#CyberIWGS

34th International Workshop on Global Security

Workshop Agenda

Theme	Global Security in the Age of Hacking and Information Warfare: Is Democracy at Stake?
Workshop Chairman & Founder	Dr. Roger Weissinger-Baylon *Co-Director, Center for Strategic Decision Research*
Honorary Chairman	Lieutenant General Bernard de Courrèges d'Ustou *Director, Institut des hautes études de défense nationale*
Presented by	Center for Strategic Decision Research (CSDR)
and	Institut des hautes études de defense nationale (IHEDN), within the French Prime Minister's organization
Principal Sponsors	French Ministry of the Armed Forces
	North Atlantic Treaty Organization - Public Diplomacy
	United States Department of Defense - Office of the Director of Net Assessment
	Cisco Systems
Major Sponsors	Fujitsu · McAfee · Area SpA · CISQ · MITRE
Associate Sponsors	AXA · NATO Communications and Information Agency (NCI)

Acknowledgements to Past Patrons, Honorary General Chairmen, Host Governments, and Keynote Speakers

Patrons

His Excellency Jean-Yves Le Drian, *Minister of Defense of France (2013-2016)*
His Excellency Giorgio Napolitano, *President of the Italian Republic (2012)*
His Excellency Gérard Longuet, *Minister of Defense of France (2011)*
State Secretary Rüdiger Wolf, *Ministry of Defense of Germany (2010)*
His Excellency Vecdi Gönül, *Minister of Defense of Turkey (2009)*
His Excellency Ignazio La Russa, *Minister of Defense of Italy (2008)*
His Excellency Hervé Morin, *Minister of Defense of France (2007)*
His Excellency Franz Josef Jung, MdB, *Minister of Defense of Germany (2006)*
Her Excellency Michèle Alliot-Marie, *Minister of Defense of France (2005, 2007)*
His Excellency Aleksander Kwasniewski, *President of Poland (1996-1998, 2000, 2002)*
His Excellency Václav Havel, *President of the Czech Republic (1996, 1997)*
His Excellency Peter Struck, MdB, *Minister of Defense of Germany (2004)*
His Excellency Rudolf Scharping, *Minister of Defense of Germany (2000, 2002)*
His Excellency Dr. Werner Fasslabend, *Minister of Defense of Austria (1998)*

Honorary General Chairmen

Lieutenant General Bernard de Courrèges d'Ustou, *Director, Institut des hautes études de défense nationale (2015-2017)*
General Biagio Abrate, *Chief of the Italian General Staff (2012)*
General George Joulwan, *Supreme Allied Commander Europe (1994-1997)*
General John Shalikashvili, *Supreme Allied Commander Europe (1993)*

Host Governments

Czech Republic *(1997)*
Kingdom of Denmark *(1989, 2001)*
Federal Government of Germany *(1995, 2000, 2002, 2004, 2006, 2010)*
Republic of Hungary *(1993, 1999)*
Italian Republic *(2012)*
Kingdom of the Netherlands (*1988)*
Kingdom of Norway *(1994)*
Republic of Greece *(1992)*
Republic of Poland *(1996)*
Republic of Portugal *(1991)*
Ministry of Defense of Austria *(1998)*
Ministry of Defense of France *(2005, 2007, 2011, 2013-2017)*
Ministry of Defense of Italy *(2008)*
Ministry of Defense of Turkey *(2009)*
Canadian Armed Forces
Russian Federation's Ministry of Industry, Science and Technology *(2003)*

Selected Keynote Speakers

General Patrick de Rousiers, *Chairman of the E.U. Military Committee (2014)*
Ambassador Alexander Vershbow, *Deputy Secretary General of NATO (2013)*
His Excellency Admiral Giampaolo Di Paola, *Minister of Defense of Italy (2008, 2012)*
The Honorable Jane Holl Lute, *U.S. Deputy Secretary of Homeland Security (2012)*
The Honorable William Lynn III, *U.S. Deputy Secretary of Defense (2011)*
General James Jones, *Supreme Allied Commander Europe (2004, 2006, 2007)*
General Henri Bentégeat, *Chairman of the EU Military Committee (2007)*

WORKSHOP PATRON

Her Excellency Florence Parly
Minister of Defense of France

MONDAY, 18 DECEMBER 2017

9:30 A.M. **WELCOME COFFEE AND REGISTRATION**

All workshop events are being held at the Hôtel national des Invalides (Invalides national monument).

