Follow us #CyberIWGS

35th International Workshop on Global Security

Workshop Agenda

35th International Workshop on Global Security and the Cyber Threats
Hôtel National des Invalides, Paris, 16-17 April, 2019

Themes — Global Security in the Age of Hybrid Conflict: Cyber Threats and Cyber Influence Operations

Honorary Chairmen — Lieutenant General Patrick Destremau
Director, Institute for Higher National Defence Studies (IHEDN)

Major General Jean-Christophe Cardamone
Deputy Director, Institute for Higher National Defence Studies (IHEDN)

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

Presented by — Center for Strategic Decision Research (CSDR)

and — IHEDN — Institute for Higher Defence Studies (IHEDN), within the French Prime Minister's Organization

and — DGRIS — General Directorate for International Relations and Strategy (DGRIS), French Ministry of the Armed Forces

Principal Sponsors

NATO OTAN — NATO Public Diplomacy Division

Liberté • Égalité • Fraternité RÉPUBLIQUE FRANÇAISE — French Ministry of the Armed Forces

Department of Defense United States of America — U.S. Department Of Defense

Technology Partner — panda — Panda Security

Major Sponsors — McAfee, FUJITSU, MITRE, CISQ, AREA (Since 1996, Intelligence Mindset)

Associate Sponsors — NCI Agency, Karakawa Foundation Peace, AXA, Cybexer Technologies

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

Patrons

Her Excellency Florence Parly, *Minister of the Armed Forces of France (2017, 2018, 2019)*
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 Patrick Destremau, *Director, Institut des hautes études de défense nation (2019)*
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 the Armed Forces of France *(2005, 2007, 2011, 2013-2019)*
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)*

WORKSHOP PATRON

Her Excellency Florence Parly
Minister of the Armed Forces of France

TUESDAY, 16 APRIL 2019

9:15 A.M. **WELCOME COFFEE AND REGISTRATION**

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

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.

In addition to being one of Paris' major attractions and containing several museums dedicated to France's military history, the Invalides complex also serves as the headquarters of ANSSI, France's main cyber security body, and as the residence of several high state officials.

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

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

Lieutenant General Patrick Destremau
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. **KEYNOTE OPENING ADDRESS ON BEHALF OF THE FRENCH MINISTRY OF THE ARMED FORCES**

Brigadier General Didier Tisseyre
Deputy Cybercommander, French Ministry of the Armed Forces

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

Lieutenant General Ludwig Leinhos
Chief of German Cyber and Information Domain Service

“The Effects of Digitization on Armed Forces”

"Digitization" is the central issue of our time. Digitization makes enormous improvements and innovations possible—also for armed forces. But, it also brings considerable risks and dependencies—across national borders. They affect all of us: states, governments, societies, business enterprises and individuals. Therefore, protection against the risks from cyber and the information space is of great strategic importance and must be considered as a matter of national concern.

Cyberattacks against states, business enterprises and private households have long been a reality. In addition to cyberattacks, activities in the information environment, such as fake news campaigns aimed at creating unrest, are often used to destabilize fundamental democratic structures. Conflicts between states as well as intra-state conflicts are increasingly susceptible to the influence of propaganda and disinformation.

Future conflict scenarios will technically be characterized by digitization, artificial intelligence and autonomy. A large-scale kinetic war is no longer the most probable scenario. Hybridity is playing an increasingly decisive role.

11:20 A.M. **PANEL: CYBER CRIME AND THE DARK WEB—COUNTERING THE THREATS**

Chair: Ambassador Istvan Kovacs
Senior Advisor, NATO Strategic Communications Center of Excellence (StratCom), Latvia; former Hungarian Ambassador to NATO

Colonel Jean-Dominique Nollet
Director of the Centre de lutte contre la criminalité numérique (C3N), French Gendarmerie Nationale

Mr. Andrea Formenti
Founder and Owner, Area SpA

"Profiling, Targeting, and Investigating the Darkest Activities of the Internet"

The actual framework used by many countries to protect the privacy of citizens, guarantee transparency, and ensure appropriate oversight is compared to the challenges of changing technologies and social/digital behaviors and all the threats that this entails. Innovations in investigative technologies are part of the debate.

12:00 NOON **END OF SESSION**

King's Council Chamber of the Hôtel National des Invalides

12:20 P.M. **LUNCH**—Hosted by Panda Security

panda

1:50 P.M. **ADDRESS BY THE TECHNOLOGY PARTNER**

Mr. Jan Lindner
Vice President, Northern Continental Europe, Panda Security

"Defense of our Digital Democracy."

