Global Security in the Age of Hybrid Conflict

Cyber Threats and Cyber Influence Operations

PROCEEDINGS OF THE *35th* INTERNATIONAL WORKSHOP ON GLOBAL SECURITY

Mrs. Florence Parly
Minister of the Armed Forces of France

Lieutenant General Patrick Destremau
Director, Institute for Higher National Defence Studies

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

Dr. Roger Weissinger-Baylon
Workshop Chairman and Founder

Anne D. Baylon, LL.B., M.A.
Editor

COVER IMAGE

Hôtel National des Invalides, Paris

Published by

Center for Strategic Decision Research | Strategic Decisions Press

2456 Sharon Oaks Drive, Menlo Park, California 94025 USA

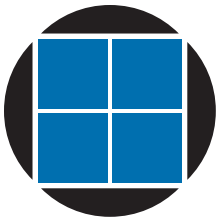
www.csdr.org

Anne D. Baylon, LL.B., M.A., Editor | anne@csdr.org

Dr. Roger Weissinger-Baylon, Chairman | roger@csdr.org

Photography by Matteo Pellegrinuzzi | mail@matteopellegrinuzzi.com

International Standard Book Number: 1-890664-



35*th* International Workshop on Global Security

Workshop Proceedings

Anne D. Baylon, LL.B., M.A.
Editor

WORKSHOP PATRON	Mrs. Florence Parly *Minister of the Armed Forces of France*
THEME	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); Institute for Higher Defence Studies (IHEDN) within the French Prime Minister's Organization; and General Directorate for International Relations and Strategy (DGRIS), French Ministry of the Armed Forces
PRINCIPAL SPONSORS	NATO Public Diplomacy Division French Ministry of Defense U.S. Department of Defense
TECHNOLOGY PARTNER	Panda Security
MAJOR SPONSORS	McAfee, Fujitsu, MITRE, CiSQ, Area SpA
ASSOCIATE SPONSORS	NCI, Karakawa Foundation Peace, AXA, CybExer Technologies

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

Center for Strategic Decision Research

IHEDN

DGRIS
Direction générale des relations internationales et de la stratégie
MINISTÈRE DES ARMÉES

NATO OTAN
PUBLIC DIPLOMACY

UNITED STATES DEPARTMENT OF DEFENSE
Net Assessment

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE LA DÉFENSE

TECHNOLOGY PARTNER

panda

MAJOR SPONSORS

McAfee FUJITSU SINCE 1996 AREA INTELLIGENCE MINDSET MITRE CISQ

ASSOCIATE SPONSORS

NCI AGENCY AXA Karakawa Foundation Peace CYBEXER TECHNOLOGIES

ACKNOWLEDGEMENTS OF PAST HOST AND SPONSORING GOVERNMENTS

Czech Republic
Kingdom of Denmark
Federal Republic of Germany
Republic of Greece
Republic of Hungary
Kingdom of the Netherlands
Kingdom of Norway
Republic of Poland
Republic of Portugal
Ministry of Defense of Austria
Ministry of Defense of France
Ministry of Defense of Italy
Ministry of Defense of Turkey
Canadian Armed Forces
Russian Ministry of Industry, Science, and Technology

With Appreciation

Mrs. Florence Parly
Minister of the Armies

Lt. Gen Patrick Destremau
Director, Institut des hautes études de défense national

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

Mr. Jose Sancho
Chairman, Panda Security
Technology Partner

Patron of the 34th International Workshop

Mrs. Florence Parly
Minister of the Armies

Table of Contents

INVITED PRESENTATIONS

RUSSIAN CYBER INFLUENCE OPERATIONS—FINDING WAYS TO SECURE OUR ELECTORAL SYSTEMS AND DEFEND OUR DEMOCRACIES

LOOKING TOWARDS OUR DIGITAL FUTURE—IMAGINING THE WORLD IN 2040

COUNTERING THE CYBER THREAT: THE ROLE OF NEW TECHNOLOGIES AND AI

RESPONDING TO CYBER CRISES—HOW TO DEAL WITH THE CHALLENGES

CONCLUDING REMARKS

Overview
Hybrid Conflict in the Post-Truth Era: the New Threats from Russia, China…and GAFA

Dr. Roger Weissinger-Baylon
Workshop Chairman and Co-Founder

Introduction. Hybrid conflicts in the post-truth era. The internet has become a battlefield where large states and giant international technology corporations (including GAFA) are fighting for power and dominance. As NATO's Assistant Secretary General Antonio Missiroli points out, hybrid threats and campaigns from Russia, China, or other adversaries "tend to be carried out through cyberspace" because they are unusually "hard to detect, deter, and attribute." By staying within a "grey zone" below the level of intensity that might trigger a conventional kinetic military response, states are able to act with such impunity that hybrid campaigns will be the principal means of future conflicts.

Military actors, however, are not alone in exploiting cyberspace to attack our societies. Cyberspace is being vampirized by criminal actors, political parties, and other powerful groups, acting in ways that sometimes mimic the hybrid campaigns of foreign adversaries. They threaten not only data and financial or physical systems, as in the past, but human dignity and the very notion of truth—which is the lifeblood of democracy. After initially exploiting unexpected vulnerabilities of the GAFA giants, political actors are now being openly allowed by social media, and notably by Facebook, to rapidly spread massive amounts of false information and emotionally charged messages. Many of these messages are artfully designed to trigger divisions and hate in a post-truth world[1] where falsehoods and lies are openly tolerated or even encouraged. George Orwell's fictional world of *Nineteen Eighty-Four* is not far away. Unfortunately, NATO and similar organizations are unable to deal effectively with the treats facing our post-truth society because they are not considered to be military in nature.

Politicians are allowed by Facebook to rapidly spread false information and emotionally charged messages.

Future conflicts will be hybrid, not conventional. In his opening remarks to the *35th International Workshop on Global Security*, General Didier Tisseyre observed that states are in continuous competition, but globalization makes them highly interdependent. As a result, aggressor states will prefer to engage in hybrid conflict—and avoid conventional attacks—in order to remain safely in the "grey areas" that are well below the levels that would trigger conventional kinetic responses. Since hybrid attacks are based in part on communication and information technologies, they can be highly asymmetric, propagate at extremely high speeds, hard to detect and deter, and strike at extremely remote or unexpected targets, while accurate attribution can be difficult or even impossible. In fact, as the Chief of the German Cyber and Information Domain Service, Lieutenant General Ludwig Leinhos, points out, "the problem of attribution often legally prevents a rapid response to cyberattacks," while McAfee Chief Scientist Raj Samani sees that a

A main reason for the migration to cyber is "because it gives nations the capability to have non-repudiation."

[1] Arnaud, Damien, "How the 'Post-Truth' Phenomenon Harms Political Dialogue between States." *The Hague Journal of Diplomacy* Vol. 14 (2019) No. 4. pp. 480-498.

main reason for attackers' migration to cyber is "because it gives nations the capability to have non-repudiation." From the perspective of state actors, this means that "conventional warfare appears more and more inefficient as a means of resolving conflicts" and future conflicts can be expected to be hybrid. George Mason University's Dr. Linton Wells II points out, in fact, that "the center of gravity of future wars may not be tanks and troops…but the minds and resilience of the populations."

Alliances must be redesigned to deal with hybrid threats. In the Black Sea region, Romanian Defense Policy Director Simona Cojocaru says that Russia is employing a hybrid or so-called "non-linear strategy…advocated by [Vice Minister of Defense] General Valery Gerasimov" that relies on "fake news, conspiracy theories, and direct support for political parties with anti-NATO or anti-EU agendas." According to Major General B. Edwin Wilson, U.S. Deputy Assistant Secretary of Defense, "Crimea was cyber-enabled and an example of achieving strategic advantages in a very quick fashion and then trying to hold the norm." According to Ambassador Jiří Šedivý, moreover, Russia may not even be the gravest danger since "China has a much wider variety of instruments available to weaponize information, investments, education, and even entertainment." With such powerful adversaries, dealing with this large range of hybrid threats requires a whole of government approach and coordination with bilateral, regional, and international partners, but many of the existing mechanisms for international cooperation are inadequate. And as McAfee Fellow Raj Samani points out, public-private partnerships are vital because industry has such a large share of the data, but "the reality is that public/private partnerships are nothing more than rhetoric."

Today's alliances including NATO were created to deal with traditional warfare—not hybrid

NATO, for example, tends to focus on defense and foreign ministries and may not be well-equipped or even appropriately mandated to coordinate between different governmental branches of its member and partner governments. The crux of the problem, as General Tatsuhiro Tanaka points out, is that "today's alliances [like NATO] were created to deal with traditional warfare"—not hybrid conflicts. Since strategies to address hybrid threats tend to be "undefined, inconsistent or non-existent," he believes that new partnerships and approaches need to be urgently invented.

Attacks on trust and values are the biggest threats. According to Ambassador Luis de Almeida Sampaio, Russia's "non-linear" attacks on our democracies by "fake news, conspiracy theories, and direct foreign support for political parties" destroy political "trust in the information space [which] is the Achilles's heel of our democratic systems." Panda Security's Jan Lindner also points out that such attacks on our values "occur anonymously, secretly, hidden away in the World Wide Web and perfidiously using our own IT infrastructure." According to Panda Chairman José Sancho, it is clear that "countries like Russia, Iran, or North Korea have an interest in influencing swing voters in elections" and are active right now. At NATO'S Strategic Communications Center of Excellence, its Director, Jānis Sārts, warns that the "checks and balances that were developed with traditional media and within democratic environments are not working." In order to protect our democracies, we need to agree on international norms of State behavior.

Trust in the information space is the Achilles's heel of our democratic systems.

Dealing with diverse threats in an environment of digital smog. According to CISQ's David Norton, we are now "in an environment of digital smog—a combination of volatility, uncertainty, complexity, and ambiguity"—an ideal terrain for hybrid conflicts. Yet, hybrid threats do not arise solely from communication systems or the internet. In the case of energy infrastructure, for example, France's Ingénieur Général des Mines Antoine-Tristan Mocilnikar cautions, "we must not forget to add the old-style threats…sabotage is still very relevant, cheap, and efficient." And CEO Andrea Formenti, founder of Area SpA, points out that the internet even plays a role in such criminal activities as the smuggling of migrants, with the so-called "white

web" that migrants use to get information (and even ratings) on prices and reputations of potential smugglers.

In dealing with such broad threats, NATO's former Deputy Assistant Secretary General Dr. Jamie Shea says that successful crisis management means that you "learn the lessons so that you are going to do better next time." In the case of RTE, France's long-distance electrical transmissions network, Xavier Carton says that one of the most important lessons that they have learned is that "there is a human mistake behind the most successful cyberattacks." For this reason, RTE is training its employees intensively to be aware of phishing and other threats. On the other hand, it is possible to exploit errors that are made by criminals. Colonel Jean-Dominique Nollet, who heads the fight against cyber criminality for the French National Gendarmerie, points out that "nicknames are very important to hackers. Perhaps they used the same nickname 10 years ago on Facebook" with a personal account. If so, it can give the police a way to find them.

Since there is always a human mistake behind cyberattacks, employees must be trained to deal with phishing and similar threats.

Future approaches to hybrid threats. In order to address the challenges of future hybrid conflicts, Dr. Josef Schroefl at the Hybrid Center of Excellence in Helsinki points out that Russia is now testing ways to disconnect from the global internet, so that the only allowable exchange points will be those inside Russia approved by its Roskomnadzor telcom regulator. A different approach is suggested by NATO Assistant Secretary General Dr. Antonio Missiroli, French Defense Innovation Agency's Emmanuel Chiva, and IHEDN's General Jean-Christophe Cardamone: an increased focus on the development of disruptive innovations which, like hybrid approaches, may have great potential. Some of the technologies that might merit special attention could include Artificial Intelligence, 5G, blockchain, digitalization, quantum computing (Google is claiming a major breakthrough with their 53-qubit Sycamore quantum computer), drones (including intelligence uses and swarming), space, hyper-speed weapons, bioengineering, facial recognition, nano technology etc.

To defend against cyberattacks, Russia is testing ways to disconnect from the global internet.

In any case, dealing with "fake news" needs to be one of the highest priorities since it is such a threat to the trust and values that are at the foundation of our democracies. Hopefully AI, coupled with new cyber technologies (or perhaps even quantum computing), can be employed in a way that will limit the harm. Facebook is suddenly at the center of our concerns because it has announced that it will not require politicians to be truthful in their ads, thus opening the door to what may be a vast onslaught of fake news that can be expected to incite hate and violence. Worse, the sources will be anonymous or even disguised. As McAfee's Maurice Cashman warned, this threat shows the need for a responsible ethics policy for all of these new technologies, and Cisco's former Vice President in the Office of the CEO, Don Proctor, says that "Software needs a moral compass" which can be especially relevant "in situations when all the outcomes are bad." Speaking from the perspective of the U.S. State Department, Deputy Coordinator for Cyber Issues Michele Markoff says that "With the new technology like cyber, states needed a way to distinguish what is acceptable state-on-state behavior from what is unacceptable behavior. For the head of the German Cyber Policy coordination staff, Wolfram von Heynitz, norms are especially needed for AI, because "whoever controls data and sets the rules controls the new oil of the 21st century. Along the same lines, General Leinhos says that "the ethics of digital war must be discussed in society as well as in the Bundeswehr."

With new technologies like cyber, states need a way to distinguish acceptable state-on-state behavior from unacceptable behavior.

There is a clear need for action by governments and especially the EU, which must find ways to better defend against Facebook as well as other GAFAM (Google, Amazon, Facebook, Apple and Microsoft) companies. The EU needs to recognize that Europe cannot be master of its fate until there are European companies that are able to operate on an even footing with the GAFAM group. According to Panda Security Chairman José Sancho, "We need to regulate telcos and social and advertising companies related to security or manipulation issues."