The workshop sessions will be held in the Grand Salon.

The Invalides—one of France's great national monuments—was founded by King Louis XIV, known as the "Sun King." It was built in 1679 by Libéral Bruant and Jules Hardouin-Mansart, one of the principal architects of Versailles. The Invalides also houses the tomb of Napoleon Bonaparte.

The Grand Salon is the former Council Chamber of King Louis XIV.

10:00 A.M. **WELCOMING REMARKS**

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

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

Ingénieur général Jean-Christophe Cardamone
Deputy Director, Institut des hautes études de défense nationale (IHEDN)

10:20 A.M. **INVITED ADDRESS**

Mr. Mounir Mahjoubi
Secretary of State for Digital Affairs

10:50 A.M. **INVITED ADDRESS**

Ambassador Tacan Ildem
NATO Assistant Secretary General for Public Diplomacy

"NATO in the Current Security Environment"

11:10 A.M. **INVITED ADDRESS: THE RAMIFICATIONS OF WAR IN CYBERSPACE**

Général Olivier Bonnet de Paillerets
Cybercommander, French Ministry of the Armed Forces

"The Ramifications of War in Cyberspace"

The notion of war in cyberspace raises more questions than answers. Is cyberspace really a theater of military confrontation? Actually, cyberspace is more an area of conflict that imposes on states, governments, and the armed forces the need to think outside of the box.

11:30 A.M. **PANEL: A NEW CYBER COLD WAR? WHY INTERNATIONAL COOPERATION IS VITAL**

The U.K.'s National Cyber Security Centre has warned that a category 1 cyberattack (the highest level) will be coming in the "not distant future", while former U.S. Presidential candidate Hillary Clinton has stated that we are at the beginning of a new cyber Cold War that is being waged against the West. Russian hackers and agents have used Facebook and Twitter to hack the U.S. presidential election and magnify social divisions. In fact, some experts, intelligence agencies, and Members of Parliament believe that Russia was involved in the Brexit referendum. Russia is also believed to have supported the movement for Catalan independence in Spain. Governments need to work together to develop and establish norms to prevent escalation so that a cyber Cold War does not become hot.

Ambassador David Martinon
Ambassador for Digital Affairs, French Ministry of Europe and Foreign Affairs

Mr. Conrad Prince
U.K. Cyber Security Ambassador, Defence and Security Organisation

"The U.K. National Cyber Security Strategy—One Year On"

It has been just over a year since the launch of the UK Government's second National Cyber Security Strategy and the standing up of the National Cyber Security Centre (NCSC). That year has seen an ever-increasing tempo of cyber attacks on the U.K. A number of lessons can be learned from the first year of implementing the new strategy and from the NCSC's initial year of operations. Amongst them is the need for close collaboration between government and industry to help nations achieve the levels of cyber security they need.

Mr. Karsten Geier
Head, Cyber Policy Coordination Staff, German Federal Foreign Office

"How Governments Can Help Protect Countries from Hacking and Cyber Influence Operations"

12:20 P.M. **END OF SESSION**

12:30 P.M. **LUNCH**

All lunches will be held in the Salons du Quesnoy (Quesnoy Salons).

2:00 P.M. **PANEL: THE IMPORTANCE OF MULTI-STAKEHOLDER COOPERATION FOR CYBER SECURITY AND DEFENSE**

Chair: Ambassador Sorin Ducaru
Senior Fellow, Hudson Institute;
Former NATO Assistant Secretary General for Emerging Security Challenges

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

Ms. Paula Walsh
Head of Cyber Policy, National Security Directorate, U.K. Foreign and Commonwealth Office

"Delivering Cyberspace Rules of the Road: From Theory to Practice"

Agreeing the rules of the road for cyberspace is not easy. We have made progress, particularly through the UN Group of Governmental Experts (GGE), recognizing the applicability of existing international law and agreeing voluntary norms. We now need to demonstrate how this works in practice. We need to build co-operation through regional and multi-stakeholder fora to help build common understanding of the threats and start implementing solutions. We need to deliver a step change in capacity building—to increase

our overall collective security. We need to make sure confidence building measures that support greater transparency and trust between states are implemented. And we need to be able to better deter and mitigate threats, raising the cost of malicious cyber activity—as well as to de-escalate if necessary.

