33rd International Workshop on Global Security

# Global Security in Crisis:

## The Deepening Cracks in the Rules Based International Order, the Rise of Radical Islam, the Cyber Threat, and Faltering globalization

## Summary and Findings

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

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

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

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

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

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

***Finding 3. According to secret CIA assessments, Russia is believed to have intervened in the U.S. Presidential Election campaign with a massive cyber influence operation and ultimately saw its preferred candidate, Donald Trump, triumph as the President-elect.*** [1]

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

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

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

***Finding 4. If the CIA's attribution is correct, Russian intervention in the U.S. election[2] may have been one of the most serious cyber influence operations ever conducted, since it undermined trust in electoral processes. The 2017 French and German elections face risks of disruption as well.***

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

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

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

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

***Finding 6. Dealing with ISIS/Daesh requires recognizing that the enemy is Salafist jihadism that seeks global supremacy through the replacement of Western influences by a Caliphate and the use of violence. Yet, most governments currently prioritize the financial benefits of strong relationships with the oil-rich Gulf States that continue to fund radical Islam.[3]***

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

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

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

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

---

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

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

***Finding 8. The exponential growth of the Internet of Things (IoT)—headed toward 50 billion connected devices—opens up vast vulnerabilities that range from cyber crime to cyber attacks on critical infrastructure. (A Mirai malware attack recently exploited 100,000 poorly protected devices including surveillance cameras in order to take down a portion of the internet.)***

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

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

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

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

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

Prepared by:
Roger Weissinger-Baylon, Ph.D.,
Workshop Chairman and Founder; Director, Center for Strategic Decision Research
Email: roger@csdr.org website: https://www.csdr.org

33rd International Workshop on Global Security

# *Workshop Agenda*

*Patron*

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

Patron of the 30th, 31st and 32nd International Workshops on Global Security

*Theme* Global Security in Crisis: The deepening cracks in the rules-based international order, the rise of radical Islam, the cyber threat, and faltering globalization

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

*Presented by* Center for Strategic Decision Research (CSDR)

*and* Institut des hautes études de défense nationale (IHEDN), within the French Prime Minister's organization
· Including the Castex Chair of Cyber Strategy

*Principal Sponsors* French Ministry of Defense

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

North Atlantic Treaty Organization
· Public Diplomacy

Cisco Systems

*Major Sponsors* McAfee | Intel Security · MITRE · Area SpA

*Associate Sponsors* Cast Software · ARES · AXA

# *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, 2014, 2015)*
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 (1996–98, 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**

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, 2014)*
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 Agenda*

His Excellency Jean-Yves Le Drian
*Minister of Defense of France*

Patron of the 30th, 31st, and 32nd
International Workshops on Global Security

## SUNDAY, 6 NOVEMBER 2016

**5:30 P.M.** **PRE-WORKSHOP VISIT OF THE INVALIDES**

***Pre-workshop visit of the Hôtel National des Invalides (Invalides national monument), including the Cathedral and Dome Church, which contains the tomb of Napoleon, and the Museum of the Army.***

**6:45 P.M.** **RECEPTION**

***Reception in the "Salons du Quesnoy," the former reception rooms of the Director of the Invalides.***

**7:45 P.M.** **END OF RECEPTION**

## MONDAY, 7 NOVEMBER 2016

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

***All workshop sessions will be held at the Invalides national monument, in the "Salons du Gouverneur Militaire" (private reception rooms of the Military Governor of Paris).***

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 the architect Libéral Bruant. Jules Hardouin-Mansart, one of the principal architects of Versailles, later completed the cathedral church and added a magnificent dome.

The Invalides also houses the imposing tomb of Napoleon Bonaparte.

Originally built as a hospital for wounded veterans, a portion of the Invalides still operates according to the building's original purpose. In addition to containing several museums dedicated to the military history of France and being one of Paris' major attractions, the Invalides complex also houses the headquarters of ANSSI, France's main cyber security body; the residence of the Military Governor of Paris; and government offices.

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

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

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

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

Mr. Camille Grand
*NATO Assistant Secretary General for Defense Investment*

"Developing the Right Capabilities to Face Global Security in Crisis"

**10:50 A.M.** **INVITED ADDRESS: FRANCE IS AT WAR—THE RAMIFICATIONS IN CYBERSPACE**

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

Security, stability and peace in cyberspace, as in the physical world, is the ultimate goal of the French Ministry of Defense and the French Armed Forces. It is a common challenge which must be met by all actors in cyberspace: states, international organizations, the private sector, and individuals. This year is a unique year—both challenging and decisive. The Paris and Nice terrorist attacks, as well as the murders of policemen and a priest, have brought terrorism to our own soil. Our President stated that France is at war. This war also has ramifications in cyberspace.