2:20 P.M. **PANEL: DEALING WITH CYBER CONFLICT AMONG STATES—BUILDING NORMS FOR STATE BEHAVIOR IN CYBERSPACE**

Ms. Michele Markoff
Deputy Coordinator for Cyber Issues, U.S. Department of State"

"Building an Architecture to Maintain Stability in Cyberspace Based on Norms, Confidence Building, and Accountability"

Over the years, the international community has worked to build consensus around a framework for responsible State behavior in cyberspace. Even as we continue to advance this effort, responsible States must also work to ensure that there is accountability for States that act contrary to this framework.

Mr. Wolfram von Heynitz
Head, Cyber Policy Coordination Staff, German Federal Foreign Office

"Europe's role in the global competition on AI"

Description of the norm-building process in the UN; the German view on the upcoming "Group of Government Experts," and the "Open-ended Working Group" of the UN; and how the new outreach process to regional organizations like the OSCE could add value to the work of these groups. There is an additional need for developing a global framework for AI and to explain how the "Ethics Guidelines" of the EU high-level working group, published this Monday, could contribute to this process.

Ambassador Károly Dan
Ambassador of Hungary to the OSCE, Chair of the IWG for Cyber

"The Role of OSCE Confidence Building Measures in Promoting Cyber/ICT Security"

3:15 P.M. **INVITED PANEL: DEALING WITH HYBRID THREATS**

Chair: Dr. Antonio Missiroli
NATO Assistant Secretary General for Emerging Security Challenges

Mr. B. Edwin Wilson
U.S. Deputy Assistant Secretary of Defense for Cyber Policy

Ms. Simona Cojocaru
General Director for Defense Policy, Romanian Ministry of Defense

“The Hybrid Threat in the Black Sea Area”

The main security challenges in the Black Sea region are all interconnected and intertwined in the wider context of Euro-Atlantic security. The most important influence on the security in the region is generated by Russia’s assertive approach and aggressive behavior in relations with its neighbors and towards NATO and the EU.

Russia is tailoring its hybrid warfare capabilities to best exploit the specific vulnerabilities of each state in the region: propaganda campaigns to reduce the cooperation in the region and undermine trust in Euro-Atlantic institutions, spread of fake news and conspiracy theories and direct support for Euro-skeptic parties.
The frozen conflicts in the region fuel organized crime, smuggling and radicalization and have significant potential to destabilize the whole region rapidly. Another leverage used by Russia is energy security as the Black Sea is a key transit corridor for energy resources.

Mr. Josef Shröfl
Deputy Director for Strategy & Defense,
Hybrid Center of Excellence, Helsinki, Finland.

“Cyber Power in Hybrid Warfare”

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

4:30 P.M. **PANEL: PREVENTING A BLACK SKY EVENT—DEALING WITH CYBER THREATS TO THE POWER GRID**

Chair: Ms. Caroline Baylon
Security Research Lead, Strategy, Research, and Threat Horizon, AXA;
Senior Advisor, Center for Strategic Decision Research

Mr. Raj Samani
McAfee Fellow, Chief Scientist, McAfee

Mr. Xavier Carton
Deputy Director of Information Systems, RTE (Réseau de Transport d'Electricité—French National Electrical Transmission Network)

"What a GRT (National Electrical Transmission Grids) Can Do to Protect against the Risk of a Cyber Blackout"

The world of electricity is in profound transformation: Renewable and intermittant energy sources, storage, production, decentralized production and consumption, auto-production, electrical-based mobility, and integration of intelligence into certain devices. As for any major transformation, it leads to enthusiam among different actors, especially among the public.

As to the cyber risks, the evolution is rather profound. Until recently, it was enough to physically and logically isolate the transmission grid and to apply appropriate security procedures to have reasonable confidence in the system's resilience.

Today, the transmission system must be connected to the internet and perimeter protection is no longer adequate. Lawmakers have become aware of the risks, however, and have imposed security rules on operators of critical infrastructure. This has had excellent consequences. France now has cyber security capabilities of sufficient size and quality to strengthen the security of the operators.

Ingénieur général Antoine-Tristan Mocilnikar
Ingénieur général des Mines; Department of Defense, Security, and Economic Intelligence; French Ministry of Ecological and Solidarity Transition

"Infrastructure and Cyber Threats in the Global Framework of Hybrid Threats."