Ms. Merle Maigre
Director, NATO Cooperative Cyber Defence Centre of Excellence

Ten years ago, Estonia's digital infrastructure was hit by waves of denial of service cyber attacks during a period of heightened tension with Russia. This incident, the first of its kind, set off a still-ongoing debate in NATO on the role of cyber operations; it also raised questions about international law and the changing nature of conflict in the internet age. What have we learned from this conflict at the national and international levels? How can NATO develop better strategies to deter attackers, build up the cyber capabilities of allies and contribute to stability in cyberspace?

Mr. Xavier Carton
Deputy Director of Information Systems, RTE (Réseau de Transport d'Electricité)

Perspectives on the cyber threat as seen by a critical infrastructure operator, the French national high tension electrical network. Discussion of the risks for the company and the country, as well as the need to cooperate with governments and internationally.

3:00 P.M. **PANEL: WINNING THE BATTLE OF IDEAS—IN THE FACE OF A SPREADING JIHADIST THREAT, WILL OUR WESTERN DEMOCRACIES HAVE THE COURAGE TO RESPOND?**

The fight against Jihadism is now a battle of ideas. As it continues to spread, it will assume new forms, possibly including cyber terrorism. At its heart are the Salafist and Wahhabist brands of Islam coming from Qatar or Saudi Arabia. In fact, Saudi religious views are so extreme that the regime has been called a "Daesh that made it." Yet, instead of blocking these Gulf monarchies from spreading Jihadism, nations compete for their arms trade and investments. Is the Saudi Crown Prince's call for a return to moderate Islam credible? Will Western democracies have the imagination, creativity and, above all, the courage to find better responses to the Jihadist threat?

The Lord Harris of Haringey
House of Lords, United Kingdom

"The Use of Social Media to Spread Extreme Ideology"

Ambassador Mehmet Fatih Ceylan
Permanent Representative of Turkey to NATO

"Post-Daesh in Iraq and Syria: How to Manage the Aftershock"

Through our collective efforts, the physical presence of Daesh in Iraq and Syria has come to an end. Yet, the threat is far from over. Treating the aftermath is now all the more important. The international community should first focus on ensuring genuine political transition in Syria and political re-calibration in Iraq to avoid the re-emergence of Daesh or terrorist organizations akin to it. In this quest, territorial integrity, sovereignty and political unity of those two countries must be preserved and strengthened. There should be no room for alternate terrorist organizations, loose actors, free-riders and regional power ambitions. Not least, Daesh's ability to inspire and incite followers to commit acts of terror is not fully diminished. The cyber domain for Daesh is still conducive to spreading its propaganda or to claiming responsibility for its attacks. Strategic overview of Syria and Iraq with particular attention to what should be our next steps, including dealing with possible cyber terrorism and the role that NATO might play.

General of the Army (Gendarmerie) Marc Watin-Augouard
Founder of the Forum International de la Cyber Security (FIC);
Former Inspector General of the Armies (Gendarmerie)

4:00 P.M. **COFFEE BREAK**

4:30 P.M. **PANEL: RUSSIAN CYBER INFLUENCE OPERATIONS IN THE U.S. AND IN EUROPE: HOW SHOULD WE RESPOND?**

With its hacking and cyber influence operations, Russia has influenced the U.S. presidential elections while stirring deep divisions among citizens. This weakens the U.S. directly and the NATO alliance indirectly, but Russia may not have benefitted from its efforts since the U.S. Congress has imposed increased sanctions. A senior Republican Senator has warned that the U.S. President is reckless, while some military leaders fear that his actions could lead to nuclear war with North Korea. Of greater concern is the U.S. withdrawal from the 2015 Iran nuclear deal. Therefore, the existing relationship with Russia is not beneficial to any of the parties and a new approach is needed.