According to Panda Security's José Sancho, "We need to regulate telcos and social and advertising companies related to security or manipulation issues."

The Need for Societal Resilience. Above all, we need cyber resilience which, according to Dr. Linton Wells II, "recognizes that your networks are vulnerable, and may be penetrated, but you have to keep operating." For MITRE's Brian Abe, resilience means "to have good backups, to validate the backups and to make sure that the backups are safe, and that your critical systems are backed up and that you know how to restore them." Estonia's Colonel Jaak Tarien has an organizational perspective, saying that "training of people of all levels is key, and this is what we refer to in Estonia as basic cyber hygiene." And his predecessor as the Director of the NATO Cooperative Cyber Defense Center of Excellence, Estonia, Ms. Merle Maigre, says, "to get people genuinely worrying about their cyber hygiene, you need to change their attitudes and mindsets." Achieving all of this on the necessary national and international scales is what brings *societal resilience.* Czech Ambassador Jiří Šedivý believes this to be the key to dealing with hybrid war and cyber threats, in order to "see in Europe societies that are resilient, and resistant to the efforts of Russia or other external actors."

Postscript – 30 October 2019

A sign of progress. Twitter CEO Jack Dorsey has announced that he will "stop all political advertising on Twitter globally" out of concern for the spread of misleading information "at increasing velocity, sophistication, and overwhelming scale."

Welcoming Remarks

Lieutenant General Patrick Destremau

Director, Institut des hautes études de défense nationale (IHEDN)

Ministers, your excellencies, Mr. chairman, fellow officers, workshop participants: Good morning and welcome to the Invalides.

Thank you for your kind words about Notre Dame. It is true that we saw with sadness a cathedral which is part of our French culture, of our heritage, and of our humanity being attacked by flames. We hope that we will have the opportunity for the cathedral to be restored to the glory that it deserves. We want everyone to be able see this magnificent monument as a place of prayer as well as a part of our culture.

It is with great pleasure that, as director of IHEDN, I welcome you today in Paris for the 35th International Workshop on Global Security, and I salute that number, under the patronage of the Minister of the French Armed Forces, Ms. Florence Parly. The IHEDN is co-organizing this seminar in Paris with Mr. Roger Weissinger-Baylon, the chairman and founder of the Center for Strategic Decision Research.

IHEDN is an inter-ministerial institute. We educate 2,500 civilian and military leaders on strategic issues on international, national, and regional levels, and it is also a tool dedicated to Europe and to European responsibility. This year we are honored to welcome your very distinguished participants, including ministers, ambassadors, chief executive officers and high-ranking generals.

During the workshop, you will be exchanging views for two days on cyber threats and will benefit from the knowledge of the best experts in their fields, so I should not and will not develop further on these subjects.

Cyber defense is a national priority for France and a collective security concern for our partners and allies.

Let me just say that cyber defense constitutes a national priority for France and is a collective security concern for our partners and allies. The cyber domain is unique in that it is man-made, recent, and subject to even more rapid changes than any other domains. Dependence on complex cyber systems for the support of military and economic activities creates new vulnerabilities, even in large states, that can be exploited by state and non-state actors. And cyber information can also become a hard power resource that can do physical damage to physical targets in another country.

Aware of these major issues, the IHEDN has been presenting over the last year a national session on digital sovereignty and cyber security in partnership with the National Institute for Advance Security and Justice Studies.

Before leaving the floor to a distinguished panel, let me introduce you to General Jean-Christophe Cardamone, Deputy Director of the IHEDN, who will also conclude your seminar. I wish you all a fruitful and constructive workshop and a very pleasant stay in Paris.

Opening Address of the 35th International Workshop

Brigadier General Didier Tisseyre

Deputy Cyber Commander, French Ministry of the Armed Forces

On behalf of the Joint Staff of the French Armed Forces and as the French Deputy Cyber Commander, it is a real pleasure to present the opening keynote of this 35th International Workshop. It is an opportunity to share views and experiences on global security. The topic this year is "Global Security in the Age of Hybrid Conflict, Cyber Threats and Cyber Influenced Operations," which is a very timely subject. Cyber fits well with the theme of hybrid conflict.

First, let us define what hybrid means. Hybrid warfare may correspond to a threat, strategy or course of action. It is adapted to the modern world—globalization, competition between groups of states that are interdependent, and the importance of information and communication technologies. In one form or another, states are in hybrid confrontation with their competitors or adversaries, while conventional war appears more and more inefficient as a means of resolving conflicts.

States are in hybrid confrontation, since conventional war appears increasingly inefficient as a means of resolving conflicts.

These hybrid strategies are invariably used in the peace-crisis-war continuum. Actors on the international scene employ different levels based on their respective objectives, for example, territorial gain, control over resources, economic domination, state disorganization, intimidation or support of minorities, or regional dominance and influence. When there is inter-governmental tension, they rely on deceit and intimidation.

A hybrid strategy is meant to remain ambiguous and to achieve the desired end-state at the lowest possible cost by combining means of action and by using ad hoc asymmetries such as motivation and the perception of stakes, public opinion, technological means, opposition between long-term vision and immediacy etc. Powerful emergent organizations without governmental status recognized by the international community take advantage of the various existing grey areas and intergovernmental divisions. They may also develop a hybrid strategy by using courses of action that differ from those of a state that is integrated into the international community.

Hybrid strategies provide ambiguity by using asymmetries like motivation and public perception.

The objective of a hybrid conflict is to weaken the adversary, erode its will, prevent the rise of an extreme situation that would result from an asymmetrical armed conflict and limit its impact. It combines military and non-military action; it has conventional/non-conventional actions and non-military levels of action. Conventional actions are military actions carried out with the means of the conventional forces of the army, air force and navy. Non-conventional action includes military action

conducted by the special forces, supplemented strategic forces, chemical, biological, radiological and nuclear (CBRN) defense capabilities and action conducted by paramilitary forces.

A hybrid conflict relies in particular on cyberspace, dual-use capabilities, supported proxies, covert or special forces, or C2 network and special capabilities. It operates in the information and economic spheres and it uses all the possible methods in the diplomatic and legal areas.

A hybrid conflict may be broken down into several activities that are conducted either in parallel or successively based on the context and objectives: Shaping of the international community through social networks, for instance, and strengthening of international support, preparation of full cyberattacks, forceful actions, maintaining gains and holding positions, standardization and legitimization, intelligence, cyber capabilities, influence strategies and actions on perceptions, economic and infrastructure security, shaping of the environment, cooperation policies, strategic mobility, targeting capabilities, special forces and rapid intervention forces, secure communication, information and command means, control of possible proxies, and exploitation of possible vulnerabilities. So, the scope is very large.

Countering a hybrid strategy requires understanding the adversary's intent, a counterstrategy, and being resilient.

Countering this type of strategy requires detecting and understanding the adversary's intent: Building a comprehensive and proactive counterstrategy to anticipate or retake the initiative, being resilient and responsive and readjusting the asymmetries sought by the adversary. The objective is to mobilize a large range of capabilities and levers of action and ensure unity of action with the use of complementary forces. The availability of social media and the use of cyberspace and psychology have created a number of new opportunities which perfectly support hybrid conflicts. There is no longer a clear distinction between peace, crisis, and war.

What is a cyber incident and what is a cyberattack? It is difficult to characterize them. We need to build a common grid, a common layer to characterize cyber activities. Hybrid conflict with the use of cyber influence and attacks changes the concept of self-defense and collective defense. This is a new reality and we have to face it.

So, how could we live with that? Cybersecurity has become a general and serious concern for all: Citizens, professionals, politicians and, more generally, all decision-makers. To preserve our freedom of action and sovereignty, we must protect ourselves against cybersecurity attacks with both preventive and reactive measures. It is especially difficult because cyberattacks may be conducted by several actors for many reasons— by criminals, or by states, for industrial espionage, to cause economic damage, to apply pressure, or to inflict real damage on infrastructures as an act of war. States and their interconnected critical infrastructures are vulnerable. Cyberattacks also put companies of all sizes at high risk. The economic damage caused by successful cyberattacks may be considerable. However, our protection level is still considered largely insufficient compared to the risk and potential damages.

Most recent power struggles, crises and conflict have been developed in cyberspace.

Cyber is a new reality and we have to face it. France is a nuclear and conventional power, a permanent member of the United Nations Security Council, a member of NATO and the EU. To protect its freedom of action, autonomous decision-making, its sovereignty and social values, France has also chosen to develop its cyber defense capabilities.

Cyber is a threat but also an opportunity. Most recent power struggles, crises and conflict have been developed in cyberspace. The armed forces must, from now on, systematically consider cyber combat as a full mode of action, whose effects must be combined in a global maneuver. As a true technological breakthrough, the cyber weapon is designed to upset the terms and conditions of warfare without renewing its principle in depth.

Multiple state actors (concealed or not), terrorist organizations, unmarked borders, confused perceptions, false references, rapid propagation of threats, unenforced international laws and disregarded codes of conduct are the risks of cyberspace. It is a shady, foggy area which affects us all as individuals, sometimes with devastating effects. The combat in cyberspace is asymmetrical, hybrid, sometimes invisible and apparently painless. Nonetheless, the use of cyber weapons is likely to seriously interfere with the capabilities and the sovereign interests of states.

The risks of cyberspace include multiple state actors, terrorist organizations, rapid propagation of threats, unenforced codes of conduct.

In France, the cyber defense strategy review, published in February 2018, confirms the relevance of all models of organization and governance which separate the offensive mission and capabilities from the defensive mission and capabilities. It has proposed a full spectrum strategy in this area by structuring the cyber defense organization around a cyber crisis interagency coordination center. This center is overseen by the defense and national security secretariat general, under the authority of the prime minister. It has four distinct operational chains: protection, intelligence, judicial investigation chains and, in addition, a military action chain which deals with offensive cyberspace operations (OCOs).

COMCYBER has the authority to use offensive cyber military capabilities, an integral part of our armed forces

The Cyberdefense command (COMCYBER), is responsible for military cyber defense. It covers the full spectrum of defensive and offensive actions conducted in cyberspace to guarantee the efficient running of the Ministry of the Armed forces and the efficiency of the armed forces in the preparation, planning and conducting of military operations. The ministry now has at its disposal capabilities as well as an employment doctrine covering the offensive cyber operation dedicated to the engagement of its armed forces. Its aim is to get operational advantages in the theatres of engagement of our armed forces and counter operations against information manipulation harmful to our military operations. Under the authority of the Chief of Defense Staff, COMCYBER has the authority to use offensive cyber military capabilities, an integral part of our armed force operational chain in perfect relevance with our organization and our organizational structure.

Cyber operations can be conducted independently or in combination with conventional military assets. In strict compliance with international laws, which is very important, the cyber weapon seeks to produce effects against a hostile system in order to alter the availability or confidentiality of data.

The various effects of the military offensive operation and the corresponding courses of action are derived from the nature of cyberspace and its three-layer structure—physical layer, logical layer, and semantic, cognitive or social layer. The use of offensive cyber operations has its own unique rhythm. If these effects can be fully routine, their integration in the global operation maneuver is a process characterized by a lengthy and very specific planning. The effects can be material in nature—as for a weapons system—or immaterial as for collection of intelligence. They can be temporary, reversible or final. They can be used as a substitute for or in combination with other capabilities for action through the whole spectrum of military engagement to inform, to defend, to act.

OCOs are used at the strategic level in the joint global operation maneuver as well at the tactical level in the maneuver of the armed forces components in the theatre of operations. The OCO operations are conducted by specialized units whose expertise includes risk analysis and the control of all the collateral or even fratricidal effects induced by the complexity of the fields.

Under the orders of the French COMCYBER, the use of OCOs requires the control of all the political, judicial and military risks throughout all the stages of the operation. Like any military operation, OCO implies an acceptance of the risk by the decision-making echelon, determined by the principle of *jus in bello:* proportionality, differentiation, discrimination, and in consideration of the cost-effectiveness ratio, the operational situation and the overall political context.

Offense cyber operations (OCO) must abide by the principles and rules of international law, including humanitarian law.

The risks associated with the use of OCOs arise in the first place from the unknown characteristics of cyberspace, immediate action, duality of targets and hyper connectivity. Any OCO must abide, like any other war weapon or method, by the principles and rules of international law—I say it many times—especially the humanitarian international law, and national laws and regulations. Therefore, it is only used in compliance with very restrictive operational rules of engagement. Besides, the sophisticated assets and courses of action conceived in view of conducting actions require a strict mastery and control over values from beginning to end, especially to avoid any risk of diversion, compromise or collateral damage. The OCOs rely on sensitive know-how and constitute one of the attributes of a sovereign defense.

The decision to make an OCO public must be weighed against the risks, including the vulnerability of highly digitized national assets.

These two dimensions require a strategic control over the OCO operations, their planning as well as their implementation. In order to preserve its efficiency and to control the risks of diversions, the whole spectrum of OCO connectivity by our armed forces remains secret. Nonetheless, political as well as military officials can, according to circumstances, assume them publicly or even claim them. This posture is a matter of political decision. The decision to make an OCO public must, in fine, be weighed against the risk associated with the inherent vulnerability of our highly digitized national assets.

As a conclusion, I will say that hybrid conflicts are now a reality and we must all work together to find the best way to face these new threats. And although we are considering that cyber could be a threat, it could also be an opportunity. Many states view cyber as a new way of fighting against threats, and we have to use it in its full spectrum. But, of course, as I said and you have heard our friends say, we are conducting offensive cyber operations, but in a very strict manner and its use is very carefully structured.

