the Cyber Defense Action Plan) considers cyberdefense to be one of the organization's highest priorities. The Alliance is the most suited to face cyber threats thanks to a systematic and efficient combination of:

- Its solid and proven political-military decisional framework,
- Its wide dissemination and capillarity of networks and communication systems, and
- Its reliable intelligence able to inform and support an effective reaction capability.

Italy has signed a Memorandum of Understanding (MOU) with NATO and is carrying out all actions agreed upon.

ITALY'S CYBERDEFENSE POLICIES

Italy's cyber policies are very much in line with NATO's. I will give you a short but broad overview, from the military perspective, of the Italian Defense Ministry's approach to this subject. Cyberspace is the fifth operational domain and is transversal to the others (sea, land, air, space). Therefore, it can directly influence the general planning, operational planning, and the conduct of operations. Given this, the Italian Defense Ministry is committed to accomplishing two main tasks:

- The first task is to develop capabilities and structures that are able to ensure Situational Awareness (SA) at every level in order to maintain a significant advantage over potential opponents. Reacting after an attack could be too late. We are thus developing capabilities to ensure: (1) the constant and continuous monitoring capabilities of our networks on a 24/7 basis, and (2) intelligence support, integrated and coordinated with other intergovernmental institutional structures as well as the NATO Computer Incident Response Capability (NCIRC) in order to share information and improve early warning capabilities (part of the NATO MOU).

- The second task is to protect Italy's own networks and critical IT infrastructures in order to both dissuade and increase resilience against potential attacks (including by adding redundancy).

The core business of defense is operations. In the cyber environment these are called Computer Network Operations (CNO) and are based on three capability pillars: defense,[1] exploitation,[2] and attack.[3] In the short to medium term, the Italian Defense Ministry is mainly focusing on the first two pillars—defense and exploitation—for several reasons: First, defense and exploitation are more coherent with the principles of our national constitution. Second, they are also coherent with the policy guidelines of NATO and the European Union. Third, these are the two pillars on which not only military organizations but also other governmental institutions and all of civilian society place their main focus, thus offering excellent opportunities for common synergies. The latest example is the Inter-Ministerial Working Group (comprised of the Cabinet Office, Ministry of Defense, Ministry of the Interior, Ministry of Economic Development, and subject matter experts) which has recently prepared and submitted a proposal to the Prime Minister for a national operational structure to deal with cyber threats, enhancing defense capabilities at the highest possible level and in a comprehensive manner.

The Official Strategy

The Italian Chief of Defense has recently approved a cyber policy document issuing directives to address operations, planning, and execution in cyberspace. The main components of the policy are:

- The implementation of a new governance system for strategic direction and operational management;
- The evolution of the CERT (Computer Emergency Response Team) in the Joint Cyber Operation Centre which, in addition to system and network protection, will ensure a 24/7 computer network defense capability;
- The implementation of deployable teams and assets in support of theatre operations. These consist of: (1) the definition of specific personnel requirements in terms of recruitment, training, technical skills, awareness, and security considerations, and (2) the development of guidelines for cooperation with industry to ensure a secure chain of CIS procurement with reliable and trusted industrial partners.

These efforts are all the more important in light of the significant transformation process which the Italian Defense Ministry is undergoing in the digitalization of domestic structures and combat assets: We are indeed developing capabilities in the field of distributed networks, called Network Enabled Capabilities (NEC), to allow real and near real-time communication and information acquisition processes, which are a critical aspect of most military operations.

International Cooperation

In any case, an effective defense against cyber threats is only achievable through a comprehensive and multi-dimensional approach at both the national and international levels. For this reason, the Italian Defense Ministry, in addition to a comprehensive approach at the national level, is also fostering the full involvement of other national institutions, industry, academia, the private sector, international organizations, Allies, and partner countries in the process. We believe it is necessary to:

- Implement a permanent link between equivalent cyber structures among/within Allied countries in order to increase alert capabilities based on a structured info-sharing system and common security standards;
- Conduct multinational exercises with various threat levels coordinated by a third party in order to evaluate reaction capabilities, test personnel skills, and increase interoperability.

An example of this comprehensive approach is the Multi National Experiment 7 (MNE7). MNE7[4] is the most recent stage of a series of multinational experimentation campaigns. In this seventh edition, the Italian Defense Ministry is leading a working group whose task is to analyze international law to determine if, where, and how it can be applied to cyberspace. The outcome of this reflection will be a pamphlet entitled, "Guidelines for decision-makers at the political-strategic level to cope with cyber incidents." This working group is composed of representatives from ten countries, all branches of

1 "The application of security measures to protect CIS infrastructures components against cyber attack" (JIC 001–CNO).
2 "l'Azione intrapresa per avvalersi di un computer, nonché delle informazioni ivi contenute, per ottenere un vantaggio" (JIC 00–CNO).
3 "Azione, condotta nei confronti di un avversario, dal territorio nazionale o dall'estero, attraverso l'utilizzo, anche combinato, di computer, sistemi informatici, telematici e cibernetici, al fine di distruggere, disattivare, rendere inaccessibili, alterare, smembrare i sistemi stessi o dati, informazioni e servizi in essi contenuti. Ciò in forma parziale, totale, permanente o temporanea" (JIC 00–CNO).
4 MNE is an international program for experimentation and concept development that is coordinated by the Joint Staffs J7 for Joint and Coalition Warfighting in the U.S. Department of Defense, and, on the Italian side, by the Center for Defense Innovation in the Italian Ministry of Defense – Division III.

the armed forces, the Ministry of Foreign Affairs, the Italian Space Agency, universities (Rome, Naples, and Malta), the private sector, and industry (ENI, Telecom, Finmeccanica, and Selex).

As stated earlier, the involvement of industry is paramount in all phases (inception, implementation, and management). Defense in cyberspace requires technological supplies that, due to the rapid and dynamic evolution of the environment, must rely on accurately selected sources (industry/academia). This means that industry continuously faces new challenges in the production process, which is strongly linked to the national strategic interest, in terms of ensuring hardware and software reliability. This also brings an innovative approach to engineering systems and related services, requiring industry to work closely with the customer given that requirements are explicitly defined, in order to develop new products for cyberspace in the most appropriate manner.

Strategic Communications

I would also like to draw your attention to the strategic communications environment (i.e. STRATCOM). Despite being a sector that is still under development, it is of vital importance and has huge implications for cyber space. The influence of traditional communication channels (TV, radio, and newspapers) on public opinion is gradually being replaced by complex interactions between information users and producers in a global network of blogs, websites, and social networks. Today's citizens are no longer "passive receivers" of information. They can interact with mass media as journalists, commentators, or opinion leaders, becoming active players in information and communication. The most recent examples, mentioned in a previous panel, came from the socio-political uprisings of the Arab Spring.

Public opinion can decisively influence many decisions about joining, remaining in, or withdrawing from international military interventions. Therefore, it is mandatory to maintain a close link and strong coherence between STRATCOM and Computer Network Operations, taking advantage of and leveraging any possible synergies.

CONCLUSIONS

To conclude, I will summarize the main concepts:

- Cyber threats do exist, are significantly increasing, and we must be ready to counter them with cyber operations, namely Computer Network Operations;
- However, in order to legitimately operate in the new cyber domain, we still need an adequate legal "umbrella" at both the national and international levels, and if necessary even through international treaties or agreements;
- NATO has an essential role and is the best placed organization for facing cyber threats and increasing mutual cooperation;
- At the national level it is necessary to define and implement governance, directive structures, joint cyber operation centres, special teams, and to recruit and retain personnel;
- The implementation of permanent links for the structured sharing of information and alert levels as well as common exercises and training programs is highly desirable with Allies and partners at the international and national levels;
- Industry must be an active part of the effort to combat cyber threats in all phases, including in the formation and recruitment of personnel;
- Personnel are and will remain the focus of any future capability developments; it is extremely important to select and continuously train qualified human resources to be employed in this very sensitive strategic sector.

The cyber challenge involves a large range and number of risks and we must be prepared to face them. It is not possible to neutralize cyber threats in isolation; we need to all cooperate.

Chapter 35

Italy's Response to the Cyber Threat Challenges

Mr. Domenico Vulpiani
Director General, Italian National Police

As Director General of the Italian National Police, I have gained my police experience mainly from coping with terrorism and cybercrime. I would therefore like to present my analysis of Italy's response to cyber threats, discussing the evolution of cyber threats, a description of the strategies used to combat them, and potential future scenarios.

THE EVOLUTION OF CYBER THREATS: CYBER CRIME, CYBER TERRORISM, CYBER ESPIONAGE, AND CYBERWAR

Cyber threats have evolved in recent years, both in terms of the targets and the actors who carry out such threats. Initially, in the 1970s and 1980s, the Internet attracted individuals who, for recreational purposes and motivated by curiosity and the desire for intellectual challenge, began to experience the power of the World Wide Web, engaging in activities that—while not conducting any apparent criminal activities—were certainly aimed at violating computer systems. As time went on, hacking became more evidently a criminal activity whose purpose was to attain economic or other benefits through the use of increasingly sophisticated attacking techniques, ranging from computer intrusions to the realization of particularly malicious viruses to phishing. In terms of cyber crime, fraud, online child pornography, and hacking represent the main areas where criminal acts are carried out. Terrorist organizations also make use of the Internet for propaganda purposes or proselytizing, giving rise to the new term "cyber terrorism." This is the case, for example, of anarchists or Islamic terrorist organizations that distribute online manuals for the training of militants, providing precise instructions for launching attacks and manufacturing homemade bombs, or even instigating the formation of so-called homegrown terrorist cells.[1]

Cyber threats even target companies possessing know-how that is essential to a country's economic underpinnings. The core business of many of these companies is being increasingly threatened by cyber espionage. This rise in cyber espionage is also demonstrated by a growing number of attacks on corporate websites, as exemplified by Julian Assange through Wikileaks.

In comparison with the past, when criminal acts on the Internet represented a unique event, at present cyber threats have gradually evolved toward more serious forms, and the actors are different from traditional hackers, occasionally involving the countries themselves. This is the case of Stuxnet,[2] a virus used to harm nuclear centrifuges at Natanz, which led to the suggestion, from the very first moment of its discovery, of the involvement of countries interested in stopping the Iranian nuclear program in a cyber war framework. Even the somewhat unusual use of social networks by NATO countries during the so-called Arab Spring[3] in support of the insurgency shows that the Web has now become a place of political-military activities that go well beyond any actions of a criminal nature. We can come to the conclusion that if the term cyber

1 After the harsh repression of Islamic terrorism following the fall of the Twin Towers that culminated in the elimination of Osama Bin Laden, Al Qaeda is now making more frequent use of the Internet.

2 The malware was supposedly introduced in the Natanz facility through a USB stick; it initially infected the hard drives of computers inside the nuclear power plant, then it reprogrammed the Programmable Logic Control (PLC) software of the centrifuges, and finally it exited the facility hidden inside the laptop of one of the many engineers. Once connected to the Internet it began to replicate itself and became publicly visible.

3 The key role of social networks in the Arab Spring is well-known, but even more important is the role played by the United States in supporting the rebels, providing them with appropriate services to communicate. You will certainly remember the telephone service set up by Google in Egypt about one year ago to avoid web censorship. It allowed a person to leave a vocal message that was automatically translated into text and posted on Twitter. The proof that the Internet has become the primary enemy of dictatorships is represented by the measures that the Tehran authorities have taken on the occasion of the 33rd anniversary of the Islamic Revolution of 1979. The services offered by Google, Microsoft, and Yahoo were made inaccessible, probably out of fear of a new revolutionary wave. Reportedly, Iran has laid a parallel network designed to replace the global network, thus independent from it, with the intent to isolate Iranian communications and be able to spy on all the communications taking place over the network.

crime" once described the cyber threat in its entirety, now we must make use of at east three other terms when addressing the wide issue of cyber security: cyber terrorism, cyber espionage, and cyberwar.

Italy, in line with other countries, has addressed cyber threats with a particular view to their criminal and terrorist aspects, providing a response essentially articulated in four strategic areas:

- appropriate and updated standards;
- a law enforcement agency specialized in combating cyber crime;
- an intense public-private partnership; and
- a broad international collaboration.

DESCRIPTION OF STRATEGIES TO COMBAT CYBERTHREATS: REGULATION AND THE POSTAL AND COMMUNICATIONS POLICE

In our country there has been consistent regulation and regulatory compliance starting from 1993,[4] when cyber crimes were included in the Penal Code. In 2008, the Convention on Cyber Crime was adopted and integrated in our legal system.[5] Other important regulations to combat cyber crime were issued as well: two laws aimed at combating online child pornography (Law No. 269 of 1998 and Law No. 38 of 2006),[6] a copyright law,[7] and finally a law for the protection of critical infrastructures.[8]

With regard to investigative competences, a single agency was appointed as the primary law enforcement agency in charge of handling cyber crime. This is the Postal and Communications Police Service, a special branch of the Italian National Police consisting of nearly 2,000 highly skilled investigators working in approximately 100 offices located throughout the national territory. The Postal and Communications Police has the exclusive power to combat online child pornography and been granted the right to use certain investigative tools (controlled deliveries and undercover activities). The above mentioned law[9] also states that the Postal and Communications Police shall ensure "the protection of information services" pertaining to the Critical Information Infrastructures (CII) identified by a decree of the Minister of the Interior dated January 2008.[10]

With the entry into force of these laws, three divisions with specific tasks have been established within the Postal and Communications Police:

- The Online Police Station,[11] an interactive police portal that any Internet user can access to send reports, file complaints, and ask questions concerning cyber crime.
- The CNCPO[12] (Centro Nazionale per il Contrasto alla Pedopornografia Online, or National Center for Fighting Child Pornography Online) is responsible for coordinating the complex activities required to fight child pornography online, especially undercover investigations. Additionally, the Center is tasked with drawing up a blacklist of websites containing child pornography and sending it to ISPs (Internet Service Providers) on a daily basis, with the aim of preventing users from inadvertently coming across them.
- Finally, in order to counter terrorist threats against critical infrastructures, the CNAIPIC[13] (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche, or National Cybercrime Center for the Protection of

4 Law No. 547 of 23 December 1993 (O.J. No. 305 of 30 December 1993) entitled "Amendments and integrations to cyber crime rules contained in the Penal Code and in the Penal Procedure Code"

5 Law No. 48 of 18 March 2008 entitled "Ratification and adoption of the Council of Europe Convention on Cybercrime, signed in Budapest on November 23, 2001, and adaptation standards of the national legal system"

6 Law No. 269 of 3 August 1998 entitled "Rules against the exploitation of prostitution, pornography, and sexual tourism involving minors, as new forms of slavery" is aimed at punishing criminal conduct involving the sexual exploitation of minors to produce online pornography. This law was subsequently modified in Law No. 38 of 6 February 2006 entitled "Measures to combat the sexual exploitation of children and child pornography, including through the internet" with a view to making it more efficient against some particularly subtle aspects of online child pornography that seemed to be invisible to investigations.

7 Law No. 128 of 21 May 2004 (O.J. No. 119 of 22 May 2004) entitled "Conversion into law, with amendments, of Decree-Law No. 72 of 22 March 2004 concerning measures against the illegal electronic dissemination of audiovisual material, in support of motion picture and other entertainment activities"

8 Law No. 155 of 31 July 2005 (O.J. No. 177 of 1 August 2005) entitled "Conversion into law, with amendments, of Decree-Law No. 144 of 27 July 2005 concerning urgent measures to counter international terrorism"

9 See footnote 8

10 Ministerial decree of 9 January 2008 entitled "Identification of nationally significant CII"

11 http://www.commissariatodips.it

12 Established with Law No. 38 of 2006 and inaugurated on 1 February 2008

13 Established according to Law No. 155 of 2005

Critical Infrastructures) has been created. This center is not a CERT but rather a SOC[14] (Security Operation Center). The various SOCs of private companies or institutions operating services that are fundamental to the functioning of the country can connect to the CNAIPIC to report incidents or other pertinent information involving cyber security. At the same time, the Center releases to the SOCs any relevant alerts or information gathered from the Intelligence activities it conducts.

Critical infrastructures can benefit from these services upon entering into an agreement (or "Convenzione") with the Ministry of the Interior. Several agreements have been signed already, the most important being with the Bank of Italy, the CONSOB (National Commission for Companies and Stock Exchange), and the RAI (Italian State Television). Without listing them all, most of the CII identified in the economic, energy, transport, and communication sectors have already signed such agreements.[15]

The three centers of the Postal and Communications Police have close relations with their counterparts in other countries. In particular, the Postal and Communications Police is part of several international networks, including Interpol (which brings together 188 countries) and Europol (which encompasses 27 countries). Regarding the fight against the online sexual exploitation of minors, in November 2008 the Postal and Communications Police contributed to the creation of a group of world-class specialized law enforcement agencies, giving shape to the Virtual Global Taskforce which includes police forces from Australia, Canada, the UAE, Italy, New Zealand, the United Kingdom, the United States, and Interpol. Furthermore, through their membership in the G8 High Tech Crime Subgroup, in 1999 the representatives of the Postal and Communications Police conceived the 24/7 Contact Points Network, which currently includes cybercrime-fighting agencies from 56 countries. Through this network it is possible to submit requests for the "freezing" of digital data—essential in international investigations—that might otherwise go missing.

FUTURE SCENARIOS: CLOUD COMPUTING AND ELECTRONIC WARFARE

Cloud computing and electronic warfare exemplify the main challenges of the future: cyber espionage and cyber war. The use of Cloud computing represents a major opportunity for companies in terms of cost savings as well as greater flexibility and scalability of resources, so it is reasonable to believe that in the near future all companies will embrace this technology. It is obviously true that this approach will bring positive results, particularly since increasingly powerful and friendly devices will enable users to have immediate access to their data from anywhere and work even when they are out of the office. At the same time, there are concerns related to the security of data residing on servers around the world, which are increasingly being stored in countries where it is least expensive to do so. However, economic rationales do not always pair with what is politically wise: How can we be certain that, in the event of a conflict with one of the countries where we store our data, the country does not decide to hold our data hostage?