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

The fact that we speak about the need for a new relationship with Russia shows the constant deterioration of relations with that country after 2012. The illegal annexation of Crimea in 2014 and the subsequent military destabilization of Eastern Ukraine—both opposed by the West—have played a crucial role; Russia has lost the confidence of the West.
The subsequent interference in the US Presidential elections, in the French Presidential elections and in the attempted separation of Catalonia from Spain—all flatly denied by Russia—have only increased that mistrust. The mistrust has been fed substantially by a brinkmanship policy in the air and on the seas inaugurated by Russia some years ago now, questioning whether one does not need new accords to prevent air and sea incidents, to replace the ones dating from the Cold War Era (although, if those were not respected, what guarantee is there that new ones will be?). Unequivocally, Russia is a major actor on the international scene, making its cooperation a desirable ingredient for the solution of so many problems we are all confronted with today (Syria, for one).

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

In just over a year, Russian-led hacking and cyber influence operations, including fake news, have emerged as a serious threat to our democracies—and to our security. Of course, the challenge of dealing with fake news is more difficult when the U.S. President is one of the principal sources. His barrages of tweets combined with other false or misleading statements reach millions of his followers. Since the legitimacy of the most prestigious newspapers and other media is being simultaneously attacked, the very notion of truth and the distinction between accurate and misleading information is being rapidly eroded.

Ambassador Jiří Šedivý
Permanent Representative of the Czech Republic to NATO;
Former Minister of Defense of the Czech Republic

"Russia's Policy: Continuation of War by Other Means"

Moscow's revisionism is challenging the very principles of the post-Cold War European security architecture, such as the commitment to refrain from the threat or use of force as well as respect for the sovereignty and territorial integrity of all states and their inherent right to choose their institutional future to ensure their security and prosperity.

Russia's strategic goal is to re-define those principles and introduce its own rules of the game: a new version of the Soviet doctrine of limited sovereignty combined with traditional Realpolitik, i.e. creating spheres of influence and building buffer zones between the country and the West. To achieve that, Russia seeks to divide and weaken: undermining Western unity, splitting our alliances (NATO and the EU) and destabilising the legitimacy of liberal democracy in our countries.

Moscow's hybrid tactics and indirect approach reflect the opportunism of a weaker (but completely ruthless) actor. Yet this also confirms that the military deterrence and defense of NATO and the political resolve of the EU work. Operating in the cyber domain is one of the prominent and, perhaps, the most feared instruments in Moscow's information war arsenal. Its effectiveness has been only limited so far. And, above all, success or failure of the Russian tactics is above all a function of our own weaknesses and vulnerabilities. As a rule, Russia does not create new frictions; it exploits existing ones. A large part of the damage resulting from Russia's efforts is therefore self-inflicted.

6:00 P.M. **END OF SESSION**

6:15 P.M. **CHAMPAGNE TASTING AND RECEPTION**

The evening event will be held in the Salle Turenne (Turenne Hall).

The Salle Turenne is the former dining hall of the veterans of King Louis XIV who were lodged in the Invalides. The walls are decorated with 17th century frescoes that depict the King's military campaigns.

7:30 P.M. **DINNER**

Music by the Clarinet Quartet of the Garde Republicaine (Republican Guard).

The Garde Republicaine provides a guard of honor for the highest authorities of the state, protecting the residences of the President and Prime Minister as well as the Senate and National Assembly. Its highly reputed orchestra is present for official state ceremonies and visits.

9:30 P.M. **END OF DINNER**

TUESDAY 19 DECEMBER 2017

8:40 A.M. **WELCOME COFFEE**

9:00 A.M. **INVITED ADDRESS: SECURITY, TRUST, DATA PROTECTION, AND PRIVACY**

Mr. Anthony Grieco
Chief Trust Strategy Officer, Cisco

"The Path to Cyber Resilience"

As the world digitizes to expand economic growth, job creation and global competitiveness, cyber attackers are also seeing the monetary and political opportunity to exploit this digital expansion. The path to enabling a trusted digital nation begins with securing critical infrastructure. It starts with solutions that are designed, developed, manufactured, sold, and serviced with security, trust, data protection and privacy from the start. Seeking productive, agile partners who can help mitigate these risks is essential for every enterprise and government entity alike. In addition to a secure infrastructure, effective cybersecurity strategies combine people, processes, technology and policy to mitigate risk and ensure resiliency. This session will discuss the importance of building security into the foundation of infrastructure and how the private and public sectors can work together in order to increase our collective resilience.