The Effects of Digitization on Armed Forces

Lieutenant General Ludwig Leinhos

Chief of the German Cyber and Information Domain Service

Digitization is the central issue of our time and one could even call it, as our minister does, the megatrend of the 21st Century. It makes enormous improvements and innovations possible, including for armed forces. But it also brings considerable risks and dependencies across national borders and may affect all of us, be they states, governments, societies, business, enterprises or individuals. Therefore, protection against the risks from cyber and information space is of strategic importance and is a matter of national concern.

Cyberattacks against states, business enterprises, critical infrastructures and private households, have long been a reality. Even low-level cyberattacks may cause economic damage running into billions. But in addition to classical cyberattacks, activities in the information environment such as fake news campaigns aimed at creating unrest are often used to destabilize fundamental democratic structures. And we have seen examples of these kinds of activities.

Conflicts between states are increasingly susceptible to the influence of propaganda and disinformation.

It is not just the technology itself that we need to consider here, but also what it is used for. Conflicts between states or intra-state conflicts are increasingly susceptible to the influence of propaganda and disinformation. Therefore, information is becoming a core resource of the future. In my presentation, I will primarily address these aspects from a military point of view.

In Germany, we established a new service which is on an equal footing with the classical services, air force, navy, and army. Called the Cyber and Information Domain Service, it was inaugurated on 1 April 2017. It has centralized capabilities that already existed in the Bundeswehr and we are continuously improving and strengthening them. It currently comprises roughly about 14,500 soldiers and civilian employees. In this way, the Bundeswehr makes an effective contribution to national security as well.

In cyberspace, physical effects can be achieved—even tens of thousands of kilometers away.

As early as 2016, at its Warsaw Summit, NATO recognized cyberspace as an independent military domain similar to the traditional domains of land, air, sea and space. In cyberspace, armed forces can reconnoiter and/or engage enemy systems by means of software, which differs from the classical spaces. In practical terms, this could mean interruption of logistic chains, or the modification of data crucial to enemy operations. The paralyzation of command and control and information systems would also be an option. Thus, cyberspace can be used to influence enemy capabilities and to prevent them from implementing their plans.

By including the information space, the Bundeswehr has defined this new military dimension in a more comprehensive way than NATO does. Information is the central aspect. It is perceived, interpreted and disseminated by human beings. What is called "published opinion," for example, is an integral part of it.

So, what are the characteristics of cyber and information space from a military point of view? What distinguishes the military dimension of cyber and information space from traditional domains? Cyber and information space is characterized by a high degree of complexity and the territoriality is complemented by virtual reality. Cyber and information space cannot be divided into combat sectors with clear spatial boundaries. The same is true for the maneuvering of troops.

But do not be fooled by the term virtual. In cyber and information space too, physical effects can be achieved, and the place where cyber and information domain operations create an effect can theoretically be tens of thousands of kilometers away. That is also different from the classical domains. Time, too, has a different meaning in cyber and information space. For example, an effect can be achieved across any distance without any delay; effects can be and are achieved in real time.

By now, the possibilities of digitization have made it feasible for non-state actors to achieve effects using cyberattacks, which previously could only be achieved by state actors. This is specifically true for international terrorism and also for organized criminals.

Moreover, thanks to these technical possibilities, actions can be concealed extremely well. This makes the attribution of attacks particularly problematic. There are many potential perpetrator groups and motives.

As a result of digitization, large-scale kinetic war is probably not the most likely scenario for the future.

In conclusion, the threat situation has become much more complicated and this is a result of digitization. This also has an effect on the most probable future conflict scenarios between highly digitized states. They will technically be characterized by digitization, artificial intelligence and autonomous systems. So, in consequence, a large-scale kinetic war is probably not the most likely scenario for the future.

We will now look at these hybrid scenarios.

Conventional military forces must, of course, still be available in sufficient numbers and quality, primarily to ensure credible deterrence. But the hybrid scenario is playing an increasingly decisive role. Hybridity is possible without and in connection with the application of traditional military force, as could be observed in Crimea, for example. These kinds of strategies involve particular challenges. They use legal vacuums created by technological progress, and they take advantage of unclear responsibilities, for example, the distinction between internal and external security. Usually, they remain below the threshold of traditional warfare. This does not mean, however, that they are not violent.

The problem of attribution often legally prevents a rapid response to cyberattacks.

As long as we are not in a state of defense, the problem of attribution, already mentioned before, often legally prevents a rapid response to cyberattacks. A problem that also has to be addressed.

The core task of the Cyber and Information Domain Service is the protection of the Bundeswehr IT systems. In the event of alliance or national defense, binding international regulations applying to armed conflicts between states must also be applied to cyber and information space. Here, the ethical standards which have already proven effective as a basis for international law could serve as guideline. Since 2017, we have a regulatory framework with the Tallinn Manual 2.0 that is not binding, but a good basis in this context.

Digitization does not mean IT support for existing processes…but rather their adaptation and optimization.

Let me say a few words on national and international cooperation as a precondition for protecting ourselves against the challenges posed by digitization. The internet knows no borders. In addition, hybrid strategies exploit interfaces between responsibilities, for instance, internal/external security, as I just mentioned. Therefore, it is indispensable that we close ranks and share knowledge at the national and international level. In this context, the National Cyber Security Centre, the first forum to promote the cooperation of government agencies in the cyber and information domain was established under the direction of the Federal Office for Information Security in 2011. The development of a National Cyber Security Centre into an inter-ministerial and operational institution is essential for Germany's future capacity to act in this field. We also consider the involvement of national internet service providers as indispensable.

Since hybrid strategies exploit interfaces between internal/external security, it is indispensable to share knowledge.

As a representative of the Bundeswehr, the Cyber and Information Domain Service actively contributes in this context. Among other things, we provide information through our new Cyber and Information Domain Situation Centre. It is a fusion center where we bring together all relevant situation pictures contributing to the Cyber and Information Domain. Our headquarters are also taking advantage of our location in Bonn as we have concluded first cooperation agreements with science and business institutions. For example, we cooperate with the German telecommunications company, Telekom, and have formed an alliance for IT security with the Fraunhofer Institute for communication, information processing, and ergonomics.

This cooperation encompasses mutual information exchange and knowledge transfer, exchange of personnel as part of job-shadowing in the partner institution and the mutual opening and support of basic and advanced training programs for IT specialists, activities that benefit both sides. Furthermore, the Cyber and Information Domain Service headquarters is a member of what we call the advisory board of the Cyber Security Cluster Bonn, an association which was founded at the end of last year and is hosting today's high-level events.

Digitization also has a severe impact on the military in other areas, not just in the technical areas, but also on organization and processes, command and control, training and corporate culture. The Bundeswehr will, of course, use the advantage offered by digitization. Besides command and control and weapons systems, other potential applications can be found in the fields of personnel and energy management and in the preparation of situation pictures and forecasts. And, of course, we are benefitting from all the advantages in the medical area, inhuman resources, and in a lot of other domains.

The integration of modern information technology into the military planning and decision-making process also has a formative impact on the operations of modern armed forces. Let me address some consequences for organizational processes. Organizational methods must be adapted to the demands on and the requirements of armed forces operating in the information environment.

Digitization does not mean "IT support for existing processes" although we quite often think in that way, but rather the adaptation and optimization of processes based on the possibilities offered by digital means. We need new strategies as a collective national response to the hybrid conflict scenarios that I have described before. In other words, the "digital state of defense" must be taken into account as a possible scenario. In addition, the ethics of digital war must be discussed in society as well as in the Bundeswehr. One of the questions is: who makes life-and-death decisions?

Consequences must also be drawn for the field of command and control. Command and control structures and procedures must be reviewed and adapted. A comprehensive situation picture and automated recommendations for action will be established at higher command levels. When it comes to issuing and implementing orders, certain intermediate levels will probably not have the same role as before or may even no longer be needed. So, in general, we have to ask ourselves a lot of questions. Are the tools and procedures of former times still suitable today? Do modern tools like, for example, design thinking, offer alternative approaches, in the military domain as well?

The ethics of digital war must be discussed in society as well as in the Bundeswehr.

This leads to other consequences for the field of training and corporate culture. Certainly, digitization will change the military profession. A digital corporate culture is required in the armed forces. The main factor here is the creation of cyber awareness among all members of these forces. A cybersecurity culture has to be developed. The qualification requirements have also changed. This must be taken into account in the area of command and control. And we must allow innovative thinking and reflect upon it. It must not be suppressed by pressure to conform.

We must accept quick cross-hierarchical communication and put it into practice. The young generation is more network oriented and the military is a classical hierarchic organization, so this thinking about where the young generation is coming from must be reflected in our means and mechanisms.

Of course, the armed forces must become more flexible in the areas of personnel recruitment and career paths in order to be able to recruit and retain the talents we urgently need. In this respect, we also need to establish a dialogue with industry and science. That is of crucial importance because we are all looking for the same skills, for the same kind of people and it is a challenge for the whole of society.

In conclusion, digitization has already had a decisive impact on the Bundeswehr and will have even more in the future with associated challenges that require new solutions and new ways of thinking in many fields. We, as the Cyber and Information Domain Services, see ourselves as the driving force for the further development of the Bundeswehr in the context of this digitization. Even beyond the technology area, we have already taken new innovative paths and we act as pioneers in a number of fields for the entire Bundeswehr. We are also contributing to national cybersecurity in a whole of government approach. To do so, we cooperate closely

with our national and international partners. Only together will we be able to successfully respond to the threats from cyber and information space, which is a precondition for the future of modern societies.

Dealing with Hybrid Threats: a NATO Perspective

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

I will focus on what we tend to define as a new set of threats that linger upon us as an alliance, individual allies, and like-minded countries. It is what we conceptualize as 'hybrid' threats or campaigns. First, the beginning, or the restart, of the discussion on 'hybrid' dates back to the notion of hybrid *warfare*, which is distinct from hybrid *threats* or *campaigns*. Hybrid warfare, which is in essence not a new concept, became fashionable again some 10/12 years ago, interestingly, in the aftermath of the 2006 conflict between Hezbollah and Israel in Lebanon, where the kind of tactics that Hezbollah used on the ground against Israel were defined as 'hybrid' warfare, combining conventional and unconventional tactics to great effect.

Then, when Ukraine occurred in 2014, the notion of hybrid warfare was also applied to the way in which Russia carried out the operation in Crimea, but also, to some extent, to the kind of subversive activities that it fomented and supported in the Donbass region. Interestingly, the Russian side tends to reject the application of the notion of hybrid warfare to what they did in Ukraine, and to claim instead that the West that used such tactics in Ukraine and elsewhere.

Russia's General Gerasimov defines non-linear warfare as a new way of conducting war in the 21st century.

There is a precedent in doctrine. General Valery Gerasimov, who is currently the chief of staff for the Russian army, wrote a few years ago a number of articles in which he defined 'non-linear' warfare as the new way of engaging in conflict in the 21st century.

Yet, the term 'hybrid' has now become common currency. You find it in official NATO documents—from the Strategy on countering hybrid warfare (2015) to the Brussels Summit communiqué from July 2018. We keep talking about hybrid campaigns, hybrid tactics, hybrid threats, and we have also gone as far as to say that, on certain conditions, hybrid campaigns and hybrid attacks or malicious hybrid activities, can lead to the invocation of Article 5.

As you know, the only case in which that happened so far was in 2001 after 9/11, following a terrorist attack. In Wales (2014), Allies also agreed that Article 5 could be invoked in the event of a cyberattack. Now hybrid attacks, too, can lead to the invocation of Article 5. But when we talk about 'hybrid' threats or campaigns, we also acknowledge to some extent that these hostile activities tend to be below the level of armed conflict, below the level of warfare proper, and below the level of invocation of Article 5. Such activities are carried out—mostly—through cyberspace, and they are cyber-enabled.

However, not every hostile activity is a hybrid activity. The notion of hybrid applies, in principle, only when a number of criteria are met.

There is no agreed definition so far of what a hybrid campaign or threat is like, but there is a broad common understanding that hybrid activities entail combined, coordinated, simultaneous hostile actions carried out by a single actor or set of actors; and that they are scalable operations, both horizontally and vertically. In other words, they could be expanded to other areas and/or escalated or de-escalated, depending also on the response (or lack thereof) from the opposing side.

Hybrid threats and campaigns are hard to detect, deter, and attribute because they tend to be carried out through cyberspace.

Furthermore, hostile hybrid activities are, by nature and definition, tailored and targeted: they are directed at pre-identified or alleged vulnerabilities of certain actors and, therefore, they tend to vary in scope and intensity. There may be common ingredients, but they tend to differ according to where, when, and how they are mixed and used. To some extent, they are like mutants, for instance the character of Dark Phoenix in the Marvel series 'X-Men': their appearance depends on the context in Last but certainly not least, hybrid threats and campaigns are hard to detect, hard to deter and hard to attribute. Paraphrasing von Clausewitz, not only is the 'fog of war' thicker here than anywhere else, but some analysts are starting to talk about such hybrid tactics as "war by other means," i.e. waging conflict and undermining an adversary by using unconventional techniques that do not amount to the traditional features and rules of direct confrontation or warfare—and that are, ultimately, also deniable by the perpetrator.

General David Petraeus, former Director of the CIA and U.S. commander in Iraq, famously spoke of "the weaponization of everything." And to some extent the term 'hybrid' can be used also with reference to the fight against terrorism: it was indeed applied to the way in which Daesh conquered territory across Iraq and Syria for its 'Caliphate' in 2015—although terrorist groups tend to (over-)claim, rather than deny, their operations.

General David Petraeus, former Director of the CIA, spoke of "the weaponization of everything."