Nevertheless, in times when the world relies increasingly on electronic warfare for the resolution of armed conflicts, and military drone bases are being enhanced and developed, the security of networks—especially military networks—has become a top priority when it comes to safeguarding the security of a country. This is particularly apparent if we consider that the Iranians have recently managed to hijack a U.S. drone, making it land on a territory

14 CERTs activities are limited to the collection of incident and software vulnerability reports submitted by users and the sending out of alerts accordingly so that appropriate measures can be taken. Based on my experience, Internet users hit by a virus are reluctant to inform others about it out of fear of damaging their own reputations. Yet it is important to be able to compare attacks on different targets launched using the same technique in order to be able to trace their common source.

15 The first agreement was signed with Poste Italiane (a major Italian operator in the postal services area and was followed by agreements with banks and other bodies in the economic sector: Bank of Italy, ABI (Italian Bank Association), CONSOB (National Commission for Companies and Stock Exchange), Intesa San Paolo Bank, and SIA SSB (a European leader in financial services and payment systems).In the communication sector, agreements were made with ANSA(the largest Italian press agency), Telecom Italia, Vodafone, RAI (Italian State Television), and H3G. In the transportation sector, agreements were signed with ENAV (National Air Traffic Control Agency), ACI (an IT body), ATM (Milan Transport Network), and Italian Railways. In the energy sector, they were signed with TERNA (the Italian electrical grid operator), ENEL (the largest Italian power company), and ENI (National Agency for Hydrocarbons). In the technology industry, agreements were signed with Finmeccanica, Symantec, Cisco, and Microsoft. As you can see, the context is varied but still susceptible to change as still more agreements are to be signed, especially with operators that possess technological know-how that is vital to the nation. Industrial espionage takes advantage of the opportunities the Internet presents in this regard, so defense against these types of intrusions will be the main priority for all developed countries in the near future. Investigations concerning critical infrastructure are conducted jointly with the judicial authority by the CNAIPIC's operatives, who also carry out Intelligence activities aimed at identifying potential threats in order be able to repel them promptly.

under their jurisdiction. In order to effectively face the new threats of cyber espionage and cyber war, it is necessary to enlarge the network of agencies commissioned to combat cyber crime, particularly by involving Isntelligence agencies and military forces. Italy is already heading in that direction, at least partially, as other speakers will describe.

Chapter 36

How to Deal with the Exponential Growth of Cyber Threats

Dr. Douglas Maughan
U.S. Department of Homeland Security

Cyber security is now among the top five missions of the Department of Homeland Security (DHS) along with countering terrorism, borders, immigration, and national resilience. This has led to some interesting activities both on the operational and Research And Development (R&D) sides: Today, many parts of Homeland Security are much more engaged in cyber security and we are working very closely with law enforcement and the operational side as part of our Research and Development mission, which is where I sit.

THE COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE

Homeland Security's activity is actually part of a larger government activity. In May 2009, the White House issued the Comprehensive National Cybersecurity Initiative, which can be consulted on the whitehouse.gov URL. It is a government-wide initiative that includes operations, R&D, discussions about issues like deterrence and, more importantly, working with the private sector and working with the critical infrastructure. As was repeatedly mentioned, there must be participation from the private sector as we move forward in this space. This initiative guides some of the ongoing Research and Development activities. There are actually 15 agencies within the U.S. government that fund R&D, some with much larger budgets like the Department of Defense, some with smaller budgets. In December 2011, an inter-agency working group which I co-chaired released a Federal Cybersecurity Research and Development Strategy which discusses how the different agencies will fund research and what types of research will be funded. Let me highlight two areas: One specific part of our program is focused on Transitioning Technologies. Those of us who have been in the Research and Development space for a long time will understand that research often ends up on the shelf collecting dust and never makes it out as a commercial product. So a part of our federal R&D plan highlighted this problem and discussed ways to get more funds into commercializing and transitioning technology. Another key area of our federal R&D plan deals with some other national initiatives: there are national initiatives for health care, smart grid, trusted identities, and for cybersecurity education, which I will talk about in more detail.

INTERNATIONAL R&D COLLABORATION FOR CYBERSECURITY

At DHS, we are well-positioned to work collaboratively on an international level. As Dr. Lute mentioned, this is very important to us. Currently, the Science and Technology Directorate has eight international agreements in place for cybersecurity with the following countries: Australia, the U.K., Canada, the Netherlands, Sweden, Israel, Germany and Japan. We are able to do those types of international agreements for collaborative research and development because our research is unclassified and we believe that this is significant. I encourage anyone who is interested in R&D collaboration to discuss it in this forum. Perhaps a future workshop might even address how we could do more collaborative R&D work. Since our panel's topic asked what we can do about these threats, we can definitely work together on new technologies and new ideas.

CYBERSECURITY EDUCATION

As to cybersecurity education, I am sure that every country faces the same problem we do: finding people who are able to work in this technical area. We are struggling with this in the U.S. and have launched an initiative called the National Initiative on Cybersecurity Education, which aims to create a general awareness from kindergarten through college, and

to develop a work force since many of the existing workers are not trained in this technical area and would need to be. This initiative is moving forward. For example, our Science and Technology Directorate is funding the National Collegiate Cyber Defense Competition with over 100 U.S. colleges and universities. Each regional winner participates in a national competition that is held every April in San Antonio. The University of Washington won this year. We are trying to take our methodology to anyone who is interested and are already helping the Australians and Canadians do collegiate competitions.

We are also working with high school students and are funding the U.S. Cyber Challenge, which is aimed at reaching these kids at that critical time in their education. We fund summer camps, competitions—all aimed at the next generation. I do not know if there is anyone in this room who is under thirty, which is a problem because many of us will retire very soon and we do not have anybody to take our place. So, a discussion on work force development (including protocols, i.e. the Border Gateway Protocol, DNS, routing) might be something that this workshop might consider. We believe that a clean slate approach requires a ten-year investment and we cannot wait. We need to address this issue because everyone has to deal with it. It is unclassified, and it does not have anything to do with the military. As a quick side note to show you why this education issue is a potential problem, I recently learned that a U.S. corporation was sponsoring a hackathon for kids in which twelve-year-olds and under could learn how to hack systems. This is not the type of education that we want to be providing to these young kids. So we need to educate them properly as early as possible and teach them about values, about what is good and bad, and about these technologies; we do not need companies to initiate these kinds of contests.

TRANSITIONING TECHNOLOGIES, INFORMATION SHARING AND LAW ENFORCEMENT

I mentioned earlier that Transitioning Technologies is one of our key activities. As we fund R&D, it is extremely important that it makes it out into the commercial market place. We do this in many ways. One is through open source software. Since our program is completely unclassified, we can make our technologies available and we have had several successes. One of them is an open source IDS (Intrusion Detection System) and we are aware of at least nine vendors, two of them international, who have picked up this open source software package and made it available as part of their commercial product. Again, here is an area in the world of collaboration: Open source software can be shared openly and with everyone and, as we think about cyber defense and innovation, open source becomes an economic discussion for us. It is potentially cheaper than proprietary software, and it offers an opportunity to look at technologies without a large investment. The creators of these open source packages are small businesses, groups of two, five, or ten people who are often more innovative than some of the larger companies. We are supporters of entrepreneurship and try to help these young companies because we believe that their innovative ideas are key to cyber security.

Two other topics are worth discussing briefly. One is Information Sharing. As Deputy Secretary Lute discussed in her address, the U.S. government is working very hard on information sharing, not only across governments, but with the private sector as well. Because our mission is to work with all our critical infrastructures, we are very focused on trying to get them the information they need. I will use the example of a neighborhood: If you knew that someone is going through your neighborhood breaking into houses, wouldn't you tell everyone you could in the neighborhood? We are trying to do just that.

Another important area is Law Enforcement. Criminals always have the newest technology, since they can afford it. But what about our law enforcement officers? Often, they are the last ones to get the technology. So, with our law enforcement partners, we are focusing on building new technologies to help them get ahead of the curve. Some of these technologies are available as open source and we are definitely making them more broadly available.

Finally, from an Internet and R&D perspective and as a follow-up to the presentation by Telecom Italia's CEO, it is worth mentioning that, as a department working within the Federal Government, we are actively supporting and pushing forward solutions for the current Internet Protocols, the Domain Name System, to try and secure some of the key pieces of the Internet and do it now. This is another focus area of ours in which we work with the private sector to put new security technologies on the existing Internet.

Chapter 37

Electronic Warfare in the 5th Domain

Ing. Daniela Pistoia
Vice President of Research and Advanced Systems Design, ELT|Elettronica

Elettronica is a private Italian company, with an order book of €1.2 billion and revenues of €200 million per year. It is one of the largest electronic defense (or spectrum warfare) companies. Its mission is to guarantee spectrum superiority to the user, with products covering the whole panorama of spectrum warfare: radar, electro-optical, communication, and cyber. Over the last few years, the company has launched an ambitious growth plan in order to increase its revenues based on this strong product portfolio. Every year, approximately 10% of revenues are reinvested to fund internal R&D programs, which bring our products to the level of technological maturity required for integration with platforms of customers or end users. Within this framework, we have created a new family of products for the rapidly growing frontier of cyber warfare. Accordingly, we will talk about electronic warfare in the 5th domain.

NETWORK-CENTRIC WARFARE

Network-centric warfare is the new paradigm for the armed forces, paramilitary organizations, and government agencies. These organizations are becoming highly interconnected throughout digital networks. This connectivity makes it possible to significantly increase information exchange among cooperating platforms, allowing better situational awareness within their environment. The network-centric warfare paradigm offers a new level of capability in terms of cooperation and synchronization of elements, providing unprecedented command and control (C2) response and mission success.

While this real-time connectivity offers advantages, it also provides new opportunities to potential opponents. The vulnerability regards the network itself, as the cooperating mobile platform needs to be interconnected through wireless communication infrastructures, with the disadvantage that it can be intercepted, corrupted, and jammed. An example of such a scenario could be the penetration of an air defense command and control, sensors and weapon systems network, leading to the inhibition or modificaton of data flow, providing false awareness information.

- This happened in September 2007 during the Israeli Operation Orchard strike against a nuclear facility in Syria. In this case, a dedicated tool for noise, fake signals, and the injection of false information in the Syrian air defense network led the command and control operators to believe that there were no enemy platforms penetrating the controlled airspace. Nonetheless, Israeli non-stealthy warplanes flew in undetected and completed the mission.
- In a more recent event in December 2011, a U.S. Lockheed Martin RQ-170 Stealth Sentinel unmanned air vehicle was forced to land on Iranian soil and was captured by Iranian forces. According to open sources, this was achieved by blocking communication between C2 and the UAV, forcing the Stealth Sentinel into an automatic recovery mode, while injecting fake GPS signals to deceive the UAV's navigation system.

These episodes clearly show that electronic defense, intended to manipulate the electromagnetic spectrum in order to inhibit the enemy's offensive capabilities, is not limited to the radar world, but also finds a perfect application in cyber warfare, where spectrum manipulation leads to data alteration, causing heavy damages to the opponent's C2 chain.

ELETTRONICA'S APPROACH TO CYBER WARFARE

Thanks to 60 years of experience in the electronic warfare sector, encompassing the whole range of defensive and attacking capabilities—from core radio-frequency (from SIGINT to jamming passing through platform protection) to infrared and communications—Elettronica has approached the cyber warfare domain, focusing on the electro-magnetic spectrum, instead of the computer networks, and using its capability to manipulate such operational environments to provide both

protection and active defense. Elettronica's response to the new requirements of cyber warfare is based on the first command and control (C2) system specifically developed for distributed electronic defense systems, called LOKI ELT/950. The name comes from the Norse God whose powers included the ability to adapt to different environments.

Conceived for network-centric operations. LOKI is the first C2 system developed for network-centric electronic warfare. The system is based on lightweight hardware and real-time software enabling the various type-independent platforms (air, ground, and naval) to work together, exchanging data on the electromagnetic environment to counter the defined threats. The operational concept is based on the Boyd OODA loop concept (observe, orient, decide, and act), which states that an opponent's action can be countered by observing his cycle of decision-making, rapidly anticipating it, and defeating it.

Decision-making support. LOKI does this in an automated environment, as is usual for the typical reaction times of electronic warfare. The system performs automatic data-fusion, exploiting a range of passive sensors including signal intelligence (SIGINT) as well as self-protection or situational awareness systems according to a distributed electronic surveillance architecture. In this phase, it provides a decision-making support function to the C2 operator, such as where and how to best deploy the sensors' assets in space and radio frequency domains to reduce interference and increase intercept probability.

Creating a situational picture. LOKI uses all the sensors in different ways to create a situational picture, establishing which enemy platforms are present in the area, identifying, locating, and providing a function to them. The system selects the most appropriate and distributed response against identified threats, accounting for scenario geometry and suggesting electronic warfare techniques for the "act" phase. In the latter case, LOKI synchronizes actions of cooperating platforms to carry out complex, distributed electronic warfare operations.

Cyberdefense. For cyberdefense, LOKI identifies suspect behavior in networked platforms. If an intrusion is detected, it verifies the identity of the suspect platform and, if necessary, removes it from the network while alerting electronic warfare management. LOKI can detect a compromised platform by monitoring data-flow integrity, timing and quantity and other parameters. Suspect behavior triggers additional security challenges to refine the analysis. The system provides a security layer when a network is compromised. It identifies and insulates a threat when a breach occurs and reconfigures the network to operate, while bypassing isolated nodes.

Analysis. All actions are recorded and stored for analysis, as well as to craft procedures and techniques, and to fine tune system logic in a machine-learning approach.

Active-defense cyber operations. Elettronica has, however, provided LOKI with the capability to manage active-defense cyber operations. To conduct these activities, based on the developed core technologies and system engineering in the electronic warfare sector, in addition to the company's knowledge of information operations, Elettronica has developed TEMPESTA (Transmitter of Electro Magnetic Power for Electronic Surveillance and Tactical Attacks), which provides physical and infrastructural layers exploitation and the capability to conduct cyber active-defense operations on the complete range of wireless distributed networks, including mobile phones and navigations (i.e., GSM, WiFi, WiMax, GPS, UMTS), in addition to satellite communications.

Testing. LOKI and TEMPESTA are tested in a numerical rig using a real-time distributed simulator of wireless networks. The simulator provides scenarios, characteristics of radio devices and propagation, routing protocols, and threat attacks to the network. Elettronica is discussing with the Italian Ministry of Defense plans to demonstrate the suite in a simulated operational environment to finally validate it in "under-law" conditions.

As a first realization, LOKI is an element of the broad network-centric modernization effort being implemented by the Italian Ministry of Defense, called Forza NEC. Elettronica is the Forza NEC design authority for the electronic warfare element, which is to include a tactical C2 system with a data-fusion center.

CONCLUSION

In conclusion, the company is addressing the branch of information warfare relating to the so-called computing systems network operations, versus the more commonly addressed computer networks operations—when assets are deployed and interconnected by a wireless infrastructure—with the intention of intercepting and exploiting both the infrastructure and/or the information itself, using the electromagnetic spectrum as a physical layer.

Chapter 38

Dealing with the Advanced Cyber Threat: Observations, Assessment, and Recommendations

Ms. Harriet Goldman
Executive Director of Cyber Mission Assurance
The MITRE Corporation

INTRODUCTION

Working for MITRE, which is a federally funded research and development corporation operating in the public interest, I sit at the crossroads of government, industry, and academia. In my 30 years of experience in the cyber security field, I have witnessed many changes—but nothing that compares to the dramatic shift in the sophistication and magnitude of cyber attacks and their consequences during the past seven years. This has altered the landscape dramatically and we have to change our way of thinking about the problem. In particular, focusing solely on protection and on keeping our adversaries out is insufficient because, quite frankly, we cannot keep them out. My remarks will cover three areas: First, I will share some of my observations on the cyber security discussions of the past few days. Second, I will identify and assess the challenges we are facing given the current political, economic, social, and technical environment. Third, I will recommend some proactive approaches to deal with the cyber security challenge.

OBSERVATIONS

During the discussions, we have used the term cyber security to refer to anything ranging from cyber hacktivism to cyber crime to cyber espionage to cyber warfare. Indeed, we do not always have a common understanding of what we are referencing. Who is the adversary and what is the threat? Is it the hacktivist? Is it the cybercriminal? Is it the nation-state? Cyber security is not one-size-fits-all. We need to understand and articulate the threat, the environment, and the context—particularly the adversary's intent and capabilities—if we are to make progress in the solution space.

Although the notion of cyber defense treats cyber as a separate domain, we need to understand that this is not the case; cyber is integral to all other domains, including business, warfighting, government, and society's way of life. We need to focus on understanding its social, financial, and political effects. We need to view cyber as an element that enables these other functions and missions, not as the area of focus itself. If we treat cyber as an independent topic, we cannot understand the full repercussions of the threat. We should therefore stop talking about defending cyber and instead talk about defending missions, defending businesses, defending critical infrastructure and defending our way of life.

There were also questions about what is the right level of funding for cyber protection, as if perhaps we could pick a number or percentage out of the air. There is no single answer. It is a continuum: If you are dealing with the advanced cyber threat then you need to spend much more. If you are dealing with low-level hacktivists you should be spending a lot less. We need to understand who the threat is—as well as its potential impact on and consequences for our missions, businesses, and society—in order to determine how much to spend. Indeed, the amount and focus of spending should be based on a risk management approach.

ASSESSMENT

We have spent large sums of money on security solutions yet our systems remain vulnerable to attack. The notion that we can achieve 100% protection is not only unrealistic but also gives us a false sense of security that puts our missions and

businesses at risk, so we have to eradicate this way of thinking. The cyber defenses generally available today, which we have tended to purchase off-the-shelf, are low-grade technology. But they can be quite useful, and we ought to apply them and apply them properly, because they will defend against the lower-level threats against our less essential systems. However, they are often ineffective against most forms of higher-level cyber attacks targeting our most mission-critical systems. We may have to invest funds in order to obtain more advanced or trusted technologies because they are not going to be required by the general populace; you are not going to convince a vendor that they should develop such products because they will be bought by the masses.