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

6:00 P.M. **RECEPTION AND DINNER IN THE SALLE TURENNE**

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.

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

WEDNESDAY, 17 APRIL 2019

9:00 A.M. **PANEL: RUSSIAN CYBER INFLUENCE OPERATIONS—FINDING WAYS TO SECURE OUR ELECTORAL SYSTEMS AND DEFEND OUR DEMOCRACIES**

Chair: Dr. Frederick Douzet
Director of the GEODE (Geopolitics of the Datasphere), University of Paris 8

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

"The Imperative of Societal Resilience."

Hybrid warfare in cyberspace poses two types of threats to our societies: physical destruction of critical infrastructure and psychological effects. Physical destruction can be deterred in a more traditional way—e.g. NATO has declared the possibility of invoking its collective defence clause (including physical retaliation) should a cyberattack result in wide-scale physical damage. Psychological effects, however, are much more dangerous –they are less visible, longer-term, creeping and the attribution of the attacker is likely to be ambiguous. Instead of deterrence, resilience is the right answer, namely for our societies. Societal resilience includes positive values and characteristics such as mutual trust and solidarity among people, society cohesion, and loyalty to the institutions of the state. The way to building such a team spirit in our societies is through good democratic governance, transparency and accountability of the power, a strong and active civil society, as well as educated people who can think critically.

Ambassador Luis de Almeida Sampaio
Permanent Representative of Portugal to NATO

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

"The Future of Russian Digital Influence"

Disinformation is surely a weapon to influence human behaviour. It is dramatically changing the ways societies perceive and consume news, make decisions and interact. Are we adjusting fast enough, are we fully aware of what can and need to be done? While reflecting on that, the foreign interference in recent elections around the globe continues to disrupt the international order.

10:00 A.M. **INVITED ADDRESS**

Mr. Emmanuel Chiva
Director, Defense Innovation Agency, French Ministry of Defense

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

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

10:50 A.M. **PANEL: LOOKING TOWARDS OUR DIGITAL FUTURE—IMAGINING THE WORLD IN 2040**

Chair: Ms. Caroline Baylon
Security Research Lead, Strategy, Research, and Threat Horizon, AXA; Senior Advisor, Center for Strategic Decision Research

Dr. Linton Wells II
Former U.S. Assistant Secretary of Defense (Acting) and Chief Information Officer

“Digital Elements of Converged Technologies—Some Security Implications of the 4th Industrial Revolution

The Fourth Industrial Revolution projects "a fusion of technologies that is blurring lines between the physical, digital, and biological spheres." In the digital sphere, these include AI and Machine Learning; Automation; Cloud Computing; Big Data and Analytics; Advanced Cyber Security and Cyber Resilience; Quantum Information Science; Advanced Mobile and Wireless; and Distributed Ledger Technologies, like blockchain. These will intersect with the physical world in areas like advanced manufacturing (including 3D printing), new materials, autonomous systems, etc., and with the biological sphere in other areas like synthetic biological, artificial organs, genetic engineering, etc. All will be affected by converging, accelerating technologies—part of what Tom Friedman has termed the "Age of Accelerations." This presentation will touch on some of the security implications of these changes.

Ms. Merle Maigre
Executive Vice President, CybExer Technologies

“Essential Collective and Individual Cybersecurity Components.”

Cybersecurity really is a strategic concern and should not be degenerated into a technical issue. In today's world, raising the awareness of our decision makers about cyber security is crucial. But even the strongest, best coordinated collective response is not sufficient without an individual response.

Independently of our jobs, our age, our level of responsibility, we all need some technological literacy at the individual level if we want not only to function in a digitized society but to make sure we don't create risks to it by our behavior. In Estonia, we call that cyber hygiene.

Captain Philippe Charton
Cyber Operations Head, NATO Communications and Information Agency (NCIA)

"NATO's Digital Endeavour—Facing the Future Cyber Threats".

NATO, like any other large international organisation, must conduct a digital transformation to face the 21st century challenges. The NATO Communications and Information Agency (NCIA) is responsible for guiding the Alliance through this transformation. The Agency is actively engaged in order to deliver a secure, modern digital infrastructure to NATO, wherever the Alliance is operating, to safeguard peace and stability.

Professor Yuki N. Karakawa (Disaster Medicine),
IAEM Ambassador (US Civil Defense Council), Board Director, IVe Hospital Foundation

"Using Digital Twins and AI to Create a New Cyber World for the Benefit of Humanity: the Risk of Conceptual Error."