The term 'hybrid' is surely a bit fashionable, but it is also a catch-all concept that is useful in order to capture this new reality that is becoming "the new normal" for most of our countries. It is about old activities by new means and in new formats. It is also about disinformation—some people prefer to talk about *mis*information— and more broadly about activities aimed at destabilization and disruption (electoral interference could also be considered as either part or a variation of these); at corruption and coercion ("elite capture", as it is sometimes defined); traditional espionage, albeit carried out through new technologies, and also sabotage.

As you know all too well, espionage is not banned by international law—although it can be prosecuted by law enforcement domestically—whereas sabotage could be a *casus belli*, it could lead to conflict. Cyber-enabled techniques, however, tend to blur the dividing lines between, for instance, infiltration of a network for reconnaissance/intelligence purposes (espionage) and exploitation and manipulation of data (sabotage). This is precisely why 'hybrid' is so fashionable, why it is becoming so common, and why it is so worrying.

NATO can assist our own allies with targeted intelligence, early warning, and by flagging up what we know that perhaps they do not.

Who are the first responders against hostile hybrid activities? The nation states are the first line of response in this particular domain. Next is the private sector. Precisely because of the nature of the tools used in hybrid campaigns, the private sector is an

important actor: cyberspace is mostly privately owned and operated, and without some form of cooperation with the private sector it is going to be very difficult to act in that field. Just think of the financial world, or think about critical infrastructure (energy, transport and communication): good cooperation between public and private actors in this field is truly essential.

And, since I am representing NATO at this workshop, what is the role of NATO? NATO plays a limited role, and in three main areas. One is what we call situational awareness: we can assist our own allies (and also our partners) with targeted intelligence, early warning, and by flagging up what we know that perhaps they do not know, about what is happening and what they should pay attention to.

The second area is support: we can support the members of the Alliance, and potentially also our partners. In particular, we can assist them —on request—with what we call Counter Hybrid Support Teams (CHST), which have been launched in July 2018. We have now assembled a group of national experts, appointed by the individual allies, that cover a wide range of expertise (from strategic communications to the management of critical infrastructure, from cyber to intelligence proper), and we are preparing ourselves to mobilize them and deploy them to those individual allies who may ask for that support. At least one ally, namely Montenegro, is asking for assistance—especially in terms of training, exercises and setting up appropriate governance structures - in countering hybrid threats to which it feels particularly vulnerable and exposed.

We are assisting Montenegro in training, exercises, and setting up appropriate governance structures in countering hybrid threats.

The third area of NATO commitment is solidarity. I mentioned earlier on the possible invocation of Article 5: that is the way in which NATO expresses its political solidarity and could act as a potential deterrent vis a vis possible initiators of hybrid campaigns.

Yet the challenge with deterrence, detection and attribution remains. It is even more acute and complex in cyber security and defense as the spectrum of domains in which hybrid campaigns can be carried out is so wide and diverse that it is even more difficult to come up with a single set of practices for detection and attribution—not to mention deterrence.

Defense against hybrid threats is about risk management, risk mitigation, and building resilience.

Basically, defense against hybrid threats is about risk management, risk mitigation, and building resilience. I heard the previous panel talk about resilience and I think that is what the game is all about. We are increasingly waking up to these risks and to our vulnerabilities. Even political leaders in individual allied countries are starting to realize that hybrid threats are not simply a traditional security issue. They can also affect the integrity of our democratic systems, our institutional structures, and their legitimacy. This is a good starting point in order to be able to develop adequate responses.

However, there may be a few no-go areas, where we cannot and would not go. Let me mention some.

First, we do not really want to 'mirror' the behavior of our opponents and adversaries. We do not want to act 'tit for tat', to apply the same tactics that they use against us. We do not intend to respond in kind, in other

words. As a result, therefore, there are limits to what we can and will do. We want to preserve the integrity of our democratic societies and systems. We want to act in full respect of international law. We do not want to restrict our own freedoms internally, be it freedom of expression, a functioning market, or the media environment.

Also, this is not an area where we can easily apply the traditional tools of arms control: in fact, how can one control the 'weapons,' especially since we 'wear' and use them ourselves, starting with our smartphones? How can one do 'inspections' of virtual stockpiles, or limit algorithms?

Our societies are open societies: we want to keep them that way, but they are also more vulnerable than others.

This is indeed a particularly demanding field, i.e. because our societies are open societies: we want to keep them that way, but as such they are also more vulnerable than others. We have started seeing this over the past couple of years, especially on the occasion of elections and referendums—that are quintessential catalysts for these types of hybrid campaigns.

NATO has a number of instruments to address all these challenges, but it is far from having all. NATO people use a lot of acronyms, but DIMEFIL is not a prerogative of NATO. It encapsulates the different tools that can be used in response to 'hybrid' activities: diplomatic, information, military, economic, financial, intelligence, and legal. NATO does not have all these instruments in its arsenal, but it cooperates with other international organizations—in particular the EU (for its regulatory capabilities)—with a view to upholding a rules-based international order and protecting our societies.

Hybrid War and Hybrid Threats

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

As the Deputy Assistant Secretary of Defence for Cyber Policy, I am going to give you a U.S. perspective on hybrid warfare and hybrid threats. I think these comments will mesh well with the previous panel as well as with Antonio Missiroli's remarks.

We have been on a journey for some time now in the United States. We have recognized some shortcomings in our current and previous strategies and made fundamental adjustments. 2018 was a very busy year for the Department of Defense (DoD), but also for the nation at large. We made some monumental decisions and changed some strategies as I just mentioned, legal frameworks, and processes on how we make decisions internal to the U.S. government.

Our adversaries are using techniques that really cut across the diplomatic, information, military, economic, or legal constructs (DIME).

I thought I would share what motivated our behavior: it was a recognition that strategic advantage was being lost against some of our revisionist countries. We are definitely in a real competition with revisionist powers that are seeking to change the world dynamic. They are operating, as Antonio Missiroli highlighted, short of our traditional thresholds for response. They are using techniques that really cut across all dimensions of power, including the diplomatic, information, military, economic, or legal constructs (DIME)[2]. These techniques move across all of them, so they are hard to recognize at times, and they can be hard to counter. From a military perspective, they also move across multiple domains of warfare, and especially cyber-enabled ones.

At the Department of Defense, we have seen some of these effects building and have recognized that we have begun to lose some of our military strategic advantage. It has not been a one-time event. It has been an erosion over time, across several areas, and I will walk you through that. These techniques are being used as overt challenges to the free and open international order and institutions on the world stage that we have relied on for stability. These countries are trying to undercut those institutions while seeking to gain tactical advantage; Crimea would be an example of being able to achieve strategic advantages in a very quick fashion and then trying to hold the norm. It was cyber-enabled early in the conflict.

Crimea was cyber-enabled and an example of achieving strategic advantages in a very quick fashion and then trying to hold the norm.

With an erosion of some of our military advantages, we have also seen activity that threatens critical infrastructure around the world, and the energy sector in the United States. There have been indications of threats in the financial sectors in the past. Some are in the form of fake news, since we identify election

2 The diplomatic, information, military, economic, or legal constructs of national power are often referred to as the DIME model.

security as critical infrastructure. There were serious threats to erode election security not only in 2016 but again in our 2018 mid-term elections. We have seen it across almost all the countries represented in this room, and that is in addition to trying to reduce economic prosperity across many of these nations.

Our military response has been to step back, do a large assessment with our interagency partners inside the U.S. government and strive to make a couple of significant changes. The first was to start modifying the strategy that we would work from, especially within the Department of Defense and including our cyber strategy.

In 2018, there was a more proactive U.S. stance on the world stage, militarily—because of the strategic advantages that we have been losing.

We published a new strategy in mid-August last year. If I were to contrast it with the 2015 DoD cyber strategy, I would say that our 2015 strategy was about building capacity and capabilities as well as being fairly reactive, in order to minimize the risk of escalation to the maximum possible extent. In 2018, you see a much more proactive U.S. stance on the world stage, as viewed through a military lens. Why do we do that? It is because of the strategic advantages that are being lost. We see militaries being leveraged for hybrid warfare tactics on the world stage. We have been reluctant to bring the U.S. military into this conflict, but we now see that as necessary because we have a unique ability to scale and scope solutions from the Department of Defense.

In addition, we have outlined five key mission areas. Some were to gain clarity on issues internal to the Department of Defense but also on our role with regards to helping defend the homeland, principally critical infrastructure within the country. I think we have improved over the lack of clarity that we had earlier. Walking very briefly through the big missions, some will strike you as normal:

1. To be able to operate in a cyber contested environment as a U.S. military alongside our allies and partners when required.

2. To be able to bring offensive and defensive cyber enabled capabilities into our joint fight, the joint force structure. This is natural and what you would expect.

3. To be able to defend, help to defend, and to secure and defend our critical infrastructure in the United States. This third mission recognizes that the Department of Defense did play a role with regards to defending the homeland. We must be able to defend energy systems, finance systems, and transportation nodes (especially those that are being used by the military for projection of force but also in defense of the homeland).

We do not do the FBI's job, but we provide support when required, like information sharing, or collecting intelligence.

We defend the homeland in all domains, there is no exception in cyberspace and so, the Department of Defense has a role. We work through the clarity of what that means. Sometimes, people hear the term 'defend forward.' That was our attempt to clarify our role internal to the United States: we do not do the Department of Homeland Security's job, we do not do the FBI's job, but we provide support when required. That may be in the form of information sharing based on activities we execute around the world. It may be collecting appropriate intelligence that we would share with our other agencies to be able to better defend. It may involve sharing with our allies and partners, and

also to be able to mitigate threats forward to the best of our ability. If we see imminent threats on our critical infrastructure, we will work with partner nations to be able to mitigate them. On the other hand, if it is an imminent threat of a significant scale and scope, the Department of Defense may be called upon to take appropriate action, just like we do in any other domain. This is now really aligned and normalized for us.

4. To be able to protect information, not just in DoD networks. It has always been our traditional role; we do that very well, but we must also be able to defend and help secure information associated with national security systems that are in development and our defense industrial base. So, we are playing a much more proactive role with regards to defending that particular critical infrastructure segment.

5. Our last mission is partnerships. Partnerships are key, and international partnerships are at the front of the line. We see that as one of the strengths, especially when countering hybrid warfare or hybrid techniques. To be able to operate together in coalitions of like-minded nations is a strategic advantage. And that is one of the reasons that coalitions are a target. The goal is to undermine them and the other international structures in place.

As to industry, we want to partner very strongly with industry as well as our interagency partners internal to the United States. The mechanisms have been put in place to build structures of deterrence and, as in any deterrent construct, you want to be able to deny benefit to a military adversary. That is what you see in terms of making our military capabilities more robust and being able to weather and fight some of these activities that are happening around the world. At the same time, we want to be able to deliver consequences when international norms, especially during peacetime, are being breached.

We changed the U.S. Code section 132 so we can now take both defensive and offensive actions in a clandestine manner.

This is an overview of our strategy. We also worked with Congress to make a couple of legal changes in the United States. Since such changes are often at the end of the list, we actually put them at the front.

- We gained clarity in terms the role of the Department of Defense, what we describe as traditional military activity. We changed the U.S. Code related to the Department of Defense to clarify that we can take both defensive and offensive actions in a clandestine manner. In particular, section 1632 of the Code was changed and that was very monumental for the nation. Since we had not changed that in eight, nine, or 10 years, it was a significant step for us.
- We gained some unique changes in our ability to do security cooperation in a much more agile fashion. We saw that as one of the bedrock capabilities that we needed to be able to reach out and work in partnership internationally.
- We worked really hard across our U.S. government for about a year to lay in place the ability to make decisions at a pace that matches the need. So, a new National Security Presidential Memorandum 13 is out. It allows us to match the pace of some of these threats, to really make decisions at the speed of relevance, to be transparent in that nature, and to do it in a very risk informed manner. This is probably a unique step for us. We have often done things inside the Department of Defense only; now we are much more transparent when working with interagency partners to understand the effects that might be delivered.

All this is an absolute must, a "must do," and a "must deliver" for this new environment that we are operating in. It is much more sophisticated; it operates at a pace within the cyber-enabled activities that we have never seen in history; have we ever seen a time where a threat moved at this type of pace sophistication and proliferation? As a military member and a student of warfare, there is nothing that matches it in my book.

We now have some structures of deterrence that are put in place, and the few operations we have executed so far seem to be providing the right kind of deterrent structures that we had in mind. Our reviews on some recent activities show that they have been very successful.

We will continue focusing on malign cyber actors—to impose costs for those that are breaching norms of behavior or if we are in a form of conflict.

We will continue our focus on the malign cyber actors. We want to impose costs appropriately for those actors that are breaching norms of behavior during peacetime and if we are in a form of conflict. That is our job in the military to be able to operate in any spectrum of conflict, high-end conflict or very low-end conflict. But what we are seeing is activity during peacetime in a hybrid fashion that Antonio described very well. That is creating a lot of strategic disadvantage for many of us.

The other objective is to be able to deny those benefits to our adversaries, and that is where, I think, industry bears such a heavy load: to be able to weather the storm, to be more robust, and to be more resilient as we operate. The threat is real and as we all know. It is a challenge, but I think it is also an opportunity, especially on the world stage. We see international coalitions as really one of the bedrocks and we want to put the right kind of structures in place to push back in a deterrent fashion.

As Jan Lindner highlighted, modernization is key. Cybersecurity has to be part of that modernization.

The other opportunity, of which we really need to be mindful as we move forward, will require modernization, as Jan Lindner highlighted during his talk. Modernization is key, and I think as our nations begin to modernize, whether it is in their military, cybersecurity has to be part of that modernization. At times, we try to leap forward to bring in new functionality, new capability, new lethality but we forget and leave behind the cybersecurity. In today's environment, that's a fool's investment. So, we see a balance in being able to modernize and bring cybersecurity along for this ride.