We have a lot of legacy systems that were developed without security in mind. Yet now we have moved toward net-centric warfare operations that involve interconnecting all of our systems, making them vulnerable to cascading failures and effects. That is, if one part of the network is attacked there can be a domino effect throughout. Furthermore, the systems are not very modular or modifiable; we cannot easily pull out vulnerable portions of the systems and replace them with new components. Moreover, our systems have become so complex that we really do not fully understand them or their behavior, especially across governance domains. At times, our adversaries have probably mapped out our systems better than we have. And sometimes they know our tactics, techniques, and procedures better than we do.

These are austere times. As a result, we have moved toward primarily commercial off-the-shelf, homogeneous products and have also been centralizing data and systems because the total cost of ownership is much lower if we do so. But by centralizing and reducing diversity, we have made ourselves vulnerable to a single point of attack and technology vulnerability, leaving us open to an all-or-nothing deal if we are attacked successfully. Therefore, some of these cost saving and business efficiency measures need to be balanced with consideration of their impact upon security. Fortunately, virtualization is available, making it possible to bring back the diversity of products we once had and distribute data and systems more broadly in a more cost effective manner.

All too frequently, we jump to the next emerging technology without first understanding its ramifications in terms of security. The more recent rush to Cloud computing holds promise but could be disastrous if not considered properly. The fiscal pressures we are facing will continue to get worse, so we need to find ways to reuse and repurpose the investments that we have made. Consequently, we must compensate for our inability to achieve full protection by ensuring that we can accomplish our missions despite cyber attacks.

RECOMMENDATIONS

Given this situation, what can we do about it? I would like to make three recommendations:

*1. To focus on mission assurance, resilience, and the continuity of mission critical operations while under cyber attack***.** At present we have two separate groups—the mission operators, or the people that execute the missions, and the cyber operators, or those that run the IT in the operation centers or are the defenders—and they do not speak the same language. We therefore need to bring them together to understand the mission dependencies on IT. This is not rocket science but it is good mission assurance engineering. If we do this, we can start looking at what we do know about the threat; we do not know everything but we know a lot. We can perform a threat susceptibility analysis of the environment. We can start making some modifications and separating architecturally mission critical elements from less critical ones—we have to understand what is mission essential and what is not. This will help us determine alternative ways to conduct mission critical operations when we are under attack.

We will then be able to apply our bag of tricks, which is quite broad. Our traditional information security techniques are still useful and we also have anti-tamper techniques and supply chain strategies. However, there is also one thing we have not yet applied: resilience.[1] The term is not always clearly defined, and as a result some people think of resilience as simply disaster recovery and ensuring the continuity of operations. Although resilience draws upon these notions, it is much more complex. For one, we are not building highly survivable, robust systems because the cost is prohibitive. We do so for some components of our systems but we certainly cannot do so for the entire system. Furthermore, most disaster recovery and continuity of operations notions are based on the premise that there is a single incident, usually a natural disaster or the failure of a component. In such cases, building in redundancy is sufficient to solve the problem. However, we could experience a prolonged, multi-pronged cyber attack campaign. In that case, these techniques, while still useful, are insufficient. We therefore need resilience tactics in such a scenario.

Resilience requires several new approaches. First, we must architect our systems differently, enabling us to move things

1 The best definition I have come across is "the ability of a system to provide and maintain an acceptable level of service in face of faults (unintentional, intentional, or naturally caused) affecting normal operations." Source: www.enisa.europa.eu/act/it/past-work-areas/procent/eg1/gorniak

around and to change our systems significantly so that we are not a static target and cannot be attacked easily. The idea is that, by the time attackers go through their reconnaissance phase in order to understand our systems, build their exploit, and then execute it, we have changed our systems enough so that the attack may not work. This is called moving target defense. Furthermore, virtualization technology makes it possible for us to easily move applications to new servers; we can bring capabilities up and down readily so that we can return to a known good state. By contrast, if all we had was redundancy as a means of defense, a technology specific attack would work again and again. Second, we must operate our systems differently. We need to develop our tactics, techniques, and procedures so that we have alternative means of accomplishing the mission. This might mean resorting to manual methods, including conveying information over the phone instead of using the network. We have been working with the community to try to achieve consistency in labeling these techniques, establish common metrics to measure their impact, and determine their cost effectiveness.

2. To facilitate integrated mission and cyber situational awareness. There are many products on the market today that will provide situational awareness for our cyber technology. They have all kinds of bells and whistles, colorful alerts, nice mappings, and event logs. However, they do not help us to understand the impact to the mission. It is therefore important to bring together our mission situational awareness and our cyber situational awareness.

We can extend and improve these products. We have also been working to bring the mission operators and the cyber operators closer together and recently ran a cyber-oriented simulation exercise with both groups. The exercise showed that the cyber operators often do not understand the mission dependencies on the IT they operate and mission operators often do not understand the implications of being served up bad data. When there was a problem, the cyber operators would generally shut down the system, effectively causing a self-denial of service. Conversely, when the mission operators saw unusual data readings, most of the time they did not realize that the information they were seeing had been modified. Thus, the exercise raised concerns not just about the availability of the system in the event of an attack—for it is obvious when you do not have access to your system—but also about the trustworthiness of information given that attackers can manipulate or modify the data, the system, or other elements that the mission operators base their decisions on.

3. To enable threat information-sharing. During the discussions, we have repeatedly talked about how to get the community to better share information regarding threats. In our experience, trying to get organizations to share information about incidents they have experienced does not work; no one wants to talk about their exposure or their vulnerabilities. They certainly do not want to admit that they have been successfully attacked. However, they are willing to share information about indicators and warnings. They may have observed these threats because they were attacked or they may simply have collected the information by setting up a special network to monitor and capture what their adversaries are doing in their systems. By approaching the issue in this manner, we will be far more successful in enabling information sharing.

Interestingly, we have observed that the critical infrastructure sector is very willing to share threat information among each other since security is not viewed as a competitive area or differentiator. Moreover, they understand the interdependencies of their systems. Their networks are often interconnected to one another, e.g. gas pipelines or the electric grid. We have also found that regional groups are particularly willing to share, even though there are many different kinds of businesses involved, because they know one another and therefore have established an element of trust. Thus, we need to favor approaches that will help build trust in order to encourage the sharing of threat information.

Chapter 39

Impact of the Internet and Social Media on National Security and Regime Change

Mr. Donald Proctor
Senior Vice President, Office of the Chairman and CEO, Cisco Systems

The genesis of this panel actually occurred at the conference in Paris last year when Admiral Zappata asked a very insightful question near the end of the presentations. The Arab Spring was very fresh in everybody's mind back then and we had some good side conversations about it. The Admiral asked how people in this region were using social media to collect and organize and ultimately bring about changes in the government. We have already heard during the conference that over a billion people around the world are connected via Facebook and Twitter alone, and so I think that the question Admiral Zappata raised was very prescient. What was the impact of social networking in the Arab Spring? And have we begun to see something we might call the "Twitter Revolution"?

THREE FUNDAMENTAL QUESTIONS ON THE SOCIAL MEDIA

As I have been thinking about this session over the past few weeks, I jotted down a couple of sound bites that I thought might be interesting to plant as we get started. One sound bite is from General Keith Alexander who is the Commander of the U.S. Cyber Command and Director of the National Security Agency in the U.S.; the other sound bite is from John Perry Barlow, the co-founder of the Electronic Freedom Foundation. Many Americans know him as the songwriter for the rock band, The Grateful Dead. I do not know if General Alexander and John Perry Barlow have ever been quoted together before but if this is the first time, remember that you heard it here.

The first sound bite is: "The United States finds itself in an awkward position to at once promote freedom of expression at home and abroad, yet struggle against forms of expression that it reviles." You get to guess which one comes from which person—it is not too hard really.

The second sound bite is: "(Protecting the private sector) doesn't require the government to read their (e)mail…It requires…the Internet service provider or (the) company to tell us that (a security) event is going on… And it has to be at network speed if you are going to stop it." So, it is perhaps not too surprising that the latter quote was from General Alexander.

In this panel, we are going to try to explore at least three fundamental questions.

- What is the impact of social media such as Facebook and Twitter on social unrest and regime change?
- What can governments learn from the use of social media and Internet technologies by their citizens?
- How should governments protect the civil liberties and privacy of their citizens while ensuring their safety and security?

We have already talked quite a bit about the Arab Spring. We have looked at it from a political dimension and from a military dimension, and many of us have read how communication technologies, social networking, cell phones, etc., played a role in places like Egypt, Tunisia and Libya. But I would like to suggest that those of us who live in countries that we do not consider harsh or "totalitarian" should not be too comfortable either. The same tools that may have enabled or at least accelerated the popular uprisings in the Arab Spring have also brought us Occupy Wall Street, WikiLeaks, and the "hacktivist" group Anonymous.

SIGNPOSTS OF RECENT HISTORY

I am going to suggest what I call "signposts" from recent history and it will be up to us together to see if these are connected in any way.

Anyone who has visited New York, San Francisco or Boston in the past year or so knows that the Occupy movement is real and it is more than just a nuisance—it has not had a lot of press lately, but it was a fairly well-organized, if somewhat inarticulate, uprising of disenfranchised people and it has had a measurable impact on the political dialogue in the U.S., especially in this election year.

Earlier this year, the U.S. State Department disclosed their sponsorship of an interesting operation called "Commotion Wireless." It is an initiative to help develop Mobile Ad-Hoc Networks (MANETS) to enable people living in areas with repressive regimes to communicate, even if the government tries to disrupt communications.

As was alluded to yesterday by Senator Rutelli, two weeks ago, the U.N. Human Rights Council adopted a landmark resolution declaring that all people have a basic human right to freedom of expression on the Internet. Perhaps ironically, the resolution was almost unanimously approved, even by countries that in fact censor their citizens' access to the Internet.

Can we connect the dots between these signposts, or are these events in fact unrelated?

I will wrap up my context setting with two more sound bites from this conference. The first one comes from Admiral Di Paola who, when he opened the conference, said, "The more you are disconnected, the more likely you are to be the source of the next global crisis." The second sound bite comes from Deputy Secretary Lute when she said, "It is not just about preventing bad things, it is about expediting good things."

Chapter 40

The Growing Role of the Social Media in Crisis Situations

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

The great English poet Shelley said of Lord Byron that he had lost the gift of communication but unfortunately not the art of speech and I will hope that, as I am speaking on this topic, I have not completely lost the gift of communication. I am a political scientist, not a techie, and therefore in opening the session on the role of the social media, forgive me if I take a strategic political view, speak more for diplomats and strategists than for technicians, and underline what some of the long-term implications of the exponential increase in the availability, use, and role of the social media might be. And since the current example that we have in the back of our minds is the Arab Spring, I will focus my examples on it but at the end, I will try to draw some more general conclusions which I think are applicable to other uprisings or social unrest crisis situations as well as to Arab governments dealing with more routine situations in normal times.

BRINGING ABOUT CHANGE

First, the social media offer tremendous advantages. If you were a Bolshevik, you used to believe that change could not come from the masses, it had to come through small revolutionary groups, elites, and corps, and Al-Qaeda of course set itself up like a Bolshevik organization to carry out change through violence and the role of an elite group. The social media show us that this model is discredited, not just because Al-Qaeda did not feature very much in the slogans of the Arab Spring, but because the social media allow a mass movement to bring about change; and if change results from a mass movement, even if it does not succeed immediately, the result is more likely to be democratic in the long run than if it comes from a small elite and is imposed from the top down.

Making Revolutions Possible with No Apparent Leaders

Secondly, the social media allow leaderless revolutions. The leaders of these social media in the Arab Spring are not political leaders, they are people who distribute the media, they are distributors of the message; they are the leaders. The political leaders remain hidden if they exist at all. This prevents disputes from arising early on about who is in the lead, or who is taking over, but of course it also means that it is very difficult for oppressive regimes to deal with the mass movements precisely because they do not know whom to arrest. They do not know who the political leaders are.

A Tool for Mobilization and a Voice for Marginalized Groups

Third, the social media are used mainly by the younger generation, the digital natives. For example, in the Arab countries that we are referring to, between 55% and 70% of the population—depending upon the countries—is under the age of 30 and, believe it or not, the use in that part of the world of the Internet, of the social media, is about 32% on average compared globally with 28%. So interestingly, Arab countries have a higher demographic with a higher use of Internet social media than in many European countries, particularly in Central and Eastern Europe, and the user growth has gone up by as much as 1,800% in just a decade from 2002 to 2010.

The role of the social media is to do two things: first, to be an extra tool of mobilization to those who would be active anyway, the urban educated elites who are politically aware, but second and more importantly, to bring together with those elites people who, until that time, had no role in society. For example, 41% of Facebook users in Tunisia are women, 36 % of Facebook users in Egypt are women. Groups that have been marginalized come together with the elites, the countryside

comes together with the cities, and the social media build bridges where socially that was impossible. So social media are an alternative to violent change, develop relationships, share interests, and allow influence to be brought to bear, which is very important in societies where the traditional media are heavily censored or, like in Syria at the moment, foreign media are not allowed in at all. In fact, interestingly most of the Western news agencies and Western television—CNN, BBC, but also Al Jazeera—in these types of situations get most of their footage from the social media, from YouTube. They are dependent on them for their pictures although they cannot always trust the authenticity of those pictures. Quite frankly, I am not a supporter of the Assad regime as you can imagine, but it has come to light that many things on the social media used by the Syrian opposition are fakes coming from Lebanon or from Iraq. So television has to be careful about the authenticity of pictures, particularly of massacres and violent scenes. On the other hand, it works the other way too. The social media allow Western television, which are censored in these countries, to gain a foothold vis-à-vis the population by being able to appear on YouTube or Facebook or other social media.

Information Awareness and Dampening of Violence

However, it is not just the social media that are powerful—I really want to insist on this. The social media are not operated in a vacuum. They are powerful because they combine with traditional media and it is still the case that, in the countries of the Arab Spring, television is more watched and more influential vis-à-vis the totality of the population than social media. Likewise, the mobile telephone is more influential in calling people to protest in Tahrir Square than Twitter or Facebook. The traditional site gets a new lease on life for being allied to the social media. In other words, social media have two functions: an information awareness raising tool but also a planning organizational tool, making journalists out of every citizen and allowing therefore every individual to be not just a better observer but also an actor of what is going on. At the same time, the presence of the social media may act as a dampener of violence. For example, in 1982, the father of the current Assad killed 10,000 people in Hama in just under three weeks. Now, I am not in any way condoning the violence we see in Syria at the moment but the degree at least of the repression has not gone on in quite the same way. Although I cannot answer that question, it is a legitimate one because the regimes that are committing terrible crimes still hold back from great excesses due to the presence of cameras, the inevitability of the crimes coming out, and the inadequacy of censorship.

Organizational Political Role

Next, are the social media important because a demonstration is already going on and they simply show it or do the social media create the demonstration in the first place? The overwhelming evidence that I see, and there has been a lot of good analysis of the social media in the Arab Spring, is that indeed the social media do create the phenomenon and the communication organizational part does come before the demonstrations. So, in that respect, what Raymond Schillinger once said about the social media, i.e., that they are "vapid troughs of celebrity gossip and self aggrandizement," is not wholly the case. The social media clearly have played an organizational political role, but two facts are important: they needed a crisis to begin the campaign there, for example the death of Khaled Saïd in Egypt at the hands of the police or the death of Mohammed Bouazizi in Tunisia. But the social media were not influential simply by bringing people together. They only became influential when there was a kinetic product at the other hand, kinetic on the left, kinetic on the right, with the social media therefore in the middle acting as a force multiplier between individual incidents and then the demonstration. If there is not a physical kinetic impact, the social media remain a conversation and nothing more.

Missing a Viable Platform for Political Action

My next point in this respect is that the social media may start a revolution but they do not finish a revolution. The evidence so far is that those who joined the Twitter/Facebook revolutions did not win the elections, mainly because they were not organized to win those elections, and that was what we saw the social media doing—starting a narrative but a very vague narrative. The narrative was freedom, which is a very powerful and attractive message but that message does not translate into a particular political platform or an ideology or a social agenda around a system of leaders. That is why traditional structures still win elections and indeed they won in the Egyptian election. Ironically, the parties that won never gained an overall majority of the votes but emerged because they were the organized parties. Where is for example Wael Ghonim, the Google manager who was so influential? Where is he now? So the social media are still experiencing problems

in translating a kind of mass phenomenon, a kind of flash mob as it is called in the jargon, into a viable platform of political action.

A second observation that is interesting in the case of Egypt is that, in the beginning of the Egyptian protest movement, we saw a heavy correlation with the use of Facebook, Twitter etc., which are all Western and American products. As the revolution went on, we saw a decreasing link between the local media and Facebook, Twitter, etc., and an increasing use of more Islamist Arabic language web sites, mainly used by the Muslim Brotherhood. So the phenomenon is very international at the beginning but its international influence takes second place to more local content as we go forward.

Is the Social Media Openness an Advantage or a Liability?

Where are we going to go in the future? One of the big debates of course is whether the very openness of the social media will be an advantage or a liability. For example, oppressive governments have had two basic responses: one response is to shut down like Mubarak did with Vodafone in Egypt or try to shut down entirely like Kadhafi did with the internet in Libya last year. There is no evidence that this works. First, the local groups that were aided, for example, in the case of Libya by the United Arab Emirates with the Etisalat telephone network, have been very good at rerouting service. Even the Muslim Brotherhood in Egypt escaped censorship for many years by using services in London when it was a prohibited party. So the ingenuity of these people in terms of rerouting has gone around censorship so far. Second, of course the censorship just gets people even madder and pushes more people onto the streets. Third, the government itself relies upon the Internet for its own vital functions and therefore alienates many of its own supporters by trying to shut down the services using a kill switch. What are governments therefore doing? They use the social media for their counter-propaganda. For example in Syria today, there is something called the Syrian Electronic Army Group. It has its own Facebook page with instructions on how to attack opponents online, at least until Facebook recently shut it down. There are plenty of examples where governments are using social media either to discredit the opposition or to get inside their system using anonymity to spread misinformation or mobilize their own supporters. These methods are probably going to be more successful.