9:30 A.M. **PANEL: HOW TO DEAL WITH SECURITY THREATS ARISING FROM SOCIAL MEDIA—ROBOTROLLING, SPREADING FAKE NEWS, AND MICROTARGETING WITH BIG DATA**

Chair: Ms. Caroline Baylon
Information Security Research Lead, AXA;
Senior Advisor, Center for Strategic Decision Research

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

"The Impact of Hybrid Warfare on NATO's Strategic Communications and What It Means for the Credibility and Effectiveness of NATO's Future Defense Posture"

Mr. Jānis Sārts
Director, NATO Strategic Communications (StratCom) Center of Excellence

"Can Digital Technologies Kill Democracy?"

Robotrolling in social media, methodologies for the spreading of fake news online and the use of big data for microtargeting in political contexts.

Dr. Linton Wells II
Advisor, Georgia Tech Research Institute;
Former U.S. Assistant Secretary of Defense (Acting) and Chief Information Officer

"Prepared for Battle, But Not Prepared for War"

The velocity and scope of information flows today, including social media and the 24 x 7 news cycle, allow adversaries to target directly the will of populations and the resilience of society overall. This is expected to be an important topic in the new US National Security Strategy that will reportedly be released during the workshop. The center of gravity in many future conflicts may shift from military forces to the minds and mobile devices of the citizens of the engaged countries. In this environment, what is the right balance between traditional weapon systems and information capabilities? How do we prepare for the conflicts we're likely to face, versus the battles we think we know how to fight?

10:20 A.M. **COFFEE BREAK**

10:50 A.M. **PANEL: IS THERE A BETTER WAY TO PROTECT AGAINST HACKING AND CYBER ATTACKS?**

Massive hacks, data leaks, and cyber influence operations are becoming larger and more frequent, while technologies ranging from the internet of things (IoT) to self-driving and autonomous vehicles will be adding significantly to the vulnerabilites. The dangers are no longer "merely" criminal, because even our most cherished democratic institutions are now threatened, and the emergence of cyber terrorism in the future is inevitable. What are the approaches that will work the best?

Mr. Bret Hartman
Vice President and Chief Technology Officer, Cisco

"Journey to the Cloud: Staying Calm Amidst the Turbulence"

Security in the cloud is deeply complex as enterprises move towards digitization and an increasing number of businesses commit to a hybrid multi-cloud approach. Exploring both sides of the cloud security debate—the benefits and the risks—we outline a path forward as organizations, and the industry at large, consider a cyber security future where the cloud enables more efficacy and less uncertainty than we experience today.

Mr. Emmanuel Germain
Deputy Director General, ANSSI (French National Information Systems Agency)

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

"Understanding the Threats and Vulnerabilities: Data, Data, Data"

Is there a better way to protect against hacking and cyber attacks? There is no single answer that covers everything, nor a silver bullet that can solve all our problems at once. The key lies in careful assessment. We need to analyze the different areas individually, in order to identify and assess the various challenges they pose. Existing and future threats make up the ever-evolving threat landscape and put immense pressure on users and operators. The large available attack surface and tools for exploiting it make comprehensive protection of our valuable data difficult. Cyber security will remain a major challenge for security professionals and users alike. Among the key issues are data as a target, the sheer amount of data, and the cloud, as more and more data is created by smart devices, the IoT and autonomous vehicles, disinformation campaigns, and cyber terrorism.

Mr. Paul Camille Bentz
Director of Government and Industry Programs, Consortium for IT Software Quality (CISQ)

"Measuring and Reducing the Cyber Risks in Application Software"

While security against cyber and other threats is a major concern, many application development teams assume that the infrastructure and operations team will prevent intruders. This can be disastrous because perimeter monitoring is insufficient as hackers and crackers have started to focus their attention on an organization's most critical asset—its data, leaving many vulnerabilities undetected and allowing applications to be attacked. The CISQ approach is to certify tools that implement its standards. US government agencies are requesting CISQ measures in their procurement policies.