The Hybrid Threat in the Black Sea Area

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

Hybrid and cyber threats can no longer be seen as merely emergent or emerging. We entered this new reality some time ago and discovered that we are insufficiently prepared. This raises important questions: Are we formulating policies and setting up tools as fast as the threats and risks are advancing? Are we able to detect the most intractable challenges?

I think the real emerging challenge is the need for institutional and cultural change in order to enable more efficient, effective, and legitimate policy responses. A change in our mindset is necessary. For many, cyber seems like rocket science. On this subject, I had a delightful conversation with Jamie Shea, who gave me his permission to quote him: with former NATO Assistant Secretary General for Emerging Security Challenges, Ambassador Sorin Ducaru, he was visiting an ambassador in order to discuss a cyber issue, but the ambassador replied, "Come on Monday, my technology man is on holiday." This means that we have all to learn more about hybrid and cyber.

Russia is no longer playing softball—after its annexation of Crimea and its invasion of eastern Ukraine.

Hybrid, cyber resilience, and military mobility all have at least one common link. They require a whole of government approach. Moreover, all these efforts need to start at home. We have to adapt and to modernize, as Edwin Wilson has said in his remarks, but we have also to look back in history, since some of today's actions and events look like *déjà vu*.

Now, I would like to speak about the Black Sea. Needless to say, Russia is no longer playing softball. Its behavior is coherent and comprehensive. So, it is very important to achieve coherence between the actions of governments, companies, and the private sector including think tanks. We are five years away from Russia's annexation of Crimea and its invasion of eastern Ukraine in 2014, which brought NATO back to Europe and to the task of collective defense.

This is quite a change from the time of cooperation between NATO and Russia, which I remember from early in my career. It is now obvious that the most important influence on the security of the Black Sea region is Russia's assertive and aggressive behavior toward its neighbors and towards NATO and the EU. The illegal annexation of Crimea by the Russian Federation and its meddling in the conflict in eastern Ukraine resulted in important transformations and challenges at the level of the Black Sea strategic reality and new threats against its riparian states.

Russia's behavior is assertive and aggressive toward its Black Sea neighbors and towards NATO and the EU.

And of course, the latest security tensions in the Kerch Strait demonstrated again that threats and challenges in the area go far beyond anything that can be considered acceptable. So, the threats are there, they are real, they are not going to disappear, and they are

going to spread. In this context, the security situation in the area continues to be fluid and unpredictable. The present militarization of the peninsula shifted the military balance in the Black Sea and significantly increased Russia's strategic footprint in the region.

We must be concerned about Russian efforts to achieve global dominance, using hybrid, cyber, and conventional tools to exert influence.

In particular, the Russian Black Sea fleet has increased its ability to project influence in the region and beyond. I do not believe that Romania is acting like a selfish ally by emphasizing the importance of the Black Sea. We are a frontline state, it is important to have security and stability in the area, and we have achieved enough strategic maturity to say to our allies that it is important to focus and to carefully watch the developments in the area.

We must be concerned about Russian efforts to achieve global dominance, using hybrid, cyber, and conventional tools to exert influence beyond its immediate neighborhood—to the Middle East, to northern Africa, and to the Mediterranean. For this reason, the Black Sea region has a major significance for the security of the whole Euro-Atlantic area. It is a major crossroads and the critical intersection of the east-west, south-north corridors.

Russia's recent strategic doctrines emphasize the use of a combination of different tactics, irregular warfare, and political subversion.

Therefore, the main challenge is to deal with the interconnected and intertwined threats and risks in this area. Aside from hybrid warfare, Russia's recent strategic doctrines—including the 2015 military doctrine and national security strategy, emphasize the use of a combination of different tactics, irregular warfare, and political subversion. This emphasis draws from a long history of Russian military thought concerning the use of irregular forces, influence operations and deception, as shown by the non-linear strategy more recently advocated by General Valery Gerasimov.

The scale and ambition of Russian information campaigns today are far greater than during the Cold War.

Moscow is using hybrid warfare to ensure compliance in a number of specific policy areas, to divide and weaken NATO, to subvert governments, to create pretexts for war in order to annex territories, and to ensure access to European markets on its own terms. Russian hybrid strategies are not new: they have simply been updated and upgraded for this new century.

Russian methods are not the same as those used in the Cold War because the scale and ambition of Russian information campaigns today are far greater. They are facilitated by the existence of the internet, by cable news, and especially by social media. The use of cyber operations is also not new either since there were incidents in Estonia back in 2007—just before Russia's intervention in Georgia in 2008.

Fake news, conspiracy theories, and direct support for political parties with anti-NATO or anti-EU agendas, are increasing Euroscepticism.

Russia is tailoring its hybrid warfare capabilities to best exploit the specific vulnerabilities of each targeted state. We are familiar with the story of Russia's protection of the ethnic Russian population in eastern Ukraine with a propaganda campaign aimed at bringing back old historic issues, to reduce regional cooperation, and undermine trust in the Euro-Atlantic institutions, including both NATO and EU. We are also

familiar with the spread of fake news and conspiracy theories with direct support for political parties having anti-NATO or anti-EU agendas in order to increase Euroscepticism.

To all this, we should add the military build-up for which the Crimea and Black Sea regions are a case in point. Russia's activities are by the book and could be studied usefully in academia. As the dominant actor in the region, Russia employs all the tools, mechanisms, and instruments at its disposal to obstruct freedom of movement and to achieve the power that they desire so much.

Russian assertive actions and hybrid threats will continue or increase in range and amplitude.

In sum, the Black Sea region is a complex mix of security interests. It is the scene of serious violations of international law, challenging the roots of international security and regional stability. Russian assertive actions and hybrid threats will most probably continue or increase in range and amplitude. This scenario potentially poses a serious threat to the security of the whole Euro-Atlantic space.

In facing these challenges, it is very important to have not only our allies on board, but our partners as well: especially Georgia, Ukraine, and the Republic of Moldova. Together, we must be ready to cope with these challenges and use all the tools at our disposal—bilateral, regional, and multilateral—to achieve a stable environment.

Cyber Power in Hybrid Warfare

Dr. Josef Schröfl
Deputy Director for Strategy & Defense
Hybrid Center of Excellence, Helsinki, Finland

Our Hybrid Centre of Excellence in Helsinki is a very young Center of Excellence (CoE), but we have been successful. Although we were founded only one and a half year ago, we already have 22 Member States. From our experience in Helsinki, I would like to discuss three issues concerning the role of cyber power in hybrid warfare.

The Nature of the Threat

Cyber plays a very special and specific role in hybrid warfare, because everything significant that happens in the real world, including every political and military conflict, will also take place in cyberspace. For national security planners, this includes cybercrime, propaganda, espionage, influence operations, terrorism, and even cyber warfare itself.

Cyber space can increase the speed, the diffusion and the power of an attack. And everything can even be anonymous.

The nature of national security threats has not changed in the last decades, but cyber space has provided a new delivery mechanism that can increase the speed, the diffusion and the power of an attack. And everything can even be anonymous. Its ubiquitous and unpredictable characteristics mean that the battles fought in cyberspace can be just as important as events taking place on the ground.

Since I have a technical background, in the 1990s I was able to program viruses for fun. The language I used was the BASIC code, which few remember these days. But five years later in about 1995, I lost the ability to write viruses, because I could not understand them anymore and I could not even understand the effects that they could cause. Now in 2019, we face successful attacks that are increasingly complex. A few years ago, Stuxnet was the most sophisticated piece of malware the public had ever seen. Nowadays, it is something that can practically be written by script kiddies.

Fewer and fewer people understand system architecture in a technical sense.

On the other hand, we must deal with a decreased understanding of the system architecture. Fewer and fewer people understand what is going on in a technical sense. And we have an increasing degree of cross-linking. We have a growing integration of IP-based systems: we have IP at home, on mobile devices and in the armed forces, linking to anything and everything, and even to weapons systems.

Cyberattacks as Part of a Wide Spectrum of Hybrid Means.

That brings me to my second point. Cyber-attacks like DoS attacks or malware are part of the hybrid-threat toolkit. Cyberspace is a key enabler for actions in other operational domains (land, sea, air, space) and has

become an operational domain of its own. Yet, cyberspace itself is hybrid in nature. It is neither owned nor operated exclusively by the public or private sector, because cyberspace is the glue that binds together actions by individuals, states, and companies. We all are responsible for securing it.

Therefore, advancing cybersecurity requires public/private as well as civil/military interaction on a whole of government approach. Inadequate cybersecurity governance risks robbing modern societies of the benefits of access to the global commons.

These remarks are only the lessons learned from our past experience, but changes are coming. There is, for example. the great firewall of China, created as a combination of legislative actions and technologies, which regulates the Chinese internet domestically. Its role in the internet censorship in China is to block access to selected foreign websites and to slow down cross-border internet traffic.

Russia is going to test whether it can disconnect its internet from the rest of the world electronically.

Russia is also planning to attempt something that no other country has tried before. It is going to test whether it can disconnect its internet from the rest of the world electronically, while keeping the internet running for its citizens. This means it will have to re-route all its data internally, rather than relying on servers abroad.

If Russia's plan works, its internet service providers will use only exchange points inside the country that are approved by Roskomnadzor.

I will not bore you with technical details. All we know is, that, if the Russian plan really works, it will require that the nation's internet service providers, the ISPs, to use only exchange points that are inside the country and approved by Russia's telecom regulator, Roskomnadzor. This internet will be called Runet. It is a very difficult technical challenge and it will also be very expensive. The estimates range from €100 million to €5 billion.

What does that mean, if it works? Nobody knows if it will work, but if it works it will create a separate entity and special communication system for centralized internet control. It will give Russia absolute control over its internal internet traffic, and there will no longer be any possible control from outside the country. And it can be sacrosanct against attacks from outside. Russia wants to be able to do this while insulating itself from the consequences, by pre-emptively cutting itself off from global infrastructure.

Russia's Plans for Hybrid Warfare

General Gerasimov argued that Russia should employ "non-linear war."

Concerning hybrid warfare, what we know about Russia's plans is what we learned from General Valery Gerasimov. In a 2013 speech for Russian officers, he mentioned that the rules of war have changed. "Political goals are no longer achievable with conventional firepower, but through the widespread use of disinformation, as well as political, economic, humanitarian and other non-military measures that are used in conjunction with the protest potential of the population.

He argued that Russia should, like the West, adopt methods of guerrilla fighters. Military measures should have a "hidden character." He spoke again, only two months ago on March 2nd, at the conference about the future of Russian military strategy. Russian armed forces must maintain both "classical" and "asymmetrical" potential. He called it "non-linear war," using that concept to describe the mix of combat, intelligence and propaganda tools that the Kremlin has deployed already in conflicts such as in Syria and the Ukraine.

In Ukraine, it is not a war for Russia, but it is for Ukraine.

The Ukraine, one of our case studies at the Hybrid CoE, is a typical example for hybrid warfare because cyber, hybrid and kinetic tools are all used in that war. The interesting thing is that this is not a war for Russia, but of course it is for the Ukraine. The Separatists, supported by Russia are using all the Cyber/Hybrid tools:

- cyber war in preparation for occupying a territory
- cyberattacks against critical infrastructure to intimidate the population and to undermine trust in the government and the political system,
- hacking of weapon systems,
- disinformation campaigns,
- using the all the human and technical means to cause confusion: Who is the enemy? Who is a friend? Who is military? Who is civilian? And the center of gravity is not military, but hybrid.

It seems all the more important to clarify the ambiguities at the strategic level in order to make the unclear visible, which, however, threatens to blur in the event of threats from cyberspace or Hybrid-threats. Such vagueness is most clearly expressed when the scientific debate speaks of Hybrid-threats and refers to cyberattacks what are only part of a wide spectrum of hybrid means.

The Defense of our Digital Democracy

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

The world is moving and moving means change. Some changes are exciting because they promise advantages. Other changes are not appreciated because they are expected to be disadvantageous. But for most changes, we just do not know what they will bring, and they are a source of worry, sometimes fear. At this Paris workshop today and tomorrow, our contribution will be to work on how these current and upcoming changes can bring about a safer world and a shared and peaceful future together.

After the fall of the Berlin Wall, we benefited from a period of greater unity and security, but the wind has turned. We are now witnessing a new period marked by less solidarity, more national alignment, and new challenges which are cause for concern. Brexit and the Catalonian conflict are just two examples that are leading to the same important question of our time: how do we manage the growing influence of nationalist and anti-democratic forces and how can we protect our democracies from their impact?

The attack on our values does not only occur with weapons and physical violence…the attack often occurs anonymously.

It is quite easy to put questions on the table; it is much more difficult to find the right answers because there are no easy answers in a complex and connected world. At the same time, the suggested easy answers are being spread by populists who seek to repeatedly undermine our democracies. The attack on our values does not only occur with weapons and physical violence. More often than not, the attack occurs anonymously, secretly, hidden away in the World Wide Web and perfidiously using our own IT infrastructure.

The cybercrimes and cyberwars we have today are real and we almost know who the players are and what weapons they are using: Robbery, extortion, propaganda, espionage and sabotage, which are a huge and dangerous arsenal. Propaganda's new digital algorithm with fake news and big personal data is another challenge to our democracy.

Future digital weapons will not be developed solely by criminals or companies. Most are developed by large countries.

All of us probably remember the role that the Cambridge Analytica company played in Brexit and in the last U.S. election. But the future digital weapons are not developed solely by criminals or companies. Most of them are developed by large countries with the support of huge investments and new and more sophisticated technologies in order to bypass our digital defenses. Armies of IT engineers are developing cyberwar weapons and when so many are involved, it always means that data technologies are moving over

into unauthorized hands. It is no secret that the well-known WannaCry attack was developed with stolen CIA technology.