SOCIAL MEDIA TRENDS IN THE FUTURE

Let me say a few words on how I see the long run. First of all, we need to analyze the social media, particularly Twitter, which is very easy to analyze, to gather real time data on what is going on. We do not do this enough. Yet, this is the best public opinion poll imaginable. According to the analyses I have read about Libya, the social media demonstrated that 41% of the Libyans wanted a strong man back in power, not necessarily democracy. This is interesting. In Egypt, data mining of the social media showed overwhelmingly that the majority of Egyptians wanted freedom but wanted more state control of industry, for example less privatization, more civil service jobs etc. So we need to do more analyses because they give us very interesting indications, not just that there is a revolution but where people want the country to go, which may sound counter-intuitive to a rather naïve sort of freedom agenda that we often see.

A second question is whether the social media will only exist in crises as in the case of the fruit seller in a Tunisian town immolating himself, or whether the social media will play a role in normal politics in our societies, in campaigns, groups or new formations that are not particularly linked to a crisis.

As a third question, will the social media ultimately bring people together as they did at least temporarily in the Arab Spring, or will the social media just confirm our view of the world, leading over time to more social fragmentation into self-identifying groups? The social media we know have been very good for an opposition agenda. They are definitely very good for being against something. The example I like is Netflix. This company suddenly upped its prices and people immediately used the social media to organize a massive campaign of "no you don't" and the company lost 800,000 subscriptions and 2/3 of its profits. Well, we know about the role of the social media in stopping something but can they play the same role in formulating a set of new ideas? Will they play a constructive role?

And finally, there is the question of anonymity versus identity. We know that governments can hide their identity in cyber space and anonymity makes it very difficult to verify the quality of the information on the social media. So what is the advantage of keeping anonymity versus trying to make things more transparent for veracity?

I will say one last word concerning diplomacy. Having filters, a number of countries in the world are considered by the Open Net Foundation and Reporters sans Frontieres as Internet enemies. They sometimes get these filters from Western companies and many Internet forums debate the responsibility of companies not to provide oppressive regimes with the type of technology that allows the web to be filtered. There have been cases of subsidiaries of Ericsson in Belarus, or

a French company in Libya doing precisely these sort of deals. But more importantly, should we imitate the U.S. State Department in supplying opposition groups with circumvention technology or should we use diplomacy to make it harder for regimes to clamp down on the freedom of the Internet? Lobbying Iran would probably be of little use but some of the enemies of the internet are countries with which we have very good relations. What is therefore the role of diplomacy in trying to prevail upon them not to censor the Internet or arrest bloggers?

Chapter 41

Impact of the Internet and Social Media on National Security Policy and Regime Change: A View from Renesys

Mr. Jim Cowie
Chief Technology Officer, Renesys

When social media suddenly became important on the streets in Cairo, they provoked reactions almost like an immune response. So that you can better understand why this particular event in Egypt was the start of a transformation in our understanding, I will first give you some background on what my company, Renesys, does. Renesys has the happy challenge of trying to come up with the most complete, detailed and accurate representation of the entire Internet—every interconnected device, everything with an IP address. Where is a device located? How does it reach the Internet? And perhaps more importantly from the cyber security standpoint, how do two IP addresses or sets of IP addresses talk to each other? Where does the traffic go? A lot of us intuitively regard the Internet as something opaque that just gets the job done like a utility. But in fact, it is possible with our data to look at the Internet and make it a little more transparent. To accomplish that, we have relationships and cooperative agreements with over 500 service providers worldwide who are feeding us in real-time their picture of the entire Internet at that moment. We complement this work by measuring from all over the planet more than a million IP addresses on a continuous basis to verify that map and figure out, both at a logical and a physical level, how it all fits together. We want to understand, not only the connectivity, the economics, the relationships and trends, but also the performance and ultimately the security of the Internet.

WHEN EGYPT DISAPPEARED FROM THE GLOBAL INTERNET MAP

In this context, imagine what it was like for me about 18 months ago on a Friday afternoon in New Hampshire when I was looking at my console and suddenly I saw the entire country of Egypt disappear from the map. It is an event that is basically without precedent in our experience. Just imagine these 500 perspectives from all over the planet suddenly realizing that there was no way to reach Egypt's networks. They were simply gone as if somebody had turned a switch or a set of switches off over a period of 10 to 15 minutes. Through active verification, we did find that all the hosts we could have previously talked to in Egypt were simply no longer answering. In fact we had no idea how to even measure them. It was as if the map of the Internet had a huge hole in it. At that time, protests on the streets had been going on for about three or four days, but it was not yet a revolution, and there was not a great recognition worldwide that these protests were a truly significant event. When the Internet was turned off, it became crystal clear to people inside and outside Egypt that the government regarded this as something substantially more serious than we had thought. We learned afterwards that the security services had gone to the Ministry of Communications, told them to go to the specific building in Cairo where all the international connectivity for Egypt meets all the domestic connectivity and once there, to turn off the power. And with that, all of Egypt went dark. You may have wondered what a kill switch is. There are in fact kill switches in certain places and this room was one such location. Four or five days followed during which there was no Internet at all. There was growing concern inside the country that this was really the start of something serious. People walked away from their computers, stopped tweeting and joined the crowds in the streets. Four days later, the Internet was turned back on, but it was too late: a week later, the government was gone.

LESSONS LEARNED FROM EGYPT

There are three lessons that we learned from this, not so much in terms of social media, but in terms of the overall role of telecommunications since text messages and mobile phones were equally important.

The Internet is a mobile access phenomenon. The first lesson is that the Internet has transformed itself over the last few years, particularly in emerging markets, into a mobile access phenomenon. We tend to think of social media as being the educated elite, the middle class in the urban environment tweeting away about their opinions, but, in fact, through the transformation of the Internet to predominantly mobile access, most of the anger was being carried out on mobile phones. This has huge implications because, not only were mobile phones used to spread the word to people on how they should move about inside Cairo, but they were also being used to talk to people in the countryside to tell them to come into Cairo as necessary.

Turning off the Internet is not an optimal response during crises. The second lesson we drew, and evidently other countries and perhaps NATO did as well, is that turning off the Internet is not an optimal activity if you are under siege. In Libya, we waited for the Internet to turn off and saw traffic rates drop to close to zero as reported by Google, and yet the routing stayed intact. By routing, I mean that the country did not leave the Internet. International gateways were still open, the fiber optics were lit, traffic could flow. The government was very carefully restricting access to the Internet domestically but, in order to support critical government services, some degree of Internet connectivity was left standing. As to Syria, I get a text message on my phone every time the Syrian government turns off the Internet briefly for whatever reason. I have only been awakened at night once and it was for about ten minutes. By and large, I think that Syria has learned the lesson that Internet connectivity during crises should not be turned off given the consequences of doing so in Egypt.

The Internet depends on a physical infrastructure. The final lesson we took away from looking at Egypt and the disconnect in our data was that none of us realized the physicality of the Internet. We think of social media as a phenomenon with no home, which roams globally and where communication between people happens instantaneously and which does not respect borders. But it is not that at all. The Internet follows a physical infrastructure that we are all familiar with. Bringing the Internet into a country typically takes the form of a submarine cable that comes up from under the ocean, lands on the beach, and then is connected to the domestic network. If a country does not have a sea coast, it will need to go to its neighbors, exchange fiber with them, and have an agreement with them that they will provide Internet service. If a country has neither friends nor a sea coast, it will be forced to use satellites, which is expensive, difficult and slow. We have mapped out the relationships between countries, showing who provides Internet to whom on earth. Our map shows what the watersheds of connectivity are, the zones of influence. It shows who ultimately gets their Internet connectivity from Turkey, who from Russia, who from the United States. So physically, telecommunications between countries create a set of interconnections among them. They are at the same time like and unlike a pipeline. Like a pipeline, they can be lost in case of war, and nobody wants a shared Internet connection between two countries to be lost. Unlike a pipeline, however, in which the relationship is traditionally asymmetric—one provider, one consumer, or one transit—Internet connectivity cannot be used as a threat in the run-up to a war, because countries traditionally have two or three different "friends" with whom they can exchange Internet traffic and if one of them fails, they will be able to use some ingenuity in rerouting traffic. So a particular relationship with friendly countries is not uniquely important in most situations.

A COUNTER EXAMPLE: AFGHANISTAN

There is a possible counter-example to this when social media do not play a big role in a country, and yet telecommunications could be the underpinning of how the security situation will ultimately evolve there. I am thinking of Afghanistan. We know the challenges that Afghanistan faces and getting connected to the Internet is probably not near the top of its list. Afghanistan has no sea coast and it relies heavily on satellites for its Internet. It also relies on its friends, but since its neighbors are difficult neighbors, traffic predominantly goes through Pakistan. When the Pakistan link went down in recent years, Afghanistan relied on Uzbekistan with transit ultimately through Russia. In Herat and some other places, however, a fiber optic ring around Afghanistan has not really functioned correctly in a long time and connectivity is not available, except via Afghanistan's nearest neighbor, which is Iran. Iran has very helpfully provided interconnectivity to the rest of the Internet through its own connectivity to Western Afghanistan. It is therefore interesting to think about how the security situation in Afghanistan will evolve with the West's exit. Perhaps countries that provide good services like telecommunications will have a disproportionate role in helping determine the ultimate stability there. Minister Di Paola pointed out in his address that the more you are disconnected, the more likely you are to be the source of the next global crisis. I would posit that telecommunications links among nations and telecommunications diversity among the set of nations that a country is connected to are one of the temperature takers that we can look at with our data as a key driver of the evolution of the security of these countries.

Chapter 42

Web 2.0 over Https and "Walled Garden," A Source and a Challenge, an Opportunity and a Risk

Mr. Mauro Collalto
CEO, RESI Group

More than providing opinions and visions, I would like to show "film clips," offering ideas for discussion from the point of view of a technology industry representative about the evolution of the cyber world. Web 2.0 and its main achievement, social networks, have changed the way we communicate, interact, plan our lives, and keep our memories. Moreover, they have introduced new vulnerabilities and cyber threats. But social networks can also be used as a source for cyber intelligence. A new perspective is necessary to understand these platforms as an opportunity to improve homeland security.

A SOURCE AND A CHALLENGE

Web 2.0, 3.0 and X.0 are a source because they offer a large mass of open data, which was unthinkable just a few years ago. But they are also a challenge because data are difficult to obtain for a normal Law Enforcement Agency (LEA); think of Gmail, Facebook, and Twitter using HTTPS encryption. Almost half of the earth's population communicating with each other is using technologies that just a few years ago were reserved only to military organizations.

The most common social media and new applications now usually operate using proprietary protocols or P2P connections. Think of iPhone Apps like Viber or What's Up. This is what we call a "Walled Garden."

And what about "Anonymizers"? You have no way to figure out where I am, you can only try to block me. And most of the time you will not succeed.

Ever heard about "The Underground"? Well, if you want to keep on sleeping peacefully, do not try to understand what it is: Jungle, Far West, Somewhere in Nowhere, Outback, call it as you like, it is virtual but it is real. You can buy anything online, from weapons to top secret documents!

And then, there is the "Cloud," which we can define as the delivery of computers as a service rather than a product—whereby shared resources, software, and information are provided to computers and other devices as a metered service over a network (typically the Internet).

It is interesting to note that most Web 2.0 users have at least 8 to 10 different accounts:

- Several social identities (Facebook, Twitter, LinkedIn, Google, etc.);
- One or more Skype accounts (home and office);
- Multiple email / webmail accounts, both private and business ones (Gmail, Hotmail, etc.);
- Multiple forum and blog identities;
- Mobile accounts (iTunes, Markets, Apps login);
- Online banking account;
- E-commerce identities (eBay, GroupOn, etc.);
- Government services accounts (PEC, Government-to-Citizen services).

In this messy world, there is a lot of information. How can we use it? Who can use it? Who and where are the good and bad guys?

AN OPPORTUNITY AND A RISK

Consider what happened during the Arab Spring: millions of people calling for freedom and democracy, protesting for human rights. This is wonderful! Web 2.0, thanks to https and "walled gardens," has been a great opportunity for anyone who dreamed of a better future for himself, his family, and his country, but it was and still remains a perfect curtain, a smoke screen, for the bad guys. The final result is that, for law enforcement agencies, cyber investigation in all countries is more complicated, if not impossible in many cases.

While it is true that the great Western social media are open to collaborate (Skype, Facebook, etc. have procedures in place to provide information to government agencies), nevertheless a few questions arise:

- How can they verify that the request for information is legitimate? I am not a real person. No one can identify me. I am what I declared to be when I registered my account on a website.
- How can a LEA do a broad-spectrum search if it has not identified the suspected target yet?
- Who has jurisdiction?

We need cooperation among states and a common purpose and vision in terms of security. A cyber investigation can only be successful with international standards and regulations that can guarantee the full support of any communication, content and media provider.

These factors suggest that the technology is often not sufficient to defeat crime and increase security. Even today, it is necessary to use traditional investigation techniques in conjunction with more innovative techniques to achieve concrete results.

The investigation techniques are changing and, in virtual life, the first and only rule is simple but vital: stay up to date. It is necessary to acquire a deep knowledge of today's cyber challenges, to be proactive rather than executor, to learn to work in a structured way to maximize the experience, to develop partnerships and collaborations, to start up a cyber task force, to develop cyber universities and be ready for tomorrow's challenges (e.g. IPv6, LTE, 100Gbps, etc.). The keys to operate in cyberspace are the people, not only the technology.

A CLOSING OBSERVATION: VENDORS, AGENCIES, GOVERNMENT

As a closing observation, I would like to simply note that Homeland Security and cyberspace are part of this larger domain. It is like a "movie" with 3 major actors: vendors, agencies and government. Neither one is strong enough, but an effective cooperation between these actors can be successful, each one playing its own role:

Vendors for technology and expertise:

- Leading independent and trusted vendors/manufacturers
- High-level ICT background
- Open to an "ever changing world"
- Frequent training

Agencies for human intelligence and social engineering:

- Informers, undercover operations
- Analysts
- Discover the habits, weakness, passions, etc.
- Tracking

Government for national regulations:

- Registry of users' ID
- Data Retention
- Standardization and regulation on LI
- International cooperation

Chapter 43

Tensions between Economic Growth and Internet Security—We Need Both!

Ms. Melissa Hathaway
President, Hathaway Global Strategies, Former U.S. Cyber Security Coordinator

As I was reflecting on the fact that this is the 29th International Workshop, I thought that it was fitting that we are in Rome because in 1983, it was the height of the Cold War and Rome was the place where the Soviet Union and the United States would come to negotiate or discuss very difficult issues in areas where international cooperation and strategic dialogue were needed. Twenty-nine years later, we are here again at the center between East and West and we are still discussing various strategic issues. For the Americans in the audience, I want to highlight that in that same year, 1983, Ronald Reagan and Yuri Andropov were Men of the Year in Time Magazine and the most popular movie was a Clint Eastwood movie with the memorable quote, "Go ahead, make my day." So, we are going to try to go ahead and "make your day."

Let me start with the following five sins or big mistakes in strategy:

- First, the failure to recognize that *resources are scarce.*
- Second, *mistaking strategic calls* for strategy.
- Third, the *failure to articulate* your strategic problem.
- Fourth, choosing *unattainable strategic goals.*
- Fifth, *not defining the strategic challenge* within a competition and competitively.

BRIEF HISTORY OF THE INTERNET

As you think about those and consider the different comments that we have heard over the last few days, I am going to walk you through a time background. The very first transmission of the Internet was in 1969 and it was the beginning of computer-to-computer transmission of communications and then it extended in 1972 to Europe. While it was an academic experiment, it was really for the military to survive a nuclear event among and within our countries and to be able to still command and control forces.

Pressing fast-forward, in 1985 there was a strategic decision to actually open the Internet and the top-level domains to allow for e-commerce. So, we moved beyond a dot.mil domain and a dot.edu or education domain and expanded to the dot.com domain. And hence 1985 saw the birth of the dependence of the global economy on the Internet.

In 1988, the Morris worm established the first real problem with the Internet. Those people who lived through that event began to recognize that the Internet was in fact insecure: The Morris worm affected 90% of the world's Internet traffic for a period of days. It resulted in at least two things in the United States. First, it resulted in a military mission of computer network defense: the start up, from an academic standpoint, of the Carnegie-Mellon Computer Emergency Response Team. Second, it also resulted in a new market, which many of us are in today, i.e., the commodity market of selling intrusion detection systems, intrusion prevention systems, firewalls, and the like because now, we have systems dependent on Internet technology that are vulnerable to exploitation as has been demonstrated. The very first firewall and intrusion detection system came out in 1990 through the Digital Equipment Corporation.

As we opened up the Internet through the global economy and we needed to have more and more domain name services and addresses, there needed to be some central management point that would actually articulate that and that was the International Corporation for Assigned Names and Numbers (ICANN) which was created in 1998.

In 2000, the world started to really flourish and growth and productivity were resulting from this information com-

munications technology and the Internet and e-commerce. The United Nations went so far as to say that the millennium goals at the time in 2000 were to adopt and embed information communications technology at a rate and speed that could drive income and employment in our respective countries; improve access to business and information at an increased rate; enable e-learning and education to our citizens and provide more citizen-facing services; and facilitate government.