For France, since the 2013 White Paper on Defense and National Security gave the Armed Forces the mission of carrying out operations in the digital arena, cyberspace is now considered a battlespace like sea, ground, and air. We now plan and conduct operations in both the offensive and defensive areas. In dealing with Daesh, we are focusing on countering its propaganda.

**11:10 A.M.** **PANEL: CYBER SECURITY—INTERNATIONAL PERSPECTIVES**

Given the global nature of the internet, cyber crime, hacking, spying, and malicious attacks can originate from anywhere—even from developing countries since they may lack adequate infrastructure or regulation and users may not be able to afford antivirus or other protections. There is also the possibility that countries, such as Russia, China, or Iran, may sometimes tolerate or even support hacking groups—some of which have significant technical capabilities. In this context, governments and international organizations need to work together to reach agreements that can reduce risk, including the real danger that some attacks could inadvertently escalate into a form of cyber war and where critical infrastructure might be at risk. With the arrival of the internet of things (IoT) and IPv6, there will be an explosion in the number of devices as well as vulnerabilities and the means to exploit them. Worse, anyone with criminal intent and limited technical skill can purchase sophisticated hacking software at affordable cost on the dark web.

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

"The U.N. Group of Governmental Experts: Perspectives for the 2016/2017 Round"

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

"EU Efforts in Increasing Global Cyber Stability"

The European Union's approach to attaining a secure and free cyberspace that will be accessible and trusted involves supporting ongoing initiatives to develop cyber norms and confidence-building measures and to apply international law in cyberspace. The EU is also funding major capacity-building programs to fight cyber crime and address cyber threats globally.

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

NATO has recognized cyber as a new military domain, although many member countries are only beginning to develop significant cyber capabilities that SACEUR will be able to use effectively. Perhaps this will eventually lead to a NATO cyber command that could acquire and develop cyber capabilities.

Mr. Atsushi Saito
*Director, Cyber Policy Division, Japanese Foreign Policy Bureau*

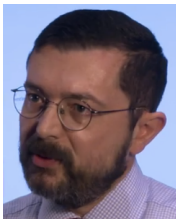
"Japan's Diplomatic Efforts in Promoting Cybersecurity"

In response to cyber threats to Japan and its neighbors, Japan's diplomatic efforts are focused on promoting the rule of law in cyberspace, confidence-building, and capacity-building of developing countries.

**12:30 P.M.** **END OF SESSION**

**12:40 P.M.** **LUNCH**

**LUNCHEON ADDRESS**



Mr. Conrad Prince
*Cyber Security Ambassador, United Kingdom Defence and Security Organisation*

"The UK's National Cyber Security Strategy"

Discussion of the UK's approach to cyber security and the new strategy that was just launched earlier this week.

**2:00 P.M.** **PANEL: THE RELATIONSHIP WITH RUSSIA—SEARCHING FOR A NEW APPROACH**

The steadily increasing strains in the relationship with Russia are in no one's interest. Neither the sanctions against Russia nor the efforts to strengthen the military capabilities of its neighbors seem to have the desired effects. Cooperation with Russia over Syria and Daesh/ISIS is fragile. Now, the U.S. government is blaming Russia for email hacks that are impacting the Presidential election campaign. As tensions rise, there is a potential for miscalculation by either side that might lead to cyber war or even the use of nuclear weapons. The prospects for such scenarios may be exaggerated, but it would be a mistake to dismiss them completely.

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

"A Northern Perspective on Relations with Russia"

In the Baltic Sea region, relations between Russia and the West have deteriorated since 2013 and the level of trust and co-operation is lower than ever since the Cold War. Is there a chance to reverse the negative trend? Could the more constructive relationship in the Arctic serve as an inspiration?

Ambassador Luís de Almeida Sampaio
*Permanent Representative of Portugal to NATO*

"A Southern Perspective on Developments in the Middle East and the Mediterranean Region"

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

**3:30 P.M.** **COFFEE BREAK**

**4:00 P.M.** **PANEL: DAESH/ISIS—DEALING WITH THE SPREADING THREAT**

Despite the spreading threat of terrorist attacks, many governments—including the U.S.—seem reluctant to attribute them to "radical Islam" or "political Islam." They also avoid mentioning Salafism or Wahhabism, despite knowing that Qatar and Saudi Arabia have financially supported these extremist religious views for decades. Actually, governments are in a bind because they are actively courting these very same wealthy Gulf States to make real estate and other investments in their countries, for armaments sales, and other trade. At the same time, increasing income inequality, uncontrolled migration, and other factors are worsening the situation. Under the circumstances, what can be done? Can we learn from some countries that have found effective ways of dealing with these threats? Looking to the future, if Mosul falls, will returning djihadists increase the threat in Europe? What if ISIS deepens its ties to

highly capable cyber criminals and/or turns to cyber terrorism?