So, we must protect ourselves and many efforts have already been made in that direction. But based on recent years, it is also obvious that we could not defend ourselves well, which brings us to raise new questions. Are we able to establish a comprehensive protection? Are the hackers more clever than we are? Why are we constantly facing this incredibly high number of infections? There are even more points to discuss; today, I just want to focus on two of them.

One is what we call the missing or divergent investment focus. Most governments, like France, Germany and others in Europe, are using a wide range of IT technology, different IT infrastructures, hidden internal network environments etc. and, as individuals, we protect ourselves with technology, mainly network security, appliances, firewalls, encryption etc.

A Verizon reports that 60% of the attacks were aimed at or used on an endpoint. But only 4% of spending on IT security is aimed at endpoints.

But most of the infections we get today are not focused on our protections, they are focused on the endpoint. A Verizon report shows in detail that more than 60% of the attacks within the last four years were aimed at an endpoint or used on an endpoint. But only just 4% of your spending on IT security is aimed at endpoint security. This huge imbalance is what we call a missing or divergent investment focus.

The main problem today is the standard office—the smart mobile, the millions and billions of computers, laptops and tablets, the cheap IT standard infrastructure based on operating systems from Microsoft, Google and Apple. Here, the hacker finds for himself a huge battlefield that is not so easy to defend. This is where the private security industry came to play a role.

It has become obvious that security vendors without innovation and technological spirit have no chance against this huge wave of attacks.

After decades of domination by market driven so-called big players, it became obvious as far back as 2008 that vendors without innovation and technological spirit had no chance against this huge wave of attacks. At the end of 2007, we had faced around 1.5 million attacks over the previous 30-year-period. In just one year, we were facing a huge and unbelievable growth of more than 70 million threats. That was more than 15.5 million new threats in one year, 10 times what we had seen in the previous 30 years.

There is still resistance to cloud technology… and we face challenging discussions with European governments saying “the cloud is dangerous.”

At that time, only one technology was able to cope with this huge amount. It was a totally new cybersecurity model, the first cloud security technology, which meant getting away from the heavy signatures using hash with deep machine learning, artificial intelligence and big data environments. It became available for purchase for the first time in 2006 under the name Panda Antivirus. A huge marketing wave against the cloud followed with most IT magazines predicting how useless this technology would be (of course, the technology was always tested offline). It turned out, however, that other technologies that were used instead led to an unprecedented wave of infection which continues today.

One reason—which leads me to my second point— is that the newest available cybersecurity technology came into use far too late. There is still strong resistance to cloud technology or doubts about it. While many technology-driven companies today celebrate the cloud as the main innovation driver of the last 10 years, we still face challenging discussions, especially with European governments saying "the cloud is dangerous, it is not safe," or, "we are not allowed to use the cloud," without even looking at it. Yet, there is not just one cloud and cloud solutions may be quite different from each other, especially in terms of security and data protection. So, we need to overcome our doubts about innovation and progress as we do very successfully in other areas of our lives.

We can see the effects of lack of innovation and information in our European history. After a huge business development at the end of the 18th Century and beginning of the 19th Century based mostly on construction and maintenance of railroads, the English economy underwent a major growth and England soon became the motherland of industrialization.

When the automobile first appeared, a person had to walk in front of every car, waving a red flag.

However, when the automobile appeared on the market as a new technology, there was an attempt to block it with the so-called Red Flag Act. This meant that a person had to walk in front of every car, waving a red flag and periodically blowing through a horn. This may sound funny today but, as a result, the infrastructure and automobile industry development in England was delayed for decades. In another example, while criminals, who tend to use the newest technologies to achieve their goals, were speeding away in their cars, the horse-mounted London police could not keep up with them. So, what was discussed in the British parliament? Not the motorization of the police. No, they discussed how they could get faster horses!

When criminals started to use automobiles, the parliament discussed how the police could get faster horses!

For the past 10 years, we have witnessed similar discussions, especially within European governments. When the Red Flag Act was established in 1865, there was no Germany and the centre of Europe was dominated only by agriculture. By the time the Red Flag Act was disabled in 1896, the young Germany, together with the United States of America, had already passed England in terms of industrialization. So, this shows how fast leadership and connection can be lost. Have we already lost connection in Europe? If we want to play a significant role in protecting our own digital environment and even digitalization itself, we need to collaborate. Only by bundling all of European resources, including governments and technology vendors, shall we be able to protect ourselves, despite an IT specialists' shortage to protect us comprehensively in the short-term, which is a mandatory requirement.

Only by bundling all of European resources, including governments and technology vendors, shall we be able to protect ourselves

Of course, the cybersecurity industry has to, is able to, and will play an important role. It is still dominated by market-driven players but there are more and more vendors. There were 500 vendors at the RSA conference in San Francisco last year, 700 this year, and the numbers are expected to increase again next year.

Panda Security is a good example in order to show that technology counts, is mandatory, and needs to be looked at carefully. Since 2018, as a pioneer in cloud security, Panda has been able to classify all processes on clients' endpoints, which means clients and servers, in real time. So, in order to avoid the execution of any malicious code, the processing of more than one billion events a day is fundamental to this ability. As we hand over these events to our users, they get full transparency on the behavior of all processes on all devices. Over the past four years, cryptologists have not been able to bypass this technology. You may all remember what Loki could do by encrypting 6,000 devices per hour. The technology was there, and you know yourselves how badly you were harmed.

However, too many people with responsibility still have not decided to use this advance protection and avoid conversations and communications on it. We have seen the implications of this in past years and in the last quarter of this year. But there is good news as well, because people have now begun using it. For example, ministries in France and Spain, public institutions—from municipalities up to state chanceries in Germany, government structures from Sweden to Hungary and, last but not least, the whole government of Cyprus, are counting on our expertise. In addition, more partners like Telefonica, which began five months ago to roll out the technology to all of their 180,000 clients, Indra, Deloitte or Airbus Security in France are using it to protect their large clients working on infrastructure protection, including, nuclear power plants in central Europe.

According to the Spanish Centro Criptologico Nacional, "governments, companies and strategic organizations must unite to face cyberwar."

Within all these success stories, however, we have only seen a small European connectivity. The security of governments, economies and societies is a real and huge challenge for all of us and especially in our federal systems where each responsible entity can and should decide on its own. We will achieve this goal only through communication, information and collaboration because, in the end, we are not capable of convincing each responsible entity individually, at least not short-term.

Let me end my speech with the words of Javier Candau, the head of the Spanish Centro Criptologico Nacional who, during our summit in Madrid last year, said: "governments, companies and strategic organizations must unite to face cyberwar."

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

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

It is my view that we have arrived at an important moment in all our shared efforts as diplomats, policy makers, and scholars: What are we going to do about cyberspace to safeguard it as a source of prosperity and prevent it from being overcome by conflict and instability?

The recent cyber incidents, as well as a growing number of states that publicly acknowledge their offensive cyber capabilities and the various negotiations, including those at the United Nations this summer and in the fall, will affect our efforts to manage conflict in cyberspace for the coming years.

With the new technology like cyber, states needed a way to distinguish what is acceptable state-on-state behavior from what is unacceptable behavior.

As a diplomat, I look at these challenges from a particular perspective. Often called the "Mother of Norms," I had the privilege and challenge of working for the last two decades on these issues precisely to construct an international policy architecture to maintain stability in cyberspace. This effort has always been a work in progress. As the small number of cyber diplomats was growing, we were constantly updating our thinking to anticipate and respond to the threats involving a technology that states and other actors are always finding new and creative ways to use.

Let me describe where we have been on this effort and where, at least, we think we are going. The place to start is our decades-long effort to establish a framework of responsible state behavior in cyberspace. The idea behind building this framework was straightforward. With the new technology that had offensive uses like cyber, states needed a way to distinguish what is acceptable state-on-state behavior from what is unacceptable behavior and they needed mechanisms to manage tension when incidents occurred.

Since 2009, we have been working at the UN to build a consensus around this notion of a framework of acceptable state behavior.

Since 2009, the United States, France, and a number of other governments have been working at the United Nations to build a consensus around this notion of a framework of acceptable state behavior. We have been exporting that notion to regional venues like the OSCE, the ASEAN Regional Forum, the Organization of American States, and even further.

Measured in diplomatic time, progress on this effort was reasonably fast. In 2013, fifteen governments, including Russia and China, joined the consensus in a UN Group of Governmental Experts' (GGE) report that confirmed the applicability of international law to cyberspace.

In 2015, twenty governments, once again including Russia and China, reaffirmed that conclusion in a subsequent Group of Governmental Experts and also recommended eleven non-binding norms of state behavior that applied during peacetime.

Regional organizations like the OSCE now have practical confidence-building measures to reduce the risk of conflict from cyber.

Throughout this time, regional organizations like the OSCE have adopted practical confidence-building measures that were recommended in these GGE reports to reduce the risk of conflict stemming from cyber incidents. And, of course, more than one resolution from the UN General Assembly has recommended and affirmed that all states be guided by the UN GGE recommendations.

I must acknowledge, as many of you know, that the GGE did not reach consensus in 2017. There were a number of reasons for this but, in our view, this failure to reach consensus did not undo or undermine our previous work. Indeed, we have entered more shark-infested waters as we look to kick off a new GGE and a second UN body called an Open-ended Working Group at the United Nations in the coming year. Our intention is to build on our previous successes and bring a broader group of countries into the dialogue about how to maintain stability and peace in cyberspace.

Certain states are using their cyber capabilities irresponsibly…our framework of responsible state behavior is not self-enforcing.

All of this brings me to a newer element of the architecture for stability that we are working to build. As I have described, we have made real progress in the last decade in building an international consensus among like-minded states about what constitutes responsible state behavior during peacetime. For states that want to be responsible and want to maintain stability, this provides helpful guidance.

We must work together—that is why the U.S. National Cyber Strategy calls for the launch of an international cyber deterrence initiative.

But it has become apparent in recent years that there are certain states that have an interest in using their cyber capabilities irresponsibly, often in ways that are designed to cause instability. And for those states, it is clear that our framework of responsible state behavior is not self-enforcing. Rather, I believe that they have chosen to act contrary to this framework because we, as responsible states, have too often failed to hold them accountable for their behavior.

For this reason, even as we continue our work to build consensus on responsible state behavior, we must also work together to ensure that there are consequences for bad behavior during peacetime. Such consequences will be more impactful and less likely to result in unwanted escalation if they are imposed in concert with a broad group of like-minded states. That is why the U.S. National Cyber Strategy, which was released in 2018, calls for the launch of an international cyber deterrence initiative. In broad strokes, that is a summary of where our efforts are to promote stability in cyberspace.

Europe's Role in the Global Competition on Artificial Intelligence

Mr. Wolfram von Heynitz[3]
Head, Cyber Policy Coordination Staff, German Federal Foreign Office

It is hard for me to speak after Michele Markoff, because she is basically the dean of the UN process that I will describe, after which I will focus on the development of norms for artificial intelligence.

The Necessity of Norms in Cyberspace

We totally agree that the development of norms is important. In fact, I would call it the second line of defense. The first line of defense is, of course, resilience building, the second line is norm building, and the third one is confidence building. It is particularly appropriate to highlight confidence building measures in this location, the Hôtel National des Invalides, where you see so many plaques honoring the dead of World War I, an example of when —inter alias—a lack of confidence measures allowed a terrible conflict to erupt. Today, I am afraid that we are in a situation that, while not exactly similar to what happened prior to WWI, is also a very dangerous one. I am referring, of course, to the lack of confidence in relation to cyberspace. Now, I would like to go back to the second line of defense, the norms process: Where do we stand? Over the last years we had several UN Group of Governmental Experts (GGE) and, as Michelle Markoff pointed out, the last one failed, but we had successes in 2013 and 2015. We have to continue to build on that. In fact, last October, two resolutions passed in the First Committee of the UN. One resolution, to establish a so-called Open-Ended Working Group (OEWG), was a Russian proposal. The second one, a U.S. proposal supported by Germany and a lot of other western countries, called for a GGE, another group of governmental experts, that will convene for the first time at the end of this year.

This means that, for the next two years, we will have two parallel processes. This will be a big challenge and I cannot tell you where the process will land (Michelle Markoff is probably the expert on it). Nonetheless, it is going to be very difficult because, first of all, we have to manage both processes, and then, of course, we will need a lot of good will. This work matters because norm building is important in order to create an urgently needed stability framework, not only to prevent bad accidents from happening, but also to increase the level of trust in cyberspace.

Norm building is important to create a stability framework, which we need to prevent bad accidents from happening.

Because norm building is important in order to create a stability framework which we need, not only to prevent bad accidents from happening, but also to increase the level of trust in cyberspace. I would also like to come back to Jan Lindner's example of the 19th century

[3] These remarks were presented on an entirely personal basis and do not reflect the official positions of the German Foreign Ministry or its Cyber Policy Coordination organization.

law requiring a red flag to be waved in front of early trains. Yet, development of railroads in Britain during the period of the red flag law was more rapid than in every other country in Europe except Germany. Why did this happen? Well, perhaps the red flag law also increased public trust in this new technology? I would not go too far with this analogy, but we must also understand that we need rules, regulations, and norms to increase the trust of the general public in new and developing technologies.

Why Norms are Needed for AI

With that point, I come to artificial intelligence, a decisive, game changing technology, still lacking a framework for the development of norms. I believe that such norms are definitely needed. There is an ethical debate about rules for AI, but I think it will be a debate about standards and a framework for AI that will be decisive. These will have to include standards for competitiveness, freedom and, of course, the security of all our countries. Whoever controls data and sets the rules for data usage basically controls the oil of the 21st century.