TENSIONS BETWEEN ECONOMIC AND SECURITY GOALS

The United Nations is measuring us in our advancement and our information societies on multiple things but largely on the embedding of information and communication technologies and Internet services in our respective countries along a number of categories:

- At what price are we delivering our telecommunications services?
- At what bandwidth are we providing that?
- What is the capacity and quality of service and speed of that telecommunications or Internet service?
- What skills is it promoting?
- What content can it deliver and in how many languages?
- And finally, what are the applications to lower end users or people who did not happen to grow up with this particular technology?

So, as we are getting measured for those particular things, the United Nations has not yet decided or started to measure us on our ability to secure that same infrastructure, although it is this same infrastructure that delivers essential services around the world. Yet in 2012, in just a few months, the U.N. International Telecommunications Union will begin to address the security aspects of telecommunications and information services—over-the-top services (OTT), mobility, net neutrality, infrastructure protection, and cybersecurity. It is no small feat that now the United Nations might begin to measure us on our ability to secure the capacity that is driving our productivity and e-commerce.

So there is this tension now in our countries on economic growth versus national security: economic growth that is driving our productivity, efficiency, innovation, and modernization, versus the national security demand of infrastructure protection, intellectual property protection, defense of the homeland, and in some cases, even regime stability. And it should not be an "either-or" but that is really what it is coming down to in many countries. We are seeing the same tensions in the European Digital Agenda versus the NATO Strategic Concept Review and there is sometimes misalignment of the incentives that are driving the requirements within the two.

I will show you additional tensions that can be broken down into a few more areas that I think you will see come out of our strategy or lack thereof. They can be broken down into the tension that drives our growth or the things that we need to assert control over in order to maintain those security requirements. They are breaking down into arguments over transparency versus secrecy for issues and capabilities. Are we going to be open or is it going to be classified? It is breaking down into market levers of laissez-faire—let the businesses heal the nations and the market forces will take care of it—versus the regulations that governments need to, or feel the need to, impose on businesses in order to get the controls and the security over the infrastructure. In other words, it is mercantilism versus capitalism, public responsibility versus private responsibility, and then finally tactical reactive approaches versus strategic and proactive methods.

With that, being in Rome, we still need to have a responsible dialogue and articulate the strategic problems because we have not done so. We need to recognize that we are in a down economy that is getting worse and that resources are scarce. So, it cannot be an "either-or," it has to be both economic growth and national security.

Chapter 44

A Chinese View on Cybersecurity

Mr. JIANG Zhenxi
Senior Research Fellow, China Institute for International Strategic Studies

I am grateful for this opportunity to make remarks on cybersecurity and, on behalf of the China Institute for International Strategic Studies, let me extend my sincere thanks to the hosts of this workshop. Today, I would like to express my view from a Chinese perspective on cybersecurity.

ASSESSMENT OF CYBERSECURITY

The Internet has introduced a profound change in human life. It has become a driving force for the globalization of the world, making our world smaller and closer, making our work more effective and our lives more convenient. It is estimated that there were about 1.8 billion Internet users in the world in 2011. The Internet is playing a vital role for economic development and social progress.

At the same time, the threat to cybersecurity is growing immensely. These threats are very complex and demonstrated in several respects:

- Firstly, due to the vulnerability of cyber networks, it is easy to attract cyber attacks. In recent years, virus attacks by botnets, Trojan horses, and malicious code have broken out on a large scale. Some of the viruses even have "zero-day attack" capabilities, which are especially dangerous.
- Secondly, national secrets and personal information were stolen and disclosed by hackers. In 2010, Mr. Julian Assange, an Australian hacker, with the help of a large number of supporters, grabbed hundreds of thousands of U.S. government documents and publicized them on the Internet.
- Thirdly, the industrial infrastructure has become a physical target for cyber attack. It is reported that an attack on the Iranian nuclear infrastructure with the "Stuxnet" virus was conducted in 2010. It may delay Iranian nuclear programs. If such an attack is launched by states or non-state actors in the future, it will put the national grid and transportation system of the target country at risk.
- Fourthly, it is well known that the Internet is widely used by terrorists for recruiting, training, and organizing terrorist activities in the world. They have engaged in "electronic jihad." This would be a great danger to the world if the terrorists were to initiate cyber conflicts, even launch a cyber war in the future.

CHINA'S CYBERSECURITY EFFORTS

China is a big cyber state, with 513 million Internet users and 7.75 million IP addresses. The Internet plays a very important role for China's national security, economic development, and social progress.

However, China is also facing severe challenges for cybersecurity. According to the report, China Internet Security 2011, there were more than 8.9 million computers in China controlled by IP servers located in other countries. Many computers in China were embedded with malware such as viruses, Trojan horses, or botnets. In May 2009, China suffered a large-scale cyber attack from outside of China. The attack caused many Chinese gateway websites to shut down. Millions of Internet users were met with denial of service. At present, cyber crime, such as financial phishing and fraudulent conduct on the Internet, is a big challenge for China. China has suffered significant losses as a result.

In recent years, the Chinese government has taken active measures to make the Internet secure. They include:

- formulating laws to regulate Internet conduct;
- establishing professional emergency teams to permit rapid responses;

- developing high-tech products to maintain cybersecurity;
- coordinating the work of government, and the private sector for cybersecurity; and
- enhancing international cooperation with foreign countries and international organizations.

SAFEGUARDING CYBERSECURITY

Cybersecurity concerns state security, economic development, and human life. Given that the threat of cybersecurity is growing very fast, the international community must take strong and effective actions. The following principles are highly recommended:

- *Responsibilities of state governments to protect and strengthen cybersecurity.* Governments have the key responsibility to protect cybersecurity as a sovereign state. They must keep the integrity, reliability, availability, and confidentiality of the information in their countries. In spite of the fact that the cyber world has no borders, the state enjoys sovereignty over the Internet. Therefore, the Internet should be properly controlled by the government while the right of the citizens' free communication is ensured.
- *Innovation of high technology to consolidate the defense capabilities against cyber attacks.* Given many kinds of new types of growing, large scale [threats], strong and effective antivirus tools should be developed. To this end, we should build efficient emergency forces to permit rapid responses and develop new products with high technology. We should strengthen shields against cyber attacks, make responses more rapid, more resilient. I am glad to hear that today, IT companies are doing a lot of work in cybersecurity. I hope these efforts will continue in the future.
- *Keeping cyberspace for peace.* Our common task is to keep cyber peace and prevent cyber conflicts. To this end, cyber war must not be launched at any time. Nowadays, the international community should make every effort to safeguard the cybersecurity and make the Internet more secure and more convenient.
- *Enhancing international cooperation.* Cybersecurity is a global issue which needs a global solution. Although the dependence on the Internet by specific countries may vary and their interests and concerns may differ, the international community has a common interest and common responsibilities to safeguard cyber peace.

Given the transnational and pervasive nature of the Internet, no single country in the world can handle it in isolation. Therefore, international support and cooperation are needed. To this end, the major powers of the Internet in the world should take active concrete actions for cooperation. The United Nations and international organizations should take a leading role in formulating an International Convention on Cybersecurity and regulating the conduct of the Internet. The regional organizations and individual states also may play an important role. The international dialogue and professional exchanges are needed in this regard.

Chapter 45

How to Protect our Critical Infrastructures

Dr. Luisa Franchina
Director General, Secretariat for Critical Infrastructures
Presidency of the Italian Council of Ministers

CRITICAL INFRASTRUCTURE AND NATIONAL SECURITY

Legislative Decree 61/2011 has transposed Directive 2008/114/EC on the identification and designation of the European Critical Infrastructures (ECI) and the assessment of the need to improve their protection. The "department in charge" that was mentioned in Decree 61/2011 has been designated by the Italian Prime Minister's Decree of 17 May 2011 as the Critical Infrastructure Secretariat, which is my organization within the Military Advisor's Office of the Presidency of the Council of Ministers.

Why is it important to have a team that works on these kinds of issues? This is because critical infrastructures are naturally related to national security. A national security strategy is one of the most important tools for dealing with security, threats, and risks. In order to carry out this strategy, it is necessary to have laws to lay out responsibilities and the chain of command and control. And why are "responsibilities" and "chain of command and control" essential? First, most of the critical infrastructure is privately owned. Critical infrastructure operators and owners face a wide range of risks and threats. In order to face these natural and anthropic risks and threats, operators and owners need to make investments, and, compliance is still the main key point for investing. The second point is based on history: there have always been security investments after emergency situations such as an offensive attack or an earthquake. For this reason, it is clearly necessary to lay out responsibilities with laws.

NATIONAL AND GLOBAL SECURITY STRATEGIES

If we wish to discuss a national security strategy, we must consider the need for a chain of command and control: defining and understanding "who does what and when" are the core steps needed for success. A good strategy also needs, among other things, harmonization. Globalization and the reality of computers and devices that are "always connected" have led to the appearance of new kinds of threats and risks that are not related to just one point on a map. If you think about such cyber threats as botnets and viruses that rapidly infect computers all over the world, you can easily see that a constant dialogue among NATO members and with the whole Alliance is needed in order to harmonize laws and strategies. And in order to achieve an international vision, it is clear that a truly global approach is required. No country can create a Critical Information Infrastructure Protection (CIIP) strategy in isolation, since there are no national boundaries in cyberspace.

Another important feature is the dialogue with the critical infrastructure security managers. A security manager is the one in charge of developing a strategy that will meet the organization's needs and be approved by its leadership. First, they ask for attention since compliance is the first key point for investing. Second, they ask for standards. In fact, the market *de facto* determines the compliance in every case in order to respond to the given standard.

Moreover, operators are working on a sort of "adaptive" security in order to improve safety and prevention. In today's dynamic threat and networking environments, critical infrastructures need protection against ever-changing attacks and vulnerabilities. They need a security strategy that can adapt in real time to the "unknown" or "unknowable" threats in this dynamic network and threat environment.

THE KEY ROLE OF INFORMATION SHARING

This new model of security comes from cybersecurity. Today, operators are trying to extend this solution to "physical security" as well. Every sort of change—e.g., in mentalities, in habits, and in social attitudes—requires an appropriate adaptive response. Such an approach obviously requires a wide range of expertise and data. In order to compensate for the lack of required expertise, the best solution is cooperation—cooperation between the private and public sectors and among private enterprises. Each entity provides only one piece of the overall puzzle. In fact, this kind of adaptive reaction requires a lot of information sharing and data analysis (e.g., cyber and social network analysis and, of course, Intelligence, which means human interpretation). In this way, an adaptive approach is a preventive reaction to the threat.

Information sharing between the private and public sectors and within the private sector itself is still the key way to build up a successful security strategy. For that reason, the creation of Information Sharing and Analysis Centers (ISAC) is fundamental. Critical infrastructure key resource operators and owners must establish these kinds of trusted entities (i.e., ISACs) in order to provide a comprehensive sector analysis which can be shared within the sector, with other sectors, and with the government. On the European level, the first step has been taken with the creation of the European Network and Information Security Agency (ENISA), whose goal is to face cybersecurity issues in the European Union. ENISA has recently issued a Good Practice Guide on Cooperative Models for Effective Public Private Partnerships. As they point out, this guide is not prescriptive but it focuses on clarity of purpose and approach so that stakeholders can easily choose those aspects that will add value to their endeavors in setting up and running PPPs (i.e., Public Private Partnerships).

As already mentioned, this is just the first step. Other efforts are needed to accomplish the remaining parts and no time must be wasted in doing so.

Chapter 46

Achieving "Shared Situation Awareness" in Cyber Space

Mr. Andrea Rigoni
Director-General, Global Cyber Security Center (GSEC)

I was born in Rome but my family was from the north, and when my grandfather would come to visit—I was 3 or 4 years old—he loved to bring me to the Via Dei Fori Imperiali, which is the large street in front of the Coliseum. Just in the middle of the Via Dei Fori Imperiali and facing the Coliseum, there are several large marble maps of the Roman Empire. The first map shows almost the entire world (although I am sorry for our U.S. friends, since from our perspective at the time, they were not considered as part of world!). You can see Europe and Asia and the Roman Empire is just a dot. The second map shows Italy and Gallia Cisalpina (Cisalpine Gaul), while the last map shows almost the entire known world under the control of the Roman Empire.

CYBER SPACE NEEDS A "SHARED SITUATION AWARENESS"

Obviously, Romans were great conquerors and one of their secrets was the way in which they were managing war, in particular the way their generals were always in full control of the theater. They were on their horses on top of hills that gave them a complete view of the theater. It was one of their secrets to beat their enemies. Now, I am not a defense or military expert but I understand that modern defense doctrine is based on an evolution of this principle—Network-Enabled Capability (NEC), or Network-Centric Warfare (NCW), is exactly based on having as detailed a view as possible of the battlefield. It is called Shared Situation Awareness. I had to learn this because my background is in engineering and a few years ago I joined a U.K. company whose employees were all former military people from Intelligence. Since I felt quite ignorant, they gave me books on NATO and network-centric warfare.

When I read the principles of the doctrine in the book written by Alberts, Garstka, and Stein, I felt that the comparison with the cyber space was strong. What we are missing is that we do not have satellites for the cyber space. If you want to have a shared situation awareness of what is going on, it is technically difficult. The Internet is a set of networks, with most of them under the control of the private sector. Technically, we can just define the Internet for the very low layers of the stack; when we enter into the application field, however, we do not have a standard definition of what the Internet is. Try to ask an engineer how difficult it is it to track a simple access to a web service from your desktop connected to a wi-fi, connected to a network, going through MPLS and then to a U.S. web server, maybe in the Cloud. Every single device that you are going through might record something. If afterwards you want to put together all of these pieces and you know what you are looking for, this is already a very difficult job. Now imagine the difficulty when you do not know what you are looking for. So Shared Situation Awareness is one of the future developments for the protection of cyber space. I personally think that this is the reason why most, if not all, cyber security strategies that have been released in the last 3 to 5 years always contain information sharing and international cooperation as key elements. This was the case in Italy where a five-point proposal for a cyber security strategy cited information sharing and international cooperation as two of its points.

A large number of countries and organizations have tried to start information sharing projects but I suspect that most of these initiatives have not been as successful as could be expected. Both the U.S. government and private sector invested in them but I am not so sure that the members of the private sector in particular can say that they achieved their objective of having a clear view of what is going on. Most of the companies we have been talking to feel like they are like in old war movies where soldiers in the trenches know that the enemy is there, hear the noise of bullets, but do not know what is happening. They simply have to defend themselves as best they can. On the other hand, it is also true that some countries are developing very interesting information sharing models.

EXAMPLES FROM AIR TRAFFIC CONTROL AND THE ELECTRICAL GRID

I believe that when we discuss cyber security, we should look at examples that are not related to cyber security such as air control or the electrical system, because they have been forced to share information. For example, you want to be sure that there are no other airplanes in a plane's flight route and you want to be sure that the connections and frequency of a power grid are fully aligned. These two sectors have developed great models even though, in the case of the electrical system, the electrical operators in Europe did not want to have one single central command or monitoring sensor with full visibility. So, the EU is studying how to foster an information sharing platform for Europe and we are working closely with countries like the U.K., the Netherlands and Sweden, which have a great connection with the private sector and have developed interesting and successful information sharing platforms. The private sector is anxious to share information with the government and it is also developing a way to get information out of governments. It is open to sharing when it sees that the government is providing Intelligence in return.

As you all know, there are problems with classified information. In my center, for example, we are developing models, policies, and procedures just to handle classified information for companies that cannot handle internally a classified document. We need to develop new governance models and we need to develop standards. Our organization works with the EU and with international standard organizations. We got ISO 2710, which is a framework. It gives us some principles that the private sector and governments can use. I mentioned earlier the energy sector, which is obviously a very critical sector. You may not immediately see the connection between cyber space and energy but it is true for the actual systems. We need cyber security there and the impact can be very relevant to our society. This is why in our projects we are addressing the energy sector as one of the most critical sectors.

SUGGESTIONS ON HOW TO WORK WITH THE EUROPEAN UNION

Finally, I would like to underline the importance of having EU member states working together since some issues cannot be addressed by the individual member states without cooperation. I know that dealing with the European Commission and with the European Union is not easy. We need to drive and lead by doing instead of waiting for the European Commission to come up with communications, and then follow with directives or regulations. I have heard that some governments are waiting for the new cyber security strategy coming out in September to give them guidelines for an information sharing project. My advice to them is not to wait, first because they will never find the detailed guidelines there, only the principle; secondly, because the best way to influence the EU is to put something in place as an international model. Let's work together with like-minded countries and then let's share the results with the EU. I am sure that the EU will not ignore the positive results and these results will contribute to making the model even better.

Chapter 47

Standing up NATO's Communications and Information Agency

Mr. Kevin Scheid
Deputy General Manager, NATO Communications and Information Agency (NCI)

REFORMING NATO'S COMMUNICATION AND INFORMATION AGENCIES

To begin, I would like to make a few comments about the NATO Communications and Information Agency (NCI). It is now eighteen days old, and I am one of three interim deputy general managers. The agency is a result of the merger of five NATO entities—the NATO Consultation, Command and Control Agency (NC3A); the NATO Communication and Information Systems Services Agency (NCSA), which was the CIS; the Communication Service Agency; the Ballistic Missile Defense Office; some IT offices at NATO Headquarters; and the Air Command and Control Management Agency (NACMA). All together, it has about 3,800 employees and funding of about a billion euros. Approximately two thirds of this funding goes to industry with which we are partnering to deliver goods, services and capabilities to NATO. The theme of this merger is to improve NATO's efficiency and effectiveness under the Secretary General's direction by combining fourteen agencies down to three. We are also focusing on making reductions over the course of the next eighteen months by seeking savings of about 20 percent out of the NATO agencies during this period.

Reform will be implemented in three phases and will be completed by the end of 2014. We are currently in a consolidation phase and operating in the stovepipes of the agencies that pre-existed. I am running the former NC3A entity for the new general manager and my colleagues, the other deputy general managers, are running their legacy organizations as we continue to merge. Some important steps have been taken. The nations have selected the general manager, Major General Koen Gijsbers from the Netherlands, a Charter has been written and approved by the North Atlantic Council (NAC) and we have established the agency's supervisory board. This new board will oversee the agency as part of the NATO Communications and Information organization.