Chair: Ambassador Miguel Aguirre de Carcer
*Permanent Representative of Spain to NATO*

"Why the Internal and External Aspects of Terrorism are Increasingly Intertwined"

Mr. Pjer Šimunović
*Director, Office of the National Security Council of Croatia; former Ambassador of Croatia to Israel*

While the territory controlled by Daesh contracts, its manpower and resources depleted, a 'Caliphate now' narrative may be losing ground, but there seems to be no end in sight for Salafi/Jihadism in general, which may be morphing yet again into a new form. With the fight most likely shifting back underground, an immediate danger is presented by Daesh and Daesh-inspired terrorist convulsions in the region and globally. In the continuously shifting sands of the Middle East, amid an orgy of violence, a new power vacuum is in the making, with a spectrum of bitter rivals racing to fill it.

Ambassador Mehmet Fatih Ceylan
*Permanent Representative of Turkey to NATO*

"The Daesh Spillover in the Middle East and North Africa: Developments and Root Causes"

Discussion of the measures taken by Turkey in order to contribute to degrading and destroying Daesh, as well as the next steps to be taken in the fight against Daesh and the role that NATO can play.

Ms. Marietje Schaake
*Member of the European Parliament*

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

Saudi Arabia, sometimes described as "Daesh that has made it," beheads its citizens, tramples on women's rights and flogs atheists. Yet it is placing itself at the heart of international human rights efforts and counter-terrorism, which are out of line with its own practices. There are equally serious reasons for concern about the actions of Iran.

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

"The Opportunities for Terrorism in Cyberspace"

The internet offers powerful capabilities for spreading propaganda and for recruitment: Daesh's success is the proof of this. In the face of the widespread diffusion of djihadist images, videos, and messages in cyberspace, the only possible responses are legal and technical. The battle of ideas has begun. And only with innovative ideas can terrorism be defeated. Do our aging democracies still have the energy and moral resources that will be needed?

**5:30 P.M.** **END OF SESSION**

**5:50 P.M.** **DEPARTURE FOR THE RODIN MUSEUM**

The Rodin Museum is almost directly across the street from the conference venue in the private reception rooms of the Military Governor of Paris.

**6:00 P.M.** **PRIVATE VISIT OF THE RODIN MUSEUM**

***Guided visit of the Musée Rodin (Rodin Museum), which features The Kiss and other famous works.***

Housed in the Hôtel Biron, a magnificent private dwelling built between 1727 and 1732 that served as Rodin's workshop from 1908 onwards, the Rodin Museum contains the world's largest collection of sculptures by Auguste Rodin and the majority of his most significant works.

When the French government announced plans to acquire the building in 1911, Rodin entered into negotiations to donate his entire collection to the French government on the condition that he be allowed to reside in the building for the rest of his life and that the collection be kept at the Hotel Biron in perpetuity as part of a museum. His collection includes not only his own sculptures but also paintings that he acquired by Vincent Van Gogh, Pierre-Auguste Renoir, and Claude Monet. The museum officially opened in 1919.

**7:30 P.M.** **RECEPTION**

*We would like to thank Cisco Systems for sponsoring the reception and private visit of the Rodin Museum.*

**8:30 P.M.** **END OF RECEPTION**

## TUESDAY, 8 NOVEMBER 2016

**8:40 A.M.** **INVITED ADDRESS**

Mr. Guillaume Poupard
*Director General, French National Agency for Information Systems Security (ANSSI)*

Our approach to cyber security is based on the reality that, without cyber security, the sovereignty of the nation is at risk. Cyber security is vital for the protection of the entire economy and our citizens—and especially for defending critical infrastructure from cyber attacks. Because of the importance of the electrical grid, nuclear power plants, and other critical infrastructure, we have decided to impose cyber security by law and regulation, rather than relying on the operators. In the case of a serious attack, the Prime Minister has the authority to take additional steps in order to limit the damage. Our policy also emphasizes the protection of our citizens, of our industry, and the role of international cooperation. As to the future, the best way to defend against cyber attacks is to imagine the worst, and prepare for it. This will lead us to broaden the notion of critical

infrastructure to include such actors as insurance companies, which may be impacted less immediately by an attack, and to work with the European Union to encourage other countries to establish organizations like ours if they do not have them already.