Norms are needed for AI. Whoever controls data and sets the rules controls the oil of the 21st century.

Also, social scoring technologies are already on trial in China and possibly in a couple of other countries. These technologies will have a large impact on societies, how we compete between societies, and the models we will have in the future for the development of open and free societies.

AI will be a game changer if it is needed to respond to hypersonic weapons—because there will not be time for human decisions.

In addition to that, there are security risks related to AI: lethal autonomous weapon systems controlled by AI may well be under development and we have to set rules for that and agree how to deal with it. If you think a bit further you may imagine malware combined with AI. And then, of course, there is the potential impact of artificial intelligence on command and control software in the military sphere. A game changer moment will also be when AI is deployed to respond to hypersonic weapons due to the lack of time for human decision.

Another potential game changer will be the combination of AI with future hardware development, notably quantum computing. Artificial Intelligence is clearly a decisive technology. Yet, we still do not have a unified framework to discuss rules and norms for it. There are some regional initiatives: There is the Council of Europe, some civil society actors, and the Toronto Declaration. We also have initiatives by private companies—the Microsoft guidelines for artificial intelligence, and the Google guidelines for artificial intelligence for example—but we do not have an international framework. The OECD came out a couple of weeks ago with proposals, but it is hard to see which impact they will have beyond the limited OECD membership and mandate. Thus, the development of AI for the time being is being mainly guided by open competitiveness.

China started an initiative in UNESCO to set rules for AI, and Europe has established a high-level commission for AI.

Who sets the standards and the norms for artificial intelligence? There is no possibility of setting standards or norms for AI on a national level. You need to do it in a broader context. Ideally, it should be done globally, but if you cannot do it globally, then you have to do it at least in the framework of the European Union.

Luckily, while the EU can be slow, it is also very thorough and determined. A high-level commission has been established for AI and it published guidelines for AI on the 8th of April. This was a significant step for the EU.

Why are these guidelines so important? First of all, because the high-level commission—despite some criticisms, resisted the temptation to follow what I would call a red line approach. Instead, the Commission has chosen a very practical approach that is focused on the robustness of systems, and on how this notion could be applied. They came up with the word, "Trustworthy artificial intelligence" as the goal, and I think that is a very good one, because it combines the expectations of the general public, including people from civil rights organizations, with the interests of industry and the desire for economic and scientific development in this field.

The EU focuses on seven requirements for trustworthy AI, including privacy and transparency. It is just as important, however, that the EU approach includes proposals for methods to implement these values. It shows how practical the approach is. Both technical measures and non-technical measures to implement criteria into AI systems are included and there is a checklist to test how these norms are actually implemented.

The new guidelines will also be tested in a real-time environment in finance, transport, health and law enforcement.

The EU guidelines will be tested in the coming months. There will be discussions with stakeholders and they will be also tested in a real-time environment in four areas: in finance, in transport, in health and in law enforcement.

The goal is to specify the guidelines for each of these different sectors because the general assumption is that general guidelines will not be sufficient. In AI you need specific guidelines for specific problems in specific areas. The EU has chosen a forward-looking approach that keeps high standards and combines them with the necessities of industry and of scientific research in a fast-developing field.

The next phase, implementation, will probably fall during the Germany Presidency of the EU. It is still an open question, how EU AI guidelines should and could be implemented so that they are relevant. Not everything will need to be set into laws. There could be voluntary guidelines, or design principles alongside more binding regulations. This is still an open process. But the part that will be put into law might have the same significance as the General Data Protection Regulation—setting standards that will be valuable and influential beyond Europe, even globally.

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

Ambassador Karoly Dan
Ambassador of Hungary to the OSCE; Chair of the IWG Cyber Group

What we have heard so far is the big picture. My talk will be much more focused towards the challenge that we are dealing with at the OSCE. We are trying to create room for civility in the confined environment that is the OSCE—57 members working toward a consensus. These 57 members are an interesting group because they represent the early 90s after the fall of the iron curtain.

We have adopted two sets of Confidence-Building Measures, sixteen of them altogether. This is an environment where, on every Thursday, every participating state has the opportunity to spill out everything and say whatever they want about each other, which is sometimes a very open conversation. It involves name-calling and a lot of things that you would not expect in a diplomatic environment. Even though it is done in a very civilized way, it is pretty harsh. So, politically, it is a highly-charged organization that has been dealing with all of the frozen conflicts in Europe. Of course, they used to be conflicts before they became frozen conflicts, but that is another story.

For the most part, we are an organization that was designed to prevent further conflicts. This is how the OSCE comes into the picture. Our thanks go to Michele Markoff and a few others who were able to recognize these issues early enough and were trying to find ways and also institutions that would move forward with certain parts of the work that has to be done. So, this is how we came to these sixteen Confidence-Building Measures (CBMs). In an effort to foster responsible state behavior, our focus is state-to-state communication: How to design the elements and how to implement them in times of incidents, accidents, crises, attacks or whatever happens to be. It can be a little bit tricky.

Designing the elements and implementing them in times of incidents, accidents, crises, attacks can be a little bit tricky.

If anything happens or initiates in cyberspace that threatens national security and stability, how do you actually deal with it? This is especially challenging in an environment where trust can be an issue. How can you talk to someone in whom you have pretty much zero trust, which can be the case in the OSCE environment? With some countries, we have a much higher trust than zero but, with others, zero is pretty much what you have. In theory, the sixteen CBMs embody all the technical elements for how to use this infrastructure for the exchange of information, and how to utilize it in communication.

When the second set of CBMs was introduced in 2016, it was immediately provided with an event that nobody could have foreseen before: The issue of the meddling in the US elections became a centerpiece in our

group for a while. Now, the group itself and the discussions are supposed to be very pragmatic and technical, but political events usually do not help these kinds of discussions. So, one of the first things that we had to deal with in early 2017 was how to overcome this issue and channel back the conversation to the working group and to being more technical and focused on implementation.

Within a very short and positive period, we truly came to a halt. We realized that, no matter how well-prepared a CBM is with consultations back and forth and all the details chiseled out in a very pioneering way, there is still no guarantee that you will be able to implement it. We then had to find a solution to decentralize a working group that was designed to be central in a certain discussion. That is when we came up with the idea that we would ask individual countries to adopt certain CMBs, one or more, team up with other countries, start the discussion and also try to put everything on paper to prepare ideas for the texts that would be discussed and hopefully adopted by the working group.

No matter how well-prepared a CBM is, there is still no guarantee that you will be able to implement it.

What we need to keep in mind is that this is a big puzzle. Although we are very focused on certain things, it is still a big puzzle and we do not truly see all the bits and pieces, especially the very small and obscure ones. Also, the technical services that are dealing with these issues might have views on implementation that are very different from those we have as diplomats. We usually try to find some kind of consensus, but that is not always the case with the technical experts who are behind us.

There are the levels of the discussion: some are more visible, some are not so visible. We are in a lucky situation since most of the truly important central CBMs have been adopted. I dare say that, if two more CBMs can be adopted, we will have achieved almost everything we need to move forward and truly talk about the big picture that we have to put together. Some of them are easy, like points of contact. Every country needs to have a point of contact and a designated location. Some of them are more difficult, like consultations. Sometimes, the very word "consultation" can lead to an academic argument about what it actually is. Then we build from there. So, the whole process is now in a very decentralized phase and moves forward at a much better speed compared to what could be achieved before.

Most of the central CBMs have been adopted, so if can adopt two more we will have achieved almost everything we need.

Now, coming back to the working group. We are going to discuss it with all the members around the table. Again, we need to face some difficulties and we need to truly look each other in the eye. But until then, we are going to have a much better understanding of what we are dealing with in terms of implementation. We do have to take risks. I just mentioned one to you, which exactly addresses the technical element in what we do.

At the OSCE, we are trying to foster a culture in which reporting is something that you do for your own sake and for others as well.

We are determined to use the communication network of the OSCE .The OSCE network has been used, at least until now, to exchange military information vis-a-vis arms control and disarmament issues. This is where you have all the reporting going back and forth. It is a safe network. It sits on a public server, secured by a very well-known private company with very good references. It has been used for the exchange of military information for many years. Now, when it comes to

cyber, interestingly, there is one participating state that is not very happy with this solution, but what makes it very interesting is that this is all voluntary. We are trying to foster a culture in which reporting is something that you do for your own sake and for others' sake as well. You are developing a culture of talking to each other about issues that are in cyberspace but you need a communication line for that, obviously.

The whole issue of this communication network has truly become the next obstacle that we have to deal with. The US took the initiative and developed the templates. We circulated the templates quite a few times, trying to get feedback from delegations. We did not get many, which means that the templates as they were designed were very good. Slightly more than a year after the first circulation of the templates, we decided that, since we had not received negative comments, the templates were good enough to be put on the network, which we will do. They will be ready to be used by every participating state within the OSCE. That might upset some, or perhaps one. But we need to make progress, otherwise we are not doing the most important part of what we should do, which is building confidence. This is exactly where we stand and again, the bottom line is to build state-to-state communication and trust.

Just one more point. There is also capacity building. Capacity building is important because there cannot be too wide a gap between capacities in the same group, which would bring about inequalities and frustration. Then, you would not be able to have the same kind of discussion around the table that is necessary for this kind of environment.

Preventing a Black Sky Event – Dealing with Cyber Threats to the Power Grid

Mr. Raj Samani
McAfee Fellow, Chief Scientist, McAfee

We work in an industry that we used to describe as being fast-paced. In reality, the threat landscape has this remarkable capability of proving us wrong continuously. Just over 10 years ago, we would talk about cybersecurity as being an IT related issue but, in 2010, Symantec uncovered an attack in a nuclear power plant in Natanz in Iran. This was an attack that nobody had anticipated, an attack of true cyber warfare whose capabilities, as was asserted at the time, had been developed five years earlier. It took the whole industry and all of us by surprise. We never for one moment expected a computer virus to have that level of destruction and the ability to slow down the nuclear program of an entire nation.

We are seeing this migration to cyber because it gives nations the capability to have non-repudiation.

I think we all recognize that the reason why we are seeing this migration to cyber is that it provides nations with the capability to have non-repudiation: the attack on Natanz was carried out in 2010 and yet, up to this day, no nation has been held accountable for it. It was one of the most disruptive attacks that we have ever witnessed but all we have is speculation and hearsay. Much like election misinformation, much like the WannaCry attacks, indictments have been made but nobody has been held to account. Let us not kid ourselves, this is a cost-effective way to be able to attack a neighbor and deny all knowledge of it.

If we move to the critical infrastructure world, what we can see today in attacks against the medical environment is the simplicity with which one can withhold patient care: it can be done and outsourced to an 11 year-old-child. Ransomware campaigns can launch an attack from small websites that can allow someone to attack hospitals.

And if we start to look at election security—I did promise not to talk about Brexit but I feel like I talk about it everywhere I go—we are talking about monumental decisions for an entire nation that were potentially manipulated by rogue states…well, not rogue states, but by third parties. This is a significant issue of which we barely even recognize the importance.

A group called GreyEnergy is seen as responsible for attacks on Ukraine…we suspect that it is available for hire to nation-states.

So, why are we discussing this today and why, when we talk about critical infrastructure, do we have more than a one-case study? For years, we sat on this attack in Iran and thought to ourselves that it was a single and unique attack on critical infrastructure. Today, however, there have been a multitude of similar attacks, from healthcare to energy and even to fair and democratic elections. This is partly because it is easier to access the tools. Three years ago, for example, we identified criminals who, for

the price of a cup of coffee, were selling access to a utility in Europe. Similarly, for about $4, it is possible to gain direct access to a US international airport, including all credentials. It is becoming simpler and simpler for anyone to launch these types of attacks.

I want to be very clear here that there is a complete difference between the attack in Iran and the criminal access to the types of environments mentioned above. More recently, however, we have had to acknowledge the work of a threat actor group named GreyEnergy. This group has been regarded as responsible for attacks on Ukraine and, to be blunt, our strong suspicion is that it is actually available and accessible for hire to nation-states that do not have the offensive capability to target assets on their own.

Troels Orting, a colleague of mine, made a claim when he was at the European Cybercrime Centre that "There are 100 cybercriminal kingpins out there. We know who they are, and they have more offensive cyber capability than nation-states." And yet, these groups are available and currently working on behalf of nation-states to go out and target infrastructure across the globe. In the particular case of GreyEnergy, the group developed fairly standard tools that are easily accessible and available to anybody with a browser and it was able to disrupt the energy of an entire nation, not once but twice. It is important to recognize the kind of impact that the group had because not only did it disrupt the entire power for the nation but, at the same time, it launched a denial-of-service attack against the customer service capabilities of the utilities. This was designed not only to disrupt power but to spread fear by eliminating the ability to even log a call or make a complaint.

This sort of disruption was not just in Ukraine but it also happened in the Middle East where the critical infrastructure is petrochemical. We have witnessed what appears to be a nation-state that acted with the sole purpose of disrupting petrochemical organisations based in the Middle East. This nation-state was successful, not only once but three times. When we delve into the analysis of the malware that was used in all three of these attacks, the most remarkable thing is that today, that nation-state is improving its capability. The original and first attack that was done against several organizations has now progressed and gained traction—the campaign is bigger and wider; and the security operation of this threat actor is improving year after year.

The adversaries that come after your critical infrastructure are improving, they are able to outsource if needed, and they have deniability.

That is the reality of the world that we live in. The adversaries that come after your critical infrastructure are improving, they have the ability to outsource and, if you can point the finger at them, there is nonrepudiation. It is very simple to say, "This was not us." In fact, you would be lucky to get a response at all.

The reality is that public/private partnerships are nothing more than rhetoric.