THE DEFENSE INDUSTRY AS AN INSTRUMENT OF NATIONAL POWER

We are changing the way we are doing business and hope to squeeze out deficiencies, work smarter and engage industry in a more effective way. In the United States where I come out of the Department of Defense, we often talk about all the elements of national power against particular problems—the war in Iraq, the war in Afghanistan, the efforts against global terrorism—via formal government proclamations from large bureaucracies such as the Department of Defense, Department of State, or the Homeland Security agency. But behind these are important industry efforts to support these elements of national power, and I would go so far as to say that a strong industry is one of the elements of national power that is needed behind the defense forces and behind the Homeland Security forces.

We have sought to develop these capabilities in the U.S. and over the past few years I have seen some remarkable transformations that have been driven by 9/11 and by the engagement in Iraq and in Afghanistan. To cite just a few examples, we have had a remarkable engagement with industry on mine-resistant ambush-protected MRAP vehicles. Twenty-two billion dollars were invested in 18 months and over 4,000 vehicles were delivered. The Predator aircraft, which started off as a surveillance aircraft, was swiftly turned into a weaponized aircraft and hundreds of these have been outfitted by industry with technical sensor capabilities and delivered in short periods of time to support the NATO troops in Iraq and Afghanistan.

TWO ACHIEVEMENTS: AFGHANISTAN'S MISSION NETWORK AND NATO'S COMPUTER INCIDENT RESPONSE CAPABILITY

In the NATO context, I will just pick two recent achievements:

- *The Afghanistan Mission Network (AMN).* When General McCrystal showed up in Afghanistan, he had five computers under his desk, one for each of the major Allies in the Alliance. He wanted to have just one computer, in order to fight the war on just one network. A policy decision was required: Technology could support the change, but no one was willing to make that policy decision. He made that call, and, in six months (from January to July 2010), my agency at NATO—with strong support from the NAC and all the elements of NATO Headquarters, put together the Afghan Mission Network. We are now in the later phases of improving AMN.
- *The NATO Computer Incident Response Capability (NCIRC).* NATO's Computer Incident Response Capability was started five years ago, in order to monitor attacks on NATO networks. Since it was not as capable as it needed to be, NATO decided at the Lisbon Summit in 2011 to improve and secure our networks. Without asking us how long it would take, they said to finish it by the end of 2012! So we have been on a quick phase to secure the networks, which means working with and teaming with industry. In fact, I have beside me on this panel the chairman of the board of SELEX ELSAG, the company that won the contract, and to my right, Northrop Grumman, which is the subcontractor to SELEX on this project. Hopefully, they are both going to give me assurances that this will be done by the end of 2012!

Chapter 48

How to Adapt to the New Threats

General S.A. Claudio Debertolis
Italian Secretary General of Defense and National Armaments Director

Delivered by Rear Admiral Francesco Covella

On behalf of the Secretary General of Defense and National Armaments Director, General Claudio Debertolis, I want to extend my warmest greetings to all of you and I would like to thank in particular Dr. Roger Weissinger-Baylon for giving me the opportunity to speak to such a qualified and diverse audience.

FROM TRADITIONAL MILITARY CONFRONTATION TO NEW THREATS REQUIRING A COLLECTIVE RESPONSE

This is a workshop on global security and the title chosen for this panel is "Dealing with Challenges in Afghanistan, Pakistan and Libya–Industry's Response." During the Cold War period, the political polarization between the Eastern and Western Blocs determined a traditional kind of military confrontation, which could be measured in terms of forces incorporated in a hierarchical structure and regular units. It was possible to gather information on these kinds of assets. The counterpart could identify and quantify them. In other words, notwithstanding the bleak prospect of a nuclear conflict, the chances of success were still estimated using criteria that were very similar to those dating back to the Second World War. Our job was still to study a clearly identified enemy.

However, since the fall of the Berlin Wall, new threats have arisen. International terrorism, the proliferation of weapons of mass destruction, and regional crises with economic, ethnic, social and religious roots have required the international community to provide a collective response to stabilize security and peace. Such responses had to be supranational in order to trigger adequate political, diplomatic, economic, and social synergies, and had to rely, where appropriate, on the support of military forces ready for all kinds of missions, including prevention operations, crisis management, military operations, and peacekeeping or peace enforcement operations.

NATO—A COLLECTIVE AND DYNAMIC SECURITY ORGANIZATION

NATO's new Strategic Concept paves the way for a different methodological approach to the organization's main mission: preventing crises by promoting international stability. While in the past NATO was generally just a collective defense system for Europeans, with this new approach it has become something more than that—a collective security organization. Our Armed Forces have progressively transitioned from a static approach to security to a more dynamic posture, and are no longer committed to border defense only but increasingly involved in out-of-area operations. The joint and multinational operations in which our Armed Forces have participated, in the most recent crisis scenarios, have required an extremely high level of integration among Land, Naval, and Air Force units, which has to be achieved well before operational needs arise.

UPDATING FORCES, DOCTRINE, AND CAPABILITIES

Over the years such coalitions and/or alliances had to face asymmetric threats characterized by a high degree of unpredictability. Moreover, since those adversaries could never aspire to military supremacy in the traditional sense, they have

adopted a long-term strategy aimed at wearing down their opponents physically and psychologically. Finally, the players involved in violent actions are so numerous, sometimes so ingenious, and the situations so diverse that we cannot provide an exhaustive description of all threats. The theaters of operations where our Armed Forces are deployed, including Afghanistan and more recently Libya, are good examples of this. Therefore, to counter new challenges rapidly and effectively, it is necessary to constantly update and retrofit our forces, doctrine and capabilities. In this perspective, the Italian Defense Ministry has launched adaptation processes for its operational forces in line with the inspiring principles of the NATO Transformation. Special attention has been paid to the protection of vehicles and personnel as well as to the accuracy of weapon systems in order to achieve the priority goal of reduced collateral damage.

In the field of force protection, I would like to mention as a fitting example the development of multi-role tactical vehicles with great protection and mobility capabilities. These systems may seem to have a simply tactical significance. However, ensuring the protection of our personnel (and of civilians) in a context characterized by asymmetric threats is, first of all, a moral duty for top-ranking military officials as commanders and, secondly, a necessity, in order to guarantee that the country where operations take place maintains the political and social willingness to pursue the goals of the operation itself. With regard to the Italian Armed Forces, I will name just a couple of vehicles: the internationally renowned MLTV "LINCE" and the 8x8 armored combat vehicle "FRECCIA," around which the construction of the future medium digitized forces (NEC force program) revolves.

Regarding firing accuracy, the development and manufacturing of long-range guided munitions has marked a significant step. I am referring, for example, to the guided MLRS (so-called GMLRS) unitary rockets developed by Lockheed Martin. These rockets have a monolithic warhead that respects the ban on cluster munitions. Other programs, which go in the same direction of increasingly improved target discrimination, are also in place. All these systems are highly or extremely highly accurate and fulfill the requirement of minimizing collateral damage risks. They have made possible what seemed out of reach only a few years ago, that is, sniping artillery. In fact, the range of action of these systems extends from a few to a hundred kilometers. They have real all-weather capability, although accuracy varies according to the kind of terminal guidance used.

THE NEED TO DEVELOP MILITARY TECHNOLOGY QUICKLY

However, the new operational scenarios are also posing other challenges. At present, we need to develop new military technology very quickly, following the production of vehicles and weapons systems closely and from the very earliest stages of design.

To achieve this, the defense industry needs to be agile and flexible, always in tune with the Armed Forces' operational requirements, and abreast of modern technologies. This is especially true with respect to net-centric and C3 technologies, since these extremely complex systems are strongly impacted by the latest technological developments in hardware, miniaturization, management software, protection systems, etc. In view of the rapidly evolving threats, the technical administrative area of the Italian MOD is adapting more flexible procurement procedures while still observing our Administration's principles of transparency, functionality, and effectiveness. The National Armaments Directorate has contributed to this process by revising the organization of procurement agencies. In this manner we will be able to speedily meet current operational requirements and procure systems and equipment that can effectively reduce the risks run by our military personnel.

DUAL-PURPOSE TECHNOLOGIES WITH A GLOBAL INFORMATION NETWORK

In addition, the ever-increasing R&D costs related to high-tech weapon systems on one hand, and the contraction of demand on the other, have compelled the industrial base to boost effectiveness and productivity, thus triggering a general process of rationalization. In fact, high costs and limited resources are increasingly pushing research toward dual-purpose technologies and new opportunities are arising from the interaction between the civilian and military sectors, whose production synergies are generating a mutual bandwagon effect. The advantages of these applications are quite obvious: while civilian industry extends the scope of its business, the defense industry optimizes its expenditure, limiting direct investment. There is no shortage of strategic areas of research: robotics; microelectronics; satellite sensors and technology,;unmanned aerial vehicles (UAVS); advanced materials; digital radio communications; nuclear, chemical, bacteriological and radiological detection and decontamination; internal surveillance and security; as well as the most innovative propulsion systems.

All current procurement and refurbishment programs have a remarkable technological content. The ultimate goal is to make our Armed Forces more net-centric. At the core of this transformation is the transition from individual technology

telecommunication platforms to a seamless global network for the collection and distribution of information. Our Armed Forces will have to be capable of sharing information with other governmental, and not just military, forces. Conventional communication backbones will be incorporated in a global network.

The largest Western Armed Forces are developing modernization programs aimed at the digitization of operational units. This will ensure information superiority, allowing the full sharing of information at troop level, while increasing the capability of effective and selective intervention. However, given the necessity of sharing several different projects within the same sphere, this work tends to be extremely complex. The whole range of military technologies is covered, including information technology, force protection, unmanned vehicles, and advanced command and control solutions. Therefore, we have had to develop a new approach characterized by the so-called "evolution through production" principle. Such an approach is also reflected by the contracting architecture, which allows for the continuous in-process improvement of technical solutions and their constant adjustment to operational requirements. Electronic and information technologies that are subject to rapid obsolescence and employed in fast-changing scenarios require flexible forms of procurement. Another feature of the new net-centric modus operandi is exemplified by the so-called spiral approach: a program is split into a number of phases, in order to harvest its early deliverable products and deploy them on the field much more quickly than before.

DEFENSE AND INDUSTRY COOPERATION

Of course, the handling of such huge program commitments demands an even closer and prompter cooperation between defense and industry. The relevant companies should also identify a system integrator in charge of managing and harmonizing several different projects that, although valid on their own, become fully significant only through mutual integration. This concerns, for example, vehicle platforms manufacturers who, more and more, must often act as system integrators as all vehicles have become extremely complex systems incorporating several C2 and communication elements. The basic idea is to develop vehicles that feature multi-role capabilities from the start so that they may perform widely varying tasks during their service life.

Notwithstanding the substantial progress made over the last few years, we will have to continue investing in strategic airlift, long-term logistic support capabilities, information superiority, and the capability of engaging the adversary with accuracy and timeliness, just to mention some of the key areas.

In conclusion, synergies among institutions, the defense ministry and the defense industry, should aim at the full satisfaction of all stakeholders involved but first and foremost our end-users, that is, our troops. They should be able to rely on systems that are constantly adjusted to the evolving threats and fielded according to the required quality and timing standards. This is the precondition for performing missions in the best possible manner.

Chapter 49

Dealing with the Challenges in Afghanistan, Pakistan, And Libya—Industry's Response

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

The campaigns in Afghanistan, Libya, and Pakistan undertaken since 2001 are unique in the history of the Alliance. The Alliance has made a decade-long commitment to expeditionary campaigns to confront a global threat to its members. That threat—a global Islamic extremist movement—is neither an Army nor a State, but it has been able to leverage modern technology developed primarily for the civil sector in ways that could pose an existential threat to the Alliance. The threat posed by this sophisticated extremist movement has undermined many of the advantages the Alliance has accumulated through decades of investment in combined arms mechanized forces.

Indeed, the Cold War paradigm of military power was inverted. During the Cold War, the Alliance forces were "stealthy" while adversaries by and large were not. In the military campaigns in Afghanistan, Libya, and Pakistan, it is the adversary that is "stealthy" while the Alliance is an omnipresent target as the adversary blended into the civil environment.

Accomplishing the military mission set by the governments of the Alliance forced the defense industry to deal with new dimensions of modern warfare. The industry did so by creating new capabilities to support new concepts of operation. Doing so necessitated a hurried transition for the defense sector from its Cold War "industrial" model to a 21st century "information-based" approach that enabled the Alliance to successfully confront the adversary.

SIMILARITIES AND DIFFERENCES IN THE CAMPAIGNS IN AFGHANISTAN, LIBYA, AND PAKISTAN

Apart from sharing an Islamic cultural base, each of the three countries involved in recent or ongoing Alliance campaigns are very different in every respect pertinent to military operations. Afghanistan involved a wide range of military operational, logistics, and intelligence challenges as a result of a well-established local adversary, Afghanistan's landlocked character, its linkage to global Islamic terrorist movements, as well as their complex and clandestine links to supporters in Pakistan.

Moreover, with the collapse of the Taliban regime, Afghanistan became an ungoverned, failed state whose governmental infrastructure had to be rebuilt while simultaneously seeking to protect non-combatants from the Al Qaeda-Taliban insurgency. The military skills called for in Afghanistan bore little resemblance to those that shaped the NATO Alliance for half a century. The need for sophisticated Intelligence, Surveillance, and Reconnaissance (ISR) to detect, locate, and track uniquely identified individuals and groups who were often embedded in Afghanistan's civil society was a dominant feature of the campaign, while organized military formations were not. Prosecuting the campaign against these insurgents had to be accompanied by a capacity to coordinate and communicate with multinational forces while being able to strike targets precisely with minimal if any collateral damage.

In Libya, the political proscription against "boots on the ground" intensified the reliance on the success of the remotely launched and controlled ISR system to support the desired political and military actions. The experience gained over the past decade in Alliance collaboration in Afghanistan and Iraq facilitated the creation of ad hoc arrangements with a number of Allied and friendly states who had never conducted expeditionary operations in the region. Political constraints piled on top of time-sensitive military operations in Libya made ISR and air campaign coordination decisive. In this respect, the demands on the Alliance for adaptation were extraordinary and unprecedented, and could not have been accomplished without the technical capabilities and processes developed in the Cold War-era. The underlying flexibility of modern IT-

based ISR enabled the Alliance to conduct effective air-to-ground operations against both residual Qaddafi military forces and Allied African mercenary units without its own forces on the ground.

Pakistan presented a wholly different circumstance as the threat created by cross-border insurgents from Afghanistan posed a potential threat to both Pakistan's internal stability and Allied forces operating in Afghanistan. Again, the capacity of the ISR system to detect, track, and locate adversary elements as individuals as well as small groups has proven to be decisive in preventing insurgents from creating an insurgent sanctuary in Pakistan and limited the capacity of the insurgents to conduct cross-border military operations.

What then were the most significant industry innovations and how were they applied to facilitate the Allied adaptation to the post-2001 global threat environment in these very different theaters of operation? Here are a few illustrative categories:

Concepts of Operation

The most important advances in military technology enable the creation of new concepts of operation. The military applications of technologies, especially information technologies primarily developed for civil use placed the affected parts of the defense sector on a "Moore's Law" modernization timeline—a sharp contrast from the classic decades-long modernization cycle associated with traditional military equipment. By leveraging and adapting civil sector IT advances, the defense industry enabled the Alliance to adapt to the diverse and ever-changing threat posed by the Islamic extremist movements in the threatened areas. As a consequence of industry innovation, the Alliance was frequently able to anticipate rather than respond to shifts in adversary tactics, and in doing so, was able to maintain the battlefield initiative, and contribute to the creation of an environment where the political and diplomatic aims of the Alliance could be engaged and achieved.

Persistent Day/Night-All-Weather Surveillance

The adversaries in Afghanistan, Libya, and Pakistan could not have been successfully engaged with Cold War-era Intelligence gathering and strike capabilities. The Alliance recognized that it needed to invert the Cold War preoccupation with targeting the adversary's Order of Battle and instead to find the individuals and small groups that were characteristic of clandestine insurgent operations. The industry's capacity to adapt civil sector IT to create and exploit nearly ubiquitous sensing from manned and unmanned platforms allowed the Alliance to move from episodic reconnaissance to persistent surveillance.

Persistent surveillance in turn created the ability to tag, track, and locate individuals, objects, and activities on a 24/7 all-weather basis—capabilities that were indispensable to deal with the nature of the terrorist threat. Persistent surveillance enabled the Alliance to conduct military operations far differently from any previous conflict. Threats to Alliance forces or non-combatants could be continuously tracked, located and targeted with greater precision. The capacity to extract knowledge from truly vast data sets rapidly—frequently in near real-time—enabled tactical commanders to simultaneously exploit the properties of multiple sources of Intelligence—imagery, signals Intelligence, human intelligence, etc.

The widespread civil destruction and the displacement of the civilian population in combat zones characteristic of most past major conflicts was largely absent owing to the greater precision of targeting systems.

Precision Strike

The capacity to precisely tag, track, and locate targets permitted the emergence of a capability to strike targets with great precision independent of range. This capacity facilitated precision strikes on individuals and small groups while avoiding to the extent possible the unintended collateral casualties among non-combatants who often are deliberately commingled with terrorist groups. The ability to strike targets with great precision also substantially reduced the logistics footprint of Alliance forces, diminishing its cost, its tactical defensive requirements, and its vulnerability to enemy attack. Moreover, because of the great precision with which targets could be struck and destroyed, it was possible to use much smaller munitions, cascading advantages of smaller and fewer munitions back onto the logistics infrastructure. The increasing precision of target location provided by a vast sensor base and a secure broadband communications network in turn made it possible to design more effective munitions, including those with tailorable effects to produce the desired military effect with a minimum of unintended or counterproductive collateral damage.