11:40 A.M. **INVITED ADDRESS**

Mr. Jose Sancho
Chairman, Panda Security

12:00 P.M. **END OF SESSION**

12:15 P.M. **LUNCH --** Hosted by Panda Security

panda

1:50 P.M. **PANEL: COUNTERING THE CYBER THREAT: THE ROLE OF NEW TECHNOLOGIES AND AI**

Chair: Ms. Caroline Baylon
Security Research Lead, Strategy, Research, and Threat Horizon, AXA; Senior Advisor, Center for Strategic Decision Research

Mr. Maurice Cashman
Chief Strategist, McAfee

"Artificial Intelligence and the Cyber Threat: A Chief Information Security Officer(CISO) Perspective"

Artificial Intelligence is a hot topic these days in cyber security. However, we need to separate the noise form reality. This talk will explore ways an organization can benefit from Artificial Intelligence in their security strategy and highlight new areas of risk caused by the introduction of AI-enabled technology into the new digital enterprise.

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

"A New Approach for Military Strategy and Planning in the Grey Zone (Non-kinetic Asymmetrical Hybrid Warfare)"

Recent adversaries have operated with near impunity within the grey zone for years. Crossing between military, civilian, and commercial targets is considered normal and appropriate to them. These non-kinetic attacks, with cyber operations as a primary capability or enabler, have only increased in intensity and are exploiting expanded opportunities. I would like to discuss non-kinetic asymmetrical or hybrid warfare that employs cyberspace as well as the challenges this type of warfare places on militaries and governments alike.

Mr. Donald Proctor
Former Senior Vice President, Cisco Systems

"Cybersecurity and AI: Second-Order Effects of Facial Recognition Technology."

Like cybersecurity, artificial intelligence has become an important matter of national security. As governments adopt new guidelines to regulate the use of AI, and industry seeks ways to create ethical guidelines for its development, we will discuss strategies to manage the second-order effects—the unintended consequences—of AI in our increasingly digital world.

2:50 P.M. **COFFEE BREAK**

3:20 P.M. **PANEL: RESPONDING TO CYBER CRISES—HOW TO DEAL WITH THE CHALLENGES**

Dr. Jamie Shea
Senior Fellow, Friends of Europe; Former NATO Deputy Assistant Secretary General for Emerging Security Challenges

Mr. Brian Abe
Technical Director, National Cybersecurity FFRDC, The MITRE Corporation

Colonel Jaak Tarien
Director, NATO Cooperative Cyber Defense Center of Excellence, Estonia

"The Importance of Training in Facing Future Challenges: Examples from the CCDCOE Exercises and Training portfolio."

Mr. David Norton
Managing Director, Consortium for IT Software Quality (CISQ)

"The Fly-By-Wire Security Strategy—Agility and Speed, with Control"

Organizations have 21st-century aspirations and 20th-century mindsets. It is analogous to wanting an F-35 fighter flight characteristics using 1903 Wright Brothers technology. Business and IT executives need to recognize that if they want shorter time to market for digital products and IoT ecosystems, they need to increase the levels of automation within the engineering and support processes. Just like the modern fighter, we need feedback-based automation that allows people to focus on the important stuff: mission outcomes.

Mr. Lauri Tankler
Cyber Security Service, Estonian Information System Authority

"State Responsibility in Dealing With Cyber Threats"

Governments and states have usually been reactive when facing new technological threats or crises. The risks and threats are not always purely technological, but usually have legal and political aspects. While legal and political discussions often revolve around protecting citizens in the foreseeable future, technical aspects are usually discussed in hindsight while implementing regulation, norms or political decisions. Discussions around the 5G technology, as well as the attribution of attacks and the dissemination of false information on social networks show that the technical aspects may need to have a more proactive approach.

4:30 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)

5:00 P.M. **END OF WORKSHOP**

“Cour d’Honneur” of the Invalides

The 35th *International Workshop on Global Security* is presented by the Center for Strategic Decision Research (CSDR), the Institute for Higher Defense Studies (IHEDN), and the General Directorate for International Relations and Strategy (DGRIS), with the sponsorship of the following governments and organizations:

TECHNOLOGY PARTNER

Panda Security

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 the Armed Forces of France
Ministry of Defense of Italy
Ministry of Defense of Turkey
Canadian Armed Forces
Russian Federation’s Ministry of Industry, Science & Technology