11:50 A.M. **INVITED REMARKS: DEALING WITH JIHADISM**

Ambassador Luis de Almeida Sampaio
Permanent Representative of Portugal to NATO

12:10 P.M. **END OF SESSION**

12:20 P.M. **LUNCH**

Lunch in the Salons du Quesnoy.

1:50 P.M. **INVITED ADDRESS: THE CYBER THREAT TO NUCLEAR INFRASTRUCTURE AND TO THE COMMAND AND CONTROL OF NUCLEAR WEAPON SYSTEMS**

The Rt Hon. the Lord Browne of Ladyton
House of Lords, United Kingdom;
Former Secretary of State for Defence

"Cyber Threats to Nuclear Infrastructure and the Command and Control of Strategic Weapons Systems"

Cyber-based threats target all sectors of society. At the same time, because of the development of a complex techno-military environment, where cyber threats and a growing reliance on computers are transforming the business of national security, governments must worry about cyberattacks with dire consequences. Unlike attacks on corporate or financial systems, a successful cyberattack on a nuclear weapon system could have the gravest consequences. Thankfully, to date, there have been no catastrophic cyberattacks on nuclear weapons systems, but historical accidents indicate what could happen. As openly advised in a seminal 2013 Report of the U.S. DoD, Defense Science Board, we should assume that our nuclear weapons systems could be, or already are, compromised and that, no matter how much we invest, technical cybersecurity measures will never again provide 100% confidence in their security.

Cyber capabilities have increased the means by which terrorists or other actors could acquire physical access to nuclear weapons or materials, with a view to causing detonation. Since hackers successfully penetrated the U.S. National Security Agency's most secret programmes, some of the best protected computer security systems in the world, this concern is no longer hypothetical. States, on the other hand, who deploy cyber against a nuclear adversary are likely to seek to prevent, not precipitate use. The threat that military, critical infrastructure and nuclear systems might be targeted or are already laced with malware will worsen mistrust, instability and fear. Whether strategic stability in such circumstances?

The obvious but challenging solution is to develop a clear understanding among the key players not to interfere with the nuclear command and control systems of their adversaries and to work together to protect all nuclear weapons systems from non-state actors. What are the chances of that?

2:20 P.M. **PANEL: CYBERWARFARE AS THE FOURTH DOMAIN OF WARFARE**

Ambassador Michael Zilmer-Johns
Permanent Representative of Denmark to NATO

"Implications of NATO's Decision That Cyber is the Fourth Domain of Warfare"

At the Warsaw Summit, NATO decided that cyber is the fourth domain of warfare, on the same level as land, air and sea. What does this imply for the Alliance, its member states and its partners? How far has NATO come in adapting to this new reality?

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

In the case of battle decisions involving conflicts that are short of war, it is necessary to understand and plan in advance for the full spectrum of threats that would potentially constitute an Article 5 situation and oblige NATO to respond. Such threats might range

from (a) the testing of NATO information and communication networks that occurs daily to (b) the appearance of Russian Bear bombers to test the borders of a NATO country and which would necessarily trigger a response by F-16s to (c) the penetration into NATO territories of "little green men," namely soldiers without insignia on their uniforms. In such cases, protocols for response need to be carefully determined in advance since battle decisions may need to be taken before the NATO Council has time to meet or give its approval.

Major General Tatsuhiro Tanaka (Ret.)
Research Principal, National Security Laboratory, Fujitsu System Integration Laboratories, Ltd.

"Speeding Up International Cooperation in Warfare's Cyber Domain"

Most of the world is aware of the potentially catastrophic effects to nations and large population centers from destructive cyber attacks. Although such attacks have rarely occurred, the capability of unleashing broader effects exists whether conducted in isolation or as part of broader asymmetric warfare strategies. This leads us to consider three areas of cyber warfare (gray areas, public-private responsibilities, and international cooperation in cyber warfare) that remain unresolved; this has impeded needed actions to bring cyber warfare within accepted international norms and the legal frameworks of war.