Secure Deployable Broadband Communications And Networks

The mutually reinforcing capabilities of persistent surveillance and precision strikes in turn have been sustained by networks that are secure, while retaining the vast amount of bandwidth needed to exploit the data generated by thousands of unmanned aerial vehicles and other ground- and air-based sensors. The employment of broadband networks—several hundred times the bandwidth used in Operation Desert Shield and Desert Storm only a decade or so earlier—significantly reduced the size of forces required. The forces employed in Operation Iraqi Freedom were one-third the size of their counterpart in 1991. The increased bandwidth enabled deployed forces to be far more effective and productive because they could access theater-wide knowledge of the adversary on a near real-time basis for optimum distribution of forces. However, these networks could never have been effectively employed without a cyber and communications security environment that denied our IT-savvy adversaries access to these networks, even as the Alliance was able to exploit the adversary's networks. The ability to rapidly deploy broadband communications networks facilitated the swift Alliance response to a fast-breaking event in Libya by allowing the sharing of information about the situation on the ground derived almost entirely from airborne sensors. While there is still more to do in this sphere, the Libyan experience was encouraging as we understand better the military applications of modern IT.

Training Superiority

The transition from large conscription-based forces to smaller professional forces enabled the industry to leverage civil sector investment in IT-based training by means of a modern infrastructure for complex and highly demanding training and rehearsals for military operations. A quickly shared, detailed understanding of the adversary's tactics permitted the Alliance to design adaptive and responsive training, making personnel far more effective on the battlefield. Training experience in the exploitation of the available sensor base to support advanced tactics enabled units rotated into the theater to operate at a high level of operational effectiveness at the outset. This development was in stark contrast with historical experience where the most dangerous job in the armed forces was to be a "replacement" arriving on the scene of an ongoing battle. Combined operations were built on shared access to advanced ISR capabilities, enabling the diplomatic aims of the Alliance to reflect the shared military burden.

Deployable Logistics

The Alliance has evolved from its Cold War focus on territorial defense supported by a centralized logistics system to one able to support expeditionary deployments. Building on the IT-driven logistics best-practices of the civil sector, industry was able to use modern logistics concepts such as "just-in-time"—rather than the logistical "mountains" created by the traditional military "just-in-case." The introduction of expeditionary capabilities with deployable logistics has established the basis for the Alliance to provide "out-of-area" military support for the political and diplomatic aims of the transatlantic Alliance for the 21st century.

Chapter 50

How Can Industry Best Contribute to Cybersecurity?

General Nazzareno Cardinali
Chairman of the Board, SELEX ELSAG

The cyber domain is changing day by day, with the rapid development of information and communications technologies and with the mobility of devices. Now, we are talking about the "Internet of things"—and we have more than nine billion devices already connected, while more than 25 billion are predicted by 2020. Therefore, I think that cyberspace is moving fast; we have to follow, and we have to be ready to modify our ways of approaching security.

Integration. Cybersecurity should be integrated in all of the architectures that we are now working on. In Italy, we are also addressing this problem of cybersecurity and, for instance, in the aeronautical field we have to see how we are going to defend ourselves in the future Single European Sky (SES) where all of the air traffic will be controlled, which will mean a very wide and a very high level of data traffic. Since we also have remotely controlled UAVs, we have to be sure that their security is assured.

Stakeholders. When we talk about this scenario we have to consider the stakeholders. As you may imagine, I will not list all the stakeholders, but I will say that these stakeholders are important—not just the governments, but the private stakeholders as well. As to the critical infrastructures in the European nations, 83% of them are run by private organizations and, of course, their problem is how to invest in order to make sure that, at the end of the day, they get good value for money as well as profits for their shareholders. To do so, they must ensure the right levels of security that will contribute to the operability of the infrastructures and the quality of life of the citizens whom these infrastructures are serving. Accordingly, any risk analysis performed on these infrastructures must take into account not only the economic impact of a service disruption, but also the impact on global welfare that can be much larger since it involves all of the citizens and the institutions.

NATO contract. As to the organizations with which we are more involved, such as NATO and the EU, I believe that they have been discussed enough by the previous speakers and therefore I will not deal with them in detail. Nonetheless, in his introduction to my presentation, Kevin Scheid mentioned our cyber contract with NATO. As you know, we are supposed to provide a full operational capability for 55 sites in 28 countries over a period of one year, in other words by the end of 2012. This will protect over 22,000 people involved in NATO operations. We are working on that; it is a very challenging job, and we are putting all of our efforts into reaching our objectives within the time that has been given to us. At this point, I will say that we will have to overcome some necessary organizational arrangements and, therefore, we are still aiming for the end of 2012—it might even be at the beginning of 2013—when we are able to provide full operability of the systems.

Cooperation. The last subject that I would like to address is cooperation. We see that we have to cooperate to make sure that the information one actor has acquired becomes a common asset for all of the actors in the area. As an air force man, I feel that the cooperation in cyber should be like the cooperation we have for flight safety. Any incident that happens to one aircraft should be known by everybody to make sure that the right measures are taken to overcome the related threats. Cooperation has many advantages, but, because we are dealing with security, some people may be cautious in sharing their information as a common asset. So a change of mindset is necessary in order to make sure that we can get all the benefits of cooperation among governments and private entities.

POSSIBLE MODELS FOR INTERACTIONS

At the national level, we must recognize that cooperation among all the stakeholders is the key enabler for establishing a common cybersecurity and defense situational awareness scenario. This approach should not only lead to methodologies and tools for monitoring and control but also to a true strategic support able to predict risk scenarios and to enable effective countermeasures. The awareness of the global security level of the country permits more effective prevention and manage-

ment of global risks. In order to accomplish this, threat intelligence and sharing among these stakeholders is crucial. And a lot of thought has gone into possible models for interactions between communities of interest.

As a case in point, Finmeccanica and SELEX ELSAG are working with the U.K. government and with British companies on the mechanics of a hub—a node model—to enable better protection of the national key infrastructure as well as the U.K.'s economic environment. The nodes are intended as joined-up industry clusters of trusted participants, which will include government departments that often share similar attack vectors. The hub is a joint government specialist node that takes feeds from the clusters and, after sanitization, disseminates as appropriate to the broader community. We are part of the defense industry cluster that will finance the other cluster as one of the first to be set up and where confidential Intelligence sharing has already commenced. This is a good step.

Consistent with this preliminary experience to permit dialogue among institutions, large enterprises, small and medium companies, and academic institutions, we propose to promote a cybersecurity ecosystem that operates through a partnership between all actors involved. In this ecosystem, an industrial center of excellence for defense and security is clearly a candidate to assume a role of *primus inter pares* within the private sector and as a trusted interface among government entities and the private market. This partnership should improve knowledge transfer, training, and information integration in order to assure the ultimate goal of contributing in a significant way to the protection of the national economy.

At SELEX ELSAG of Finmeccanica, we are supporting and promoting this viewpoint whenever we have the opportunity—at the institutional, academic, and public levels. So we are glad to have the opportunity to do so at this important workshop, with such a distinguished audience and speakers. We are also glad to reaffirm that Finmeccanica is a major player in the security and defense arena, with its cyber sector excellence and both the ambition and the capability of performing this role in its domestic market.

Chapter 51

Industry's Response to Challenges to Security

Mr. Marco Morucci
Rome Lab Leader, IBM

IBM'S CONTINUOUS INVESTMENT IN SECURITY

I would like to start with an overall perspective on my company, IBM. IBM invests $6 billion every year on new technology and products. These investments are triggered by an annual study called the "Global Technology Outlook." Already back in 2006-2007, the study was predicting that security would become a major focus area—especially for global security, threats arising from wireless connections, the increase in connectivity, and the Internet of things. Based on these considerations, IBM has put a big chunk of its $6 billion investment into security technology, which means not only making its products more secure but also creating a completely new organization focused on security. Our company is building a large number of security operation centers around the world in order to help customers improve their security systems. So, we have a continuous investment in security, and the next step is to move from security to what we call "intelligent security," which is a combination of business intelligence, business analytics, and the more traditional security technology.

LOOKING AT SECURITY FROM A BUSINESS PERSPECTIVE

In this respect, I am glad that Harriet Goldman of MITRE mentioned the need to defend our businesses while recognizing that we cannot keep attackers out of our systems. We need to find ways to look at security more from a business perspective using technology to help identify those threats in advance. Since I am responsible for our Rome Lab, let me say a few words about our organization. We are part of the IBM development and research family, which includes 36 development centers and 8 research centers around the world. I am proud to be leading the one based here in Italy. Why is it important for local institutions in Italy or other enterprises? First of all, we have in-house competencies in security that range from virtualization to the Cloud, to business analytics, etc. We not only have those capabilities in-house in Rome, but we are also interlocked with the security operation centers that I mentioned earlier and with all the other IBM development research centers. Thus, we are a strong asset in our country since we are able to help any kind of new business or project, either through our in-house competencies or by engaging other colleagues around the world.

Just to give you some numbers, we have 600 engineers in Rome who are very focused on innovation and we submit approximately 1,000 patents per year with the support of 200 inventors and 11 master inventors. We cooperate with important institutions in Italy and around the world, including research institutes and universities, to provide strong support to enterprises and public institutions. In Italy, we have worked with key integrators like SELEX and with the Ministry of Defense. For example, we have built a fairly complex test bed to analyze calls from the field with speech recognition and we have also collaborated on other projects related to ATMs. We are therefore an important part of the system that is contributing to these key security projects, even though you might not think of a large laboratory in Italy when you think of IBM Labs.

This workshop has been a great opportunity to discuss our capabilities and, especially, to let Italian business and government agencies know that IBM has these resources right here in Rome, which are ready to address their needs.

Chapter 52

"Smart Defense": A Rational Approach to Reconciling NATO Security Imperatives with Dwindling Resources

Mr. J. David Patterson
Executive Director, National Defense Business Institute, University of Tennessee
With Research Assistance by Daniel Whitaker III

OVERVIEW

Crisis drives rational thinking more often than deliberation and long study. It was simply a matter of time before the deteriorating economic conditions in Europe and the United States drove the NATO to reconcile its need to preserve a credible security capability in the context of the current critical pressures on member nations' defense budgets. This paper takes a critical look at NATO's Smart Defense initiative as an answer to making NATO more efficient and consistent with what must be considered the most worrisome economic condition Europe has faced since the founding of NATO.

SMART DEFENSE: A RATIONAL RESPONSE

Almost every economy in the developed world—and groups of economies such as the Eurozone—have been destabilized or critically weakened in the economic crises that have developed since about 2007. Both the political and business worlds within their economies have imposed on Europe and the United States the necessity of finding means to provide for the NATO members' common security more efficiently—read: less costly.

To that end, NATO embarked on what is hoped to be a tour de force to bring the organization's spending in line with fiscal realities. NATO Secretary General Anders Fogh Rasmussen revealed the initiative, called Smart Defense, as the organization's strategic way forward at the 47th Munich Security Conference in January of last year.

Linking the financial stress NATO members face with the security jeopardy that could result, Rasmussen explained, "I want to highlight the importance of what I call Smart Defense—how NATO can help nations to build greater security with fewer resources but more coordination and coherence, so that together we can avoid the financial crisis becoming a security crisis."

Rethinking the Alliance's structure and strategy in Smart Defense terms is the most rational response to the current economic circumstances facing NATO nations. It is not an exaggeration to say that this effort is not just financial prudence but is crucial if the Alliance is to survive as an organization capable of collective security for its members. This paper will first describe what the economic situation and other stresses on NATO are and secondly discuss how Smart Defense can help mitigate those pressures.

ECONOMIC CHALLENGES FACING NATO

In its publication "Strategic Comments," the International Institute for Strategic Studies (IISS) wrote that not only are the European members of NATO suffering economic pressure, but the United States faces some very hard national security choices as well. The Pentagon faces a mandatory reduction in defense spending of $487 billion over the next 10 years.

Though U.S. defense expenditures have risen since 2001 (and were relatively flat for the decade prior), for NATO's European members, defense reductions are continuing a long-established trend. In the period between 2006 and 2010, defense spending in real dollars declined an average of 7.4% from $296 billion to $275 billion. And, in the 2010 to 2011

period, European spending on defense was reduced by an additional 2.8%. Adding to NATO's financial dilemma is the fact that in the past year, twenty of the NATO partners have reduced their level of spending on defense.

There may not have been a time in NATO's history when the economic challenges facing the organization have been as dire as they are today. Though often it is the European Union (EU) that gets the headlines with its collective financial worries, when it comes to economic conditions, there is little separation between NATO's European members and the European Union.

In Europe there does not seem to be any momentum to reverse what can only be called complacency toward defense and common security issues. As Jos Boonstra, a senior researcher at the European think tank, FRIDE, has noted, there is clearly no sense of urgency on the part of the European public to address evolving potential threats to EU security. This lack of interest in security results from the fact that there are no new military missions on the horizon for Europe. It is the view of many Americans that the EU has relied too much on U.S. defense spending and has not kept up its part of the NATO defense agreement.

For many reasons—not the least of which is that the EU lacks a central financial authority to impose fiscal responsibility and to establish governance over banks and other key institutions—there is no unanimity among the European countries to assist those with ailing economies. Despite the momentary relief of the recent deal concluded in Brussels to persuade Germany to help with concessions for Italy and Spain, long-term solutions are still in doubt. A July 2, 2012 Reuters article, "Finland to Block European Stability Mechanism Secondary Market Bond Buying," explains that since there was not the unanimous approval bond purchasing to fund a permanent bailout fund, it "is unlikely to happen." The Netherlands did not sign up to the bond deal either.

A NEW WORLD OF AUSTERITY

Looking to the U.S. is not the ready option that it once was. The appetite for propping up NATO while the U.S. is facing significant financial pressure on its Defense Department is significantly lower than in previous years.

The U.S. Department of Defense is facing a reduction in funding that will certainly be on the order of $458 billion over the next ten years and could be as high as $1 trillion in reduced budget in the event of the "sequestration" that may occur in January 2013. Dealing with the prospect of having less spending capability will drive the U.S. to re-think how it prioritizes its national security spending. The current willingness to fund NATO is clearly evident by the reduction of 5% from the estimated 2013 U.S. contribution, lower than the contribution in 2010. With the focus of the U.S national security strategy turning with greater emphasis on the Pacific theater of U.S. operations, the reduced financial support to NATO by the U.S. may become a trend.

With regard to this last point, some would suggest that because the U.S. and Canada are bordered by the Pacific Ocean, NATO too has an opportunity to focus on the Pacific area of potential operations. As valid a geographical point as this might be, the suggestion that NATO is a Pacific power will probably not be persuasive when it comes to increasing the U.S. financial support to NATO or in NATO's ability to invest and project power in that theater. What is at issue for both European members of NATO and the U.S. is that there is not the money available now—or foreseeably in the near future—to continue to be a credible force for the defense of its members. What is needed is a new approach to achieving NATO member mutual security in a new world of austerity.

EXTERNAL PRESSURES ON NATO

The pressures on NATO to evolve are not only created by increasing financial austerity, but also by a variety of external pressures. NATO—and by inference European collective security—must deal with member political pressure, industrial capability and how it is preserved, economic pressure and true existential threats. Each of these factors—and this list is by no means exhaustive—comes with a variety of elements—and they must be addressed in order to achieve an acceptable level of collective security for the NATO members. Smart Defense must address these pressures as well.

Recently, the Center for Strategic and International Studies held a conference on NATO's Smart Defense initiative with Mr. Gerald Howarth, Minister for International Security Strategy for the U.K. Ministry of Defense, as the principal speaker. Though Mr. Howarth focused on U.S. and U.K. defense industry sharing issues, his larger point was a good explanation of Smart Defense. Howarth talked about the initiative in terms of two key principles:

- Deeper collaboration between Allies is a sine qua non, i.e., joining with other nations in shared tasks and addressing shared burdens, and
- Deeper, more sophisticated partnerships with industry.

The ultimate outcome is to be a more streamlined, efficient approach to weapons and services procurement. Howarth's comments support Secretary General Rasmussen's comments at the Chicago NATO Summit held on May 20, which stated that:

> Smart Defense is a vital principle. We have agreed to make it the new way NATO does business, and we are putting it into practice. Today, we approved a robust package of more than 20 multinational projects, to provide the capabilities we need, at a price we can afford.

Linking achieving greater efficiencies in acquisition programs to the economic challenges gives much greater energy to implementing Smart Defense. Efficiencies can be as complex as integrating the C-17 cargo aircraft into NATO as an airlift operations asset, or as straightforward as having commonality in systems.

Implementing Smart Defense efficiencies includes the idea that countries will specialize in specific warfighting and NATO management capabilities. This specialization is intended to increase productivity and to create mutual dependency among the NATO members. However, as Joshua Foust, a fellow at the American Security Project, has pointed out: "This poses a critical question for future NATO operations: once countries specialize so much that they depend on one another to carry out a military campaign, what happens to NATO's military effectiveness if its political leaders start disagreeing?" There are certainly times when NATO members have disagreed on participation in military operations. A good example is during the recent Iraq campaign Operation Iraqi Freedom. France did not participate, but did contribute forces in Afghanistan.

Too much specialization could easily leave NATO without a crucial capability if, for political or economic reasons, a member with that capability should elect not to participate. In this case productivity would not make up for the loss of vital capability. But, as some would suggest, there are complementary approaches that will help mitigate the cost issues and provide greater opportunities for efficiencies.

Erik Brattberg, visiting fellow at the Center for Transatlantic Relations at the Johns Hopkins University's School of Advanced International Studies, has pointed out that "improved cooperation with non-member states could spur others to follow suit, while encouraging members to commit greater resources to the Alliance." One very good example of where NATO countries participated along with non-member states with NATO command and control is the military operation in Libya.