**9:10 A.M.** **INVITED ADDRESS**

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

"Cyber Security for a World of Rapidly Intensifying Cyber Warfare"

Cyber crime and cyber warfare are on a path of dramatic increase, impacting citizens, communities and countries. Catastrophic attacks on existing communication infrastructures are further intensified by the rapid growth and adoption of IoT. Defeating these relentless adversaries will require a more dynamic, effective approach to cybersecurity. Appropriate security principles can serve as a baseline for organizations as they strive to become more effective in their approach to security. These are challenges that industry and the public sector should consider addressing jointly.

**9:40 A.M.** **PANEL: CYBER INFLUENCE OPERATIONS—DAESH PROPAGANDA, MANIPULATING ELECTIONS, AND INFLUENCING PUBLIC OPINION**

Cyber propaganda has been effective in radicalizing youth, who are encouraged to join ISIS/Daesh in Iraq or commit terrorism at home. In fact, internet propaganda has proven to be effective with individuals who would not normally be considered vulnerable to radicalization; it has convinced terrorists to give their own lives, and to attack people who are innocent of everything except not following a Salafist lifestyle. Under the circumstances, neither extreme income inequalities nor the funding of mosques by wealthy Arab States (and their citizens) seem to offer a sufficient explanation for the success of cyber propaganda. Its effectiveness has facilitated the expansion of Daesh/ISIS into the Balkans and North Africa.

With the hacking of the Democratic Party and of Hillary Clinton's presidential campaign, which is being attributed to the Russian cyber groups Cosy Bear and Fancy Bear, Russia seems to be deliberately destabilizing the U.S. political system. Since President Obama has threatened Russia with some form of cyber retaliation, cyber influence operations have reached a dangerous new level.

Chair: Ing. Général Daniel Argenson
*Deputy Director, Institut des hautes études de défense nationale (IHEDN)*

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

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

Discussion of recent major cyber attacks and how they link to NATO's cyber defense agenda after the Warsaw Summit. Cyber attacks are becoming more sophisticated and more damaging, both for governments and the private sector. Cyber is increasingly being used as a tool of hybrid warfare—not just to gather intelligence and information but as part of propaganda and information operations. Examination of the use of the internet by ISIL for propaganda, recruitment and operations. What can be done to disrupt the terrorist narrative? Finally, discussion of whether cyber terrorism is a likely or realistic concept.

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

"Hacking During the U.S. Presidential Campaign"

During the U.S. election campaign, the effects of hacking, which the U.S. government has officially attributed to Russia, have been increasingly disruptive. In the final weeks before the election, the direct and indirect consequences have reached the point where they could affect election results, and perhaps even the leadership of the Senate. Could hacking influence the choice of the next President? Or undermine the integrity of the electoral process?

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

"Russian Strategies for Cyber Influence"

**10:30 A.M.** **COFFEE BREAK**

**11:00 A.M.** **PANEL: PROTECTING CRITICAL INFRASTRUCTURE FROM CYBER ATTACK**

Until now, much of the concern surrounding cyber attacks on critical infrastructure has been focused on the vulnerabilities of the electrical grid, water treatment plants, and other facilities due to a growing trend to connect them to the internet for efficiency reasons. Last month, however, a massive distributed denial of service (DDoS) attack against Dyn, a kind of switchboard for the internet, and another attack which took down the internet in Liberia last week has shown that the internet itself is far too vulnerable. It is especially worrisome that these attacks employed millions of smart devices belonging to the internet of things such as smart thermostats or smart home security systems, which have little protection against malware. Since the IoT will soon be adding billions of additional devices, many with minimal security, the danger is still growing.

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

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

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

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

"The Economics of Cybercrime"

Discussion of the economic impact of cybercrime on the economies of nations, including the inhibition of growth, and the steps needed to address such challenges.

Dr. Linton Wells II
*Advisor, Georgia Tech Research Institute*

There are growing cyber vulnerabilities in all infrastructures in all countries, and especially "smart cities," stemming from the exploding deployment of the internet of things and other factors. Ultimately, this will make nations more vulnerable to the kind of multi-domain cyber (mis)information/psychological/economic attacks we see in Ukraine. This burgeoning weakness seems to be generally under-appreciated at senior levels.

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

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

For the very first time, the UN Security Council will address the issue of cyber security, in an informal "Arria-formula meeting" that will be led jointly by Spain and Senegal. The protection of critical infrastructure from cyber attack is one of the issues that needs to be addressed, following a UN Group of Governmental Experts (GGE) report that was presented to the Secretary General a year ago. The UN GGE report suggests that the UN should play a leading role in promoting dialogue in order to deal with the risk of attacks against critical infrastructure systems.