3:10 P.M. **COFFEE BREAK**

3:40 P.M. **PANEL: DATA PROTECTION—THE KEY TO CYBER SECURITY?**

Chair: Mr. Phil Stupak
Director of Cyber Security and Information Systems, Clark Street Associates

Ms. Flora Garcia
Data Privacy Officer, McAfee

"The General Data Protection Regulation (GDPR): Through a Cyber-Lens"

Ms. Patricia Murphy
Vice President, Southern Europe, McAfee

The GDPR has already changed how companies and organizations talk about personal data, how it is collected and used, where it is stored, and when it is deleted. But the GDPR says little directly about cybersecurity (Recital 49), which relies upon the collection of data. McAfee's interpretation of GDPR included reflecting on the Directive and the laws that came before it and has resulted in a review of products and processes relating to data and in developing risk-based questions around data use. Looking at the GDPR through a cyber lens raises questions around online identifiers, data residency, workforce monitoring, communications between processors and controllers, and the importance of making sure regulators understand the basics—and importance—of information security technologies.

Mr. Daniel Bagge
Director, Cyber Security Policies, Czech National Cyber and Information Security Agency

"The Importance of Strategic Decision Making for Cyber Security"

A seemingly insignificant cyber security incident can escalate to become a significant national security threat within hours. However, decision makers are not usually equipped with the background information to make an informed decision. Therefore, the way to cripple a government/institution is to manipulate the decision making processes with time pressures, false information, and interfering with the ability to understand the consequences. Strategic table top exercises are necessary in order to prepare senior and mid-level leadership for cyber security crises. We draw on situations that we have witnessed during the Crimea campaign and afterwards between the Russian Federation and Ukraine.

4:20 P.M. **PANEL: THE WAY AHEAD FOR COUNTERING THE GROWING CYBER THREAT**

Chair: Ms. Lori Scherer
Vice President for Intelligence Portfolios, The MITRE Corporation

Mr. Andrea Formenti
Founder and Owner, Area SpA

Mr. Maurice Cashman
Chief Strategist, McAfee

"Artificial Intelligence and Cyber"

Increasingly, businesses depend on advanced analytics to derive new insights, drive automated processes or increase the speed of decision making. In parallel, advanced analytics are increasingly applied to cyber security for similar outcomes—better insights for prevention or detection, improving adaptability, and driving automated processes. With this new dependence on artificial intelligence or machine learning comes new risks and opportunities. Attacks on analytic models and evasions by adversaries are growing in concert with the application of more automation in security and business intelligence systems. What impact does automated processing have on privacy? Organizations now need to understand how to build a secure analytic strategy and design cyber defensive systems that are resilient on another level. How to recognize those risks and recommendations for improving cyber resilience in the analytic-driven business.

Ms. Caroline Baylon
Information Security Research Lead, AXA;
Advisor, Center for Strategic Decision Research

"Cyber Threats to Connected Cars and Autonomous Vehicles"

Overview of some of the major cyber vulnerabilities in connected cars and what it means from a futures perspective.

Mr. Don Proctor
Former Senior Vice President, Cisco

"Does Today's Software Need a 'Moral Compass'?"

In a world of artificial intelligence, self-driving vehicles, and both civilian and military drones, how do the hard decisions get made? By humans operating behind the scenes, or by software algorithms that have programmed the most likely situations in advance, and can be updated continuously? How does software decide what to do in the case of an unavoidable vehicle collision, or when to drop a bomb?

5:15 P.M. **CONCLUDING REMARKS**

Ingénieur général Jean-Christophe Cardamone
Deputy Director, Institut des hautes études de défense nationale (IHEDN)

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

5:30 P.M. **CLOSING RECEPTION**

The closing reception will be held in the Salons du Quesnoy.

6:30 P.M. **END OF WORKSHOP**

The *34th International Workshop on Global Security* is presented by the Center for Strategic Decision Research (CSDR) and the Institut des hautes études de défense nationale (IHEDN), with the sponsorship of the following governments and organizations:

MAJOR SPONSORS

ASSOCIATE SPONSORS

ACKNOWLEDGEMENTS TO PAST HOST & SPONSOR GOVERNMENTS

Czech Republic
Kingdom of Denmark
Federal Republic of Germany
Republic of Hungary
Kingdom of the Netherlands
Kingdom of Norway
Republic of Greece
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 Federation's Ministry of Industry, Science & Technology