CONCLUSION

Smart Defense, despite some downsides, is an answer to the need for greater efficiencies and cost savings for NATO and Europe to continue to participate in collective security. There is nothing to suggest that the economic woes of both Europe and the United States are going to abate any time soon, and demands placed on NATO to respond to global contingencies continue as well. To that end, the conferees at the Chicago Summit in May embraced Smart Defense and in doing so made a significant step toward creating a more cost-effective organization with a rational approach to common security goals.

Chapter 53

Introduction of the Honorable Franco Frattini

Ambassador Stefano Stefanini
Diplomatic Advisor to the President of Italy

After having trained myself with the introduction of my friend, Minister of Defense Admiral Giampaolo Di Paola, our Chairman, Dr. Roger Weissinger-Baylon, thought I could face a new challenge by introducing to all of you the Honorable Franco Frattini.

This is a meaningful task for me since Franco Frattini was my boss as Minister of Foreign Affairs for many years, but it is a straightforward one as well given that he is a widely known and recognized personality that really needs little presentation worldwide. As Vice President of the European Commission from 2004 to 2008, he handled highly sensitive and strategic policy issues involving justice, freedom, and security. The key issue of migration has been touched upon during this seminar; Minister Frattini deserves strong credit as one of the few European politicians who had the vision to consider it a matter to be tackled in the EU framework and with EU instruments, such as through the upgrade of the Frontex agency.

He was one of the real engines of the Barroso Commission and his tenure was characterized by farsightedness and innovation, advocating a more liberal and forward-looking European migration policy in times when populism and xenophobia were rising across the continent. No less significantly, Franco Frattini also called for a "European Islam" that would promote tolerance and integration, in line with the European values of freedom and democracy.

Serving twice as Minister of Foreign Affairs from 2002 to 2004 and again from 2008 to 2011, he has been a strong advocate of the coherent and generous participation of Italy in all NATO, EU, and U.N. international peace and security operations. As part of this commitment, he has restlessly explained to the Italian public and to Italian and European political forces that our common security is indivisible and that we cannot close our eyes when threats to common security originate from theatres that lie outside of the Euro-Atlantic area.

I served as the Permanent Representative of Italy at NATO during a large part of the second tenure of Franco Frattini as Foreign Minister and can thus testify as to the strength of his personal belief in the Euro-Atlantic pillar of our diplomacy. This led him to become a vocal supporter of NATO-Russia relations, trying to fully exploit the tools established at the Pratica di Mare Summit, as well as of a stronger and fruitful NATO-EU cooperation. Franco Frattini is undoubtedly a man with a vision and with the curiosity to understand and possibly anticipate new challenges and new threats, including in terms of cyber and energy security.

He has been among the first to understand the historic magnitude and scope of the Arab awakenings. That is why he bravely understood that NATO could not avoid playing a role in the Libyan crisis. If the Libyans finally got rid of a bloody dictator, Minister Frattini is among the first row of those who deserve their gratitude.

Chapter 54

The Evolution of Security Challenges and the Role of the Transatlantic Community

The Honorable Franco Frattini
Member of Parliament; Former Foreign Minister of Italy

In today's increasingly interconnected world, security challenges have become more transnational and are no longer contained within national boundaries. This is mainly due to two major historical developments that occurred over the past two decades: One is a new and broader concept of security that emerged in the post Cold War security environment and includes new components in addition to the purely military ones. The other, which is globalization, is characterized by an increased interdependence of the world economy but also by a real revolution in the way in which people come together, through global ways of doing business and trade, new ways of working on a global scale and new ways of communicating instantly across the world. Thomas Friedman wrote eloquently about the positive global impact of "world flatteners" in which knowledge and resources connect globally, and Alfred Thayer Mahan about the strategic significance of the "global commons": sea, air, space, and cyberspace.

But a more interdependent world can also be a more fragile one. One billion people, including about 340 million of the world's extremely poor, are estimated to live in states that are very fragile. The interconnection of fragile states and globalization also points out the link between economics, governance, and security. Increasingly, post Cold War conflicts occur within states and largely within fragile states. The tensions deriving from these security challenges have led to crises that the members of our transatlantic community have been forced to address far from our borders, going to the crisis before the crisis came to our doorsteps.

With the end of the Cold War, we have seen Europe, the United States, and Canada come together through NATO to organize the international management of the crises in Bosnia, Kosovo, Afghanistan, and Libya in order to protect civilians. We have also seen a new and broader concept of security emerge, one that is no longer characterized by the defense of our countries' borders from clear and predictable security threats but marked instead by multifaceted and multidimensional security challenges and threats that are more difficult to predict. This broader approach to security recognizes the importance of political, economic, social, and environmental factors, in addition to the indispensable defense dimension. The consequence is therefore that international security and stability depend on political, economic, social, and environmental elements, alongside military aspects.

We are all affected by the scourge of international terrorism; the proliferation of weapons of mass destruction and their delivery means, accompanied by the erosion of the nuclear non-proliferation regime; failing and failed states; the protection of sea lanes of communication and energy supply routes; cybersecurity; and environmental challenges. The global character of these factors is evident. But while we have made good progress in intensifying our efforts to fight terrorism and to promote international cooperation on environmental issues, I have the feeling that much more needs to be done when we look at the new security challenges, such as energy security and cyber security.

THE NEED FOR ENERGY SECURITY

The increasing globalization of the oil market has increased the pace of exploration and production, thereby highlighting the need for energy security. Substantial new oil reserves are being exploited worldwide but much of the new production will continue to be in the Middle East, whose overall contribution to the world energy supply is actually likely to grow during the next 20 years. At present, about 70% of proven oil reserves are in the Middle East. With new exploration, this percentage will likely increase and so will the overall contribution of Middle Eastern supply to world trade.

The Middle East region accounts for about 30% of the 82.1 million barrels a day of oil produced across the globe. The Gulf region in particular is the most important oil transit channel in the world, with about 15.5 million barrels per day, about a third of all seaborne oil. This region also exports about 18% of the world's Liquefied Natural Gas (LNG) production, with Qatar being the world leader in LNG exports. Current estimates are that, by the end of 2012, Qatar will produce 77 million tons of LNG annually. About three-quarters of the oil produced in this region is sent to Japan, India, South Korea, and China. The rest goes to Europe and North America creating a common interest of producers and of consumers in securing the shipping lanes.

Russia and the Middle East together will continue to account for roughly three-quarters of world gas reserves. Oil reserves in the Caspian Sea, North Africa and Latin America and their exploitation, while diversifying energy production, will not reduce the global importance of the Gulf in the next 20 years. According to many analysts, new trends following the next two decades could bring a major rise in energy demand in China and India that could be met through imports from the Gulf region and less from Russia and the Caspian.

Access to oil in adequate amounts and at reasonable prices will remain the key variable in the energy security equation over the next decades but it will also be accompanied by increasing attention to the supply and transport of natural gas. Think for example of the pipeline going through Tunisia and Sicily that allows Algerian and Libyan gas to reach the rest of Europe. Gas consumption is indeed growing fast in Western Europe and in Asia. It is therefore no surprise that, for countries in these continents, gas figures very prominently as well in their energy security concerns.

When looking at the gas trade, we also need to consider that, because LNG cooled to -162 degrees Celsius is shipped via high technology and specially designed vessels, security at LNG terminals and at sea is a crucial factor for both producers and consumers. Since half of the world's oil and the majority of the LNG are shipped by sea, even a brief blockage of oil and gas supplies could cause high price increases likely to threaten global economic growth.

Transport routes for oil and gas in and around the Middle East and from the Maghreb to the Caspian Sea, will be an important new factor in the strategic environment. More and more energy security in the region will be crucial for the security of transport and transit countries, as well as for the security and stability of producing ones. Therefore ensuring the free flow and security of critical energy supplies against attack and disruption must be one of the new security priorities of the transatlantic community.

THE NEW CHALLENGE OF CYBER SECURITY

Allow me now to look at another transnational and more global new security challenge that requires our attention because it has a direct impact on our daily safety and security. Starting with Kosovo in 1999, when the NATO website and Allied websites came under cyber attack during the Allied Force NATO operation, up to the attacks against Estonia in 2007, cyber security has revealed the importance of securing the digital infrastructure that our economies and our military security depend on.

The communications and information technology revolution has made the world the "Global Village" that Herbert McLuhan had predicted through our daily interaction in cyberspace by the use of iPhones, BlackBerries, laptops and tablets. From our cellular communications to hospitals, from schools to airports, from classified military and security infrastructures to the World Wide Web, security in cyberspace is crucial to our public safety and to our national security alike. There is therefore a growing need to prepare our societies for cyber emergencies and for our states to develop strategies capable of successfully managing cyber crises that will require both technical and political responses and coordination across states as well.

We will need to develop our ability to absorb new concepts in our strategic thinking such as "cyber resilience," which will involve making our digital infrastructure more resistant to penetration and disruption. And we will need to develop new capabilities to defend against sophisticated cyber threats and deal quickly with cyber emergencies by developing research capabilities that will allow us to stay ahead of the evolving cyber threats. But as members of a transatlantic security Alliance, we will also need to define minimum requirements for the cyber defense of the national networks that are critical to the performance of NATO's core security tasks of collective defense and crisis management. Cyber defense could even give a totally different meaning to Article 4 and Article 5 of the Washington Treaty.

THE ROLE OF THE TRANSATLANTIC COMMUNITY

Managing the diversity of security challenges and threats facing the transatlantic community requires a broad approach to security. This is reflected in three mutually reinforcing elements of our Allied security policy: dialogue, cooperation, and the maintenance of an effective collective defense capability. Keeping an effective and efficient collective defense capability at a time of financially constrained budgets must be achieved by, whenever possible, increasing "multi-nationality" to facilitate the acquisition of high-end capabilities, avoiding national duplications and creating economies of scale. This would maximize practical ways to provide security while minimizing costs to all member countries of NATO.

In this new political and strategic international environment, the success of a policy aimed at preserving peace and preventing war depends even more than in the past on an effective preventive diplomacy and on the successful management of crises affecting our security. No country alone can address these new, more complex and global security challenges and threats. Their successful management requires a multinational and cooperative approach to security.

This is indeed the approach that the transatlantic community has developed since the end of the Cold War when we decided to undertake the transformation of NATO. We began at the Rome Summit in November 1991 when the Heads of State and Government of the Alliance decided to revise and make public for the first time NATO's new Strategic Concept. Since then, the Strategic Concept of the Alliance has been revised twice, in Washington in April 1999 and in Lisbon in November 2010. These three strategic documents give us a detailed view of the major transformation NATO has undergone since the end of the Cold War in order to adapt, in a very flexible way, to the fast-changing security environment. I do believe that this has been a most successful transformation on a political, diplomatic, and military level.

Transformation for a security organization such as NATO is a continuous process. It never ends. In order to accomplish its core security tasks NATO must continue to transform, refining periodically its security concept, and making sure that its civilian and military structures are flexible enough to adapt to the evolution of a fast changing and unpredictable international security environment.

NATO embodies the transatlantic link by which the security of the United States and Canada is permanently tied to the security of Europe. As Hillary Clinton recently said: "Europe is and remains America's partner of first resort." At the Lisbon Summit in November 2010, together with the core tasks of collective defense and crisis management, NATO's Heads of State and Government stressed the importance of "cooperative security." NATO's cooperative approach to security has indeed enabled us to develop political consultations and practical cooperation with partner countries of the most diverse backgrounds and security cultures.

NATO is not and does not aspire to be "the global cop." It is not NATO that has become a global organization but rather, security challenges have become global in character. Consequently, in order to be an effective security provider for its members, NATO must be able to deal with the security challenges that affect the security of its members wherever they come from. But in order to be an effective security provider, NATO must continue to improve its ability to work together with other security partners. From the seven Mediterranean Dialogue countries to the Gulf countries in the Istanbul Cooperation Initiative, to the Structured Cooperation Framework with Iraq, to more global partners such as Japan, New Zealand, and South Korea, NATO's security partnerships have not only made it possible to build a better mutual understanding but also to contribute to the successful management of security crises.

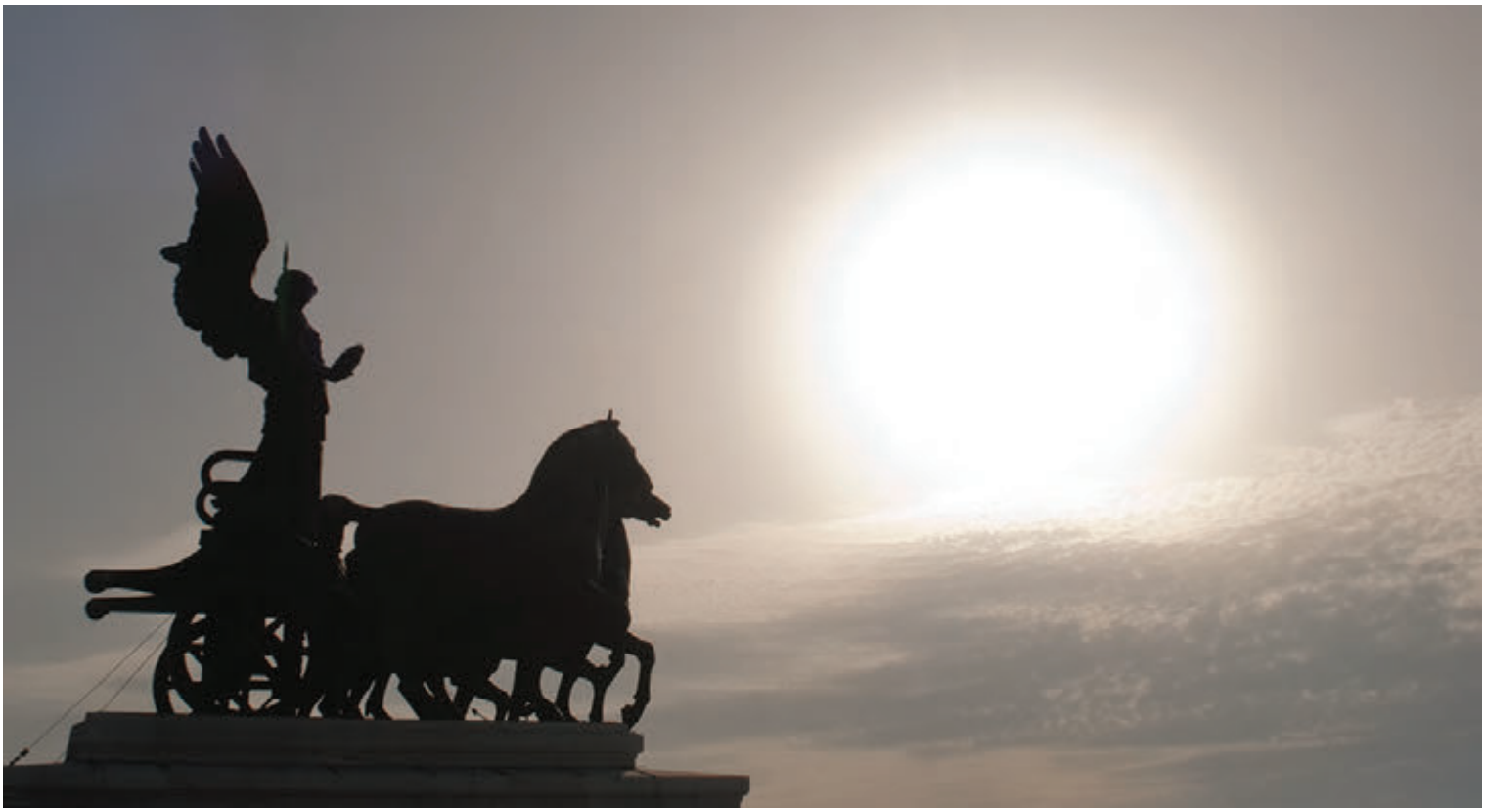
Thirty-seven NATO and partner countries helped the people of Bosnia build better lives, 30 NATO and partner countries are doing the same in Kosovo, and 50 NATO and partner countries are currently helping Afghanistan to assume full responsibility for its own security by 2014, without help from outside. All these operations have been and are conducted on the ground, under U.N. mandate. In Libya, most recently, we have seen NATO countries help protect the Libyan people together with five partner nations, four of which are Arab partner countries that are members of the Mediterranean Dialogue and of the Istanbul Cooperation Initiative. As promised in the Strategic Concept, these operational partners were given a structural role in shaping the strategy and decisions of the operations in which they participated during the NATO-led operations in Afghanistan and Libya.

NATO has also been able to develop a comprehensive approach during the management of its operations, involving other international actorss such as the United Nations, the European Union and the OSCE and working in a complementary fashion with all of them in order to avoid duplications. It has also reached out to new ones that have become increasingly more active internationally, such as the Gulf Cooperation Council and the League of Arab States, as we have seen during the Libyan crisis.

I am convinced therefore that our transatlantic community will be able to deal more effectively with today's global security challenges, if it is able to develop political consultations and practical cooperation with a wide network of partnership

countries and international organizations around the world. This must be indeed our vision for the future. No country can successfully address alone the global security challenges of today's complex world. By building a new culture of cooperation in the security sphere on a multilateral level, NATO and its partner countries will be able to work together more effectively in order to promote better conditions of international security, stability, and peace.

international workshop series on global security



PRESENTED BY

Center for Strategic Decision Research | Centro Innovazione Difesa | Centro Militare di Studi Strategici

PRINCIPAL SPONSORS

Presidency of the Italian Republic | Italian Ministry of Defense | United States Department of Defense
Cisco | McAfee · Intel | Finmeccanica

MAJOR SPONSORS

AFCEA | ELT/Elettronica | MITRE | IBM | Northrup Grumman | Renesys | Resi Group | URS
The University of Tennessee (NDBI) | SELEX Elsag | SELEX Sistemi Integrati

---

CENTER FOR STRATEGIC DECISION RESEARCH & STRATEGIC DECISIONS PRESS
2456 Sharon Oaks Drive | Menlo Park, California 94025 USA | www.csdr.org