**12:15 NOON** **END OF SESSION**

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

**1:50 P.M.** **PANEL: CYBERWARFARE AS THE FIFTH BATTLESPACE**

Just two months after the NATO Summit's decision to add cyberwarfare as the fifth battlespace, President Obama's threat of possible retaliation against Russian hacking, as well as the DDoS attack on Dyn and internet infrastructure via smart devices, suggests that cyber may have a permanent place in hybrid war. It also shows the potential seriousness of any future cyber war.

Chair: Mr. Don Proctor
*Senior Vice President in the Office of the Chairman and CEO,*
*Cisco*

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

Recognizing cyber as the fifth military-operational domain has boosted cyber capability development across the whole spectrum of NATO´s command and force structures. Furthermore, it has enabled a

more forward-leaning approach in developing Allied active defense capacity. At the same time, enhancing the cyber defenses of national infrastructures and networks remains primarily a national responsibility.

Yet, in our cyber debates at NATO, one can still hear some nations expressing their expectations that the Alliance will eventually do the job for or instead of them in the event of a serious attack. Those Allies are by and large the same ones that have problems with delivering on their commitments in other areas of capability development. Results of the first annual assessment will be known in roughly one year. Only then will we have a first set of comparable data on national cyber progress or a lack thereof. Nevertheless, one cannot avoid concerns that it will take only a grave cyber disruption until some of our slower Allies wake up and begin to take their cyber defense pledges seriously.

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

"NATO After Warsaw: Don't Get Lost in Cyberspace"

NATO has traveled a long way in dealing with threats and challenges stemming from the growing importance of cyberspace. What should the Alliance do in order to implement the decisions taken at the Summit in Warsaw?

Major General David Senty, USAF (Ret.)
*Director, Cyber Operations, The MITRE Corporation;*
*former Chief of Staff, U.S. Cyber Command*

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

**3:00 P.M.** **COFFEE BREAK**

**3:30 P.M.** **PANEL: THE WAY AHEAD—FOR EUROPE AND THE RELATIONSHIP WITH RUSSIA**

Chair: Ambassador Imants Liegis
*Ambassador of Latvia to France;*
*former Minister of Defense of Latvia*

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

"Europe's Common Security and Defense Policy Post Brexit"

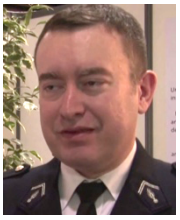
EU citizens are increasingly concerned about security, which is becoming a unifying factor. Since ISIS/Daesh in Iraq is spreading terrorism across Europe, internal and external security can no longer be treated as separate concerns. In the past, Britain was an obstacle to the development of European defense capabilities, but Brexit means that Europeans must assume more responsibility for their own defense. In the past, with 40% of the entire defense budget of all EU countries, the Franco-British engine led the EU. Will it be replaced by a new Franco-German engine? Can Italy play a stronger role? And where will more funds for European defense come from?

Ambassador Boris Grigić
*Permanent Representative of Croatia to NATO*

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

Can Russia eventually decide not to accept the independence of former members of the USSR, including the right to choose the alliance they would like to join? In the Balkans, what is the real extent of Russia's influence and what should the West do? Is the appeal of the historical Slavic brotherhood, supported by access to oil and gas, stronger than the EU?

**4:15 P.M.** **PANEL: THE WAY AHEAD FOR COUNTERING THE GROWING CYBER THREAT**



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

Mr. Andrea Formenti
*President, Area SpA*

"Cyber Intelligence—The Challenge of Determining Attribution in Cyberspace, While Balancing the Digital Economy, Privacy, Security and International Public/Private Cooperation"

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

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

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

Kurt Westerman
*Vice President, ARES Corporation*

"Cyber Security within the Framework of an Overall Security Strategy—including the "Insider Threat"

**5:30 P.M.** **CONCLUDING REMARKS**

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

**5:45 P.M.** **CLOSING RECEPTION AT THE INVALIDES**

***Wine and cheese reception.***

**7:00 P.M.** **END OF WORKSHOP**

The *33rd International Workshop on Global Security* is presented by Center for Strategic Decision Research (CSDR) and Institut des hautes études de défense nationale (IHEDN), with the sponsorship of the following governments and organizations:



UNITED STATES
DEPARTMENT OF DEFENSE
Net Assessment


PUBLIC DIPLOMACY

Center for
Strategic
Decision
Research



## MAJOR SPONSORS




## ASSOCIATE SPONSORS




## ACKNOWLEDGEMENTS TO PAST HOST AND 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