When I talk, I often try to provide some feedback as to what we can do as an industry or what we can do as a society. I laugh because we talk about this concept of public/private partnerships and yet, the reality is that public/private partnerships are nothing more than rhetoric. We claim that we do public/private partnerships, we sit in meeting rooms every three months and expect to be able to discuss some of the issues that we see today, but it is not enough, and it is certainly not working. So, if we are truly going to address these issues—and we absolutely need to, there has to be real-time sharing of information; it cannot be three months, it cannot be

four months afterwards. A great example is when a threat actor targeted banks in the United Kingdom: they came after Bank A, Bank B and Bank C. Why were they successful? Because none of the banks spoke to each other and shared any of the indicators of compromise in a timely fashion.

To conclude, we need to have real-time sharing, we have to share information quicker and faster, and we have to begin to track the adversary. We have to understand who the adversary is and how it is improving. When we uncovered a recent campaign targeting the Winter Olympic Games, we saw a level of capability that even surprised me. Our ability to protect and our ability to detect these attacks is going to be based upon how we work together.

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

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

According to the workshop agenda, "France now has cybersecurity capabilities of sufficient size and quality to strengthen the security of the infrastructure operator." In fact, this is a little bit optimistic. While we can say that critical infrastructure is state of the art in matters of cybersecurity, what does being state of the art mean? It means that it is not easy to hack us, but it does not mean that it is impossible to hack us. So, to avoid blackouts, we have only one solution and that is to be able to control the network without information systems. This means that we have to train to be ready to control our electrical infrastructure without information systems.

I will develop my presentation about the human factor, because there is a human mistake behind the most successful cyberattacks. An infected USB stick is inserted into a computer, a password is not strong enough, some accounts are shared, or an attachment is opened when it should not have been, and a link to a compromised site is executed. No one, including those of us in this room, can pretend they have never made such a mistake. Happily enough, in most cases, this bears no consequences. Unfortunately, there are examples to the contrary. Also unfortunately, they are legion.

How much time do you spend checking your emails carefully before you open an attachment?

Why is this? That is probably because hackers, in addition to their technical skills, are well-versed in human behavior. Would you object if a colleague, whom you know quite well, and whose computer is out of service and cannot be used for a presentation, were to hand you a USB stick so you could display it from your own computer? Most of you in this room definitely would object, but many of your colleagues probably would not.

You probably receive dozens or even hundreds of emails a day. How much time do you spend checking them carefully before you open an attachment or click on a link once you feel the mail is genuine? A few seconds, not much more.

Hundreds of laptops or smartphones are lost weekly at Paris's Roissy Airport. How many of these are properly protected and encrypted?

If one is not trained, properly briefed, or alerted, or if one is not a professional in cybersecurity, or if their CSO (chief security officer) is not a bully, there is always a sense that they will make a mistake. The probability of a mistake may not be one, but for sure it is not zero. RTE has conducted several phishing tests on our own employees. The results are intriguing. We are continuing such tests in order to train to the level of zero mistakes. Getting hold of a user password is probably one of the easiest things one could do; when

you know most people use the same password on every application, for a hacker, the possibilities behind this are quite attractive.

As another example, several hundred laptops or smartphones are lost each week in Terminal 2 at Paris's Roissy Airport. How many of these are actually properly protected and encrypted? A hacker just has to bend down and pick one up.

As you can see, we spend a considerable amount of money and energy in order to protect our IT systems to make them safer and more resilient. We are right to do that and we must continue. There is one field, however, in which we must also collectively invest. It is training and raising awareness. RTE has made it a priority in our fight against cyber criminality. We have set up a training program for each of our employees. We are also delivering workshops on a regular basis and we test our employees.

My contention is that, in France today, not all of my fellow citizens are fully aware and trained in cybersecurity; far from it. Regardless of the cybersecurity cooperation effort to develop increasingly competitive tools, regardless of the efforts by the officers of critical infrastructure to protect the system, as long as the human factor remains at its current level, a hacker's life will not get any harder.

We must, therefore, commit to a large investment in training. Considering that bad habits are more easily acquired than good ones, children should be made aware of the danger of cyber criminality, starting with their first interaction with a computer, including at school.

Children should be made aware of the danger of cyber criminality, including at school.

No one would ever consider handing over the keys to his house to a delivery person he does not know. Nobody would sign a blank check to a perfect stranger. Nobody would dare let a burglar know that they will be away from home for several weeks on a trip to the other side of the world. In real life, certainly not; but online, thousands of people do that. Why?

Certainly, it is because, in real life, people are reasonably paranoid, whereas online, they show a staggering lack of judgement. Yet they know that the internet is dangerous; television, newspapers, and all the media talk about it regularly. There are many articles on the subject, but people act as though they do not see the internet as dangerous. This is as simple as it gets.

At the end of the day, it is because of this simplicity that our job, I mean the CSO's, has to be so complex. Making it less complex is the main reason for training the next generation to be cyber resilient.

Infrastructure and Cyber Threats in the Global Framework of Hybrid Threats

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

Since I am working in the department of security and defense of the Ministry of Energy, Transportation, Environment and Housing, the title of this very interesting seminar, "Global Security in the Age of Hybrid Conflict," is really our agenda. This is what we do at our ministry in terms of defense and security for energy infrastructure and infrastructure in general.

My focus will be on a subset of the workshop agenda, "Cyber Threats and Cyber Influence Operations," and I will address the global framework in which we deal with those cyber issues. Our first priority is to have a full spectrum approach. Cyber threats are very important, but they are relevant to only a part of our toolbox and we manage the toolbox as a whole. This is the vision that we have at our department.

Traditionally, energy infrastructure, including energy for transportation, were key elements for war, both as tools and as objectives. We conduct war by means of energy and transportation, and we conduct war, in particular, for energy and transportation reasons. The global setting has not changed that much, but what has changed is that we are in an era of hybrid threats in global affairs. As engineers, it is hard to understand that the kinetic aspect has become only an element of war while the cyber aspect has become rather important, central, and pivotal. We have to understand this in the global context.

How do we deal with energy infrastructure in this era of hybrid threats? First, there is cybersecurity. From the many comments we have had on the subject, it is clear that even cybersecurity is an expanding field. This is understandable, because we need to include the Dark Web—a market of cyber and other vulnerabilities. There is also the cryptocurrency question. Since it helps bad people who usually try not to leave traces, cryptocurrency is a very central and pivotal element. Yet when we build security around energy infrastructure, which is very critical for our societies, we must not forget to add the old-style threats, such as physical security: old-style activities like sabotage are still very relevant, very cheap, and very efficient. Of course, there is now a new way of doing such things as sabotage with an unmanned aerial vehicle. There is also the weapon detection issue, which is interesting.

With energy infrastructure, we must not forget to add the old-style threats: sabotage is still very relevant, cheap, and efficient.

Other threats are very well-known, like chemical, biological, radiological and nuclear hazards (CBRN), and low-cost CBRN hazards can be very damaging. For example, 18 years ago, our American friends suffered an anthrax attack. As a result of this attack, a limited number of rooms that contained an anthrax envelope are still are off limits today. Hopefully, there were no critical components in these rooms.

In order to place these hybrid threats in a full spectrum perspective, I must add social activities. There are internal social events, such as social threats involving colleagues. There are external social events—such as efforts to hijack the infrastructure, and there are also threats to the environment. Let us take a couple of scenarios to be more explicit. What threatens us and what needs to be analyzed? Hybrid threats are in fact a mixture of threats. For example, you may get involved in a social activity and use it to hijack an infrastructure. At the same time, you might make a cyberattack on the infrastructure to diminish the infrastructure's capacity for reaction, so you can participate both externally and internally in a socially destructive action.

If there is an attack on an infrastructure at the same time as a political attack, a country's capacity to react is diminished.

Similarly, we have to add media communication to our discussion. While it has not yet been seen, there is no reason not to couple a reputational attack, a cyberattack, or a sabotage attack. You can mix different aspects. For example, when there is a merger and acquisition issue involving infrastructures, there are media and political aspects. When there is a political attack by a hostile entity, one consequence is the diminished capacity of the state to react. So, if there is an attack on an infrastructure at the same time as a political attack, the fact that the capacity of the state is limited means that its capacity to react to an attack is diminished.

We should not forget that we are operating in a planning timeframe of five to 10 years. Bad people, hostile states, non-state actors, mafias, are not like Wall Street. They are not acting on a quarter-by-quarter basis. Their activities are based on long-term planning. For example, if you are planning an attack on France for some time during the next 10 years, you will know that at some point between year five and year 10, there will be a heatwave, or a very cold winter. Therefore, you will be able to plan an attack to take advantage of severe weather conditions, either cold or hot. Of course, an attack on our infrastructure will have a stronger effect in a cold winter than in a very light summer. So, if you incorporate climate conditions in your planning, you can actually plan your attack within a three-year timeframe.

A terrorist (or state actor) will be able to plan an attack to take advantage of severe weather conditions, either cold or hot.

Our ministry deals with all those vast threats in a global security framework. How does it work? A pivotal time is crisis management. We start with crisis management because it is clear that there are crises. Ten or twenty years ago, we were debating whether there would be a crisis or not. Now, we admit that crises are more or less normal. Of course, we try to vent those crises or mitigate them. In order to handle that, we work on crisis management and we work on early warning exercises, prevention and standardization. After the crisis management, we work on post-crisis reconstruction and resilience.

Finally, I would like to propose that we reinforce early warning and intelligence, early notifications and simulation.

To finish, I will make a final comment on the approach of the French government. Based on a critical analysis of how we are operating, we believe that our governance is fairly robust. But we want to cooperate with everyone in order to provide our governance with the necessary elements and decision-making tools. This is what cooperation is for. Going forward, I would like to propose to this audience that we reinforce early warning and intelligence, and early notifications. I also hope we can reinforce simulation. At the end, these are those buzz words—early warning & anticipation, simulation and continuity of activity—that I wanted to bring to the debate.

Cyber Crime and the Dark Web

Colonel Jean-Dominique Nollet

Director of the Centre de lutte contre la criminalité numérique (C3N), French Gendarmerie Nationale

I am a colonel in the French Gendarmerie. We are a rather large force, 120,000 strong. We enforce law throughout the French territory, overseas, and during our missions with our colleagues from the military. We are military, but we are attached to the minister of the Interior instead of the minister of the armed forces. My role is to run the cyber center for the Gendarmerie, and I will explain what we do.

We try to arrest bad guys, which is a part of our role that is easy to understand, but we try to do this through cyber, or we try to arrest people who are performing cyber- criminal activities. Therefore, my speech will be about safety and security, but not about conflicts that states have among each other. In fact, we are very happy not to worry about them, because they are much more complex than the very pleasant work that we do every day.

What about the Dark Web? First, I am going to try to destroy a few myths. While some people attach importance to the distinction between the Dark Web versus the Deep Web, we are not really concerned by these differences. For me, the difference is just that you cannot index the Dark Web, you cannot easily search it, and this provides a degree of anonymity. So, it covers everything from the RC channels from the 1980s that still exist up to the latest ones that I will mention at the end of my speech.

Two million people benefit from the Dark Web's anonymity, but this is *not* the best tool for the safety of your kids or our companies.

Accessing the Dark Web requires a special platform, usually Tor (or I2P). It was invented by our friends from the US military, specifically the Navy. They invented it because it was fantastic for transmitting large files from one point of the continent to the other. They decided to have it run as Open Source, because it would allow anonymity of the Tor nodes, a clever idea. Today, two million people are using it and benefitting from this anonymity. As a cop, I must say that this is *not* the best tool for the safety of your kids and for our companies, but that is the new world we have to live with.

The Dark Web is a place where people can do things in total or semi-total anonymity, which brings new challenges. Who uses it? You are probably thinking of criminals, researchers, or defenders of liberty in China and Iran, which is all true. However, I would like to add a few other actors to this list. We are using Tor at the Gendarmerie, the military are using it, and a great many others use it as well, because of its fantastic anonymity. You cannot trust all the nodes, or all of the traffic, but it is pretty cool. So, everybody is having fun on Tor, which is both good and bad. If it allows good guys to do good things, it is good; if it allows bad guys to do bad things, it is bad.

What is the threat? I believe that our big enemy in cyber is called PR (public relations). Everybody wants to do press releases in order to be popular on the web. This kills knowledge. We have many companies and governments making claims about the Dark Web, about criminal actors, and about cyber, but how often is it true?

During the WannaCry crisis, I was at Europol, which is a kind of NATO for law enforcement. We brought together antivirus companies, including Anton Shingarev at Kaspersky Lab—all the guys who had grown up together—in order to deal with attribution. We wanted to do more than just attribution for intelligence purposes. We wanted to do it at the level of evidence and law, which is a different ball game because you have to have real evidence. But when we brought these experts together, they all said that attribution is just PR. Journalists will capture PR from a company and repeat it. Worse, governments have also lied in attributing attacks. I am not naming anyone, but this mindset does not help.

The Tor node list is published hourly. If you download this list of public Tor nodes, you will be able to protect against access from them.

It is important to understand Tor, but how many people even know how many Tor nodes there are? There is a legend that 80% of the Tor nodes are run by the FBI, but I have a good relationship with the FBI and I know it is not true. It is useful to understand, for example, that the Tor node is published every hour, so If you download this list of public Tor nodes, you will be able to at least block and protect against access from the nodes. You will reduce your threat tremendously. For me, understanding Tor and the Dark Web is an indication of how well you understand your job in cyber. It is not enough to have professional certifications.

For me, understanding Tor and the Dark Web is an indication of how well you understand your job in cyber.

If people are selling things on the Dark Web, what is the real danger? A few years ago, there was concern that nuclear materials might be sold. But what is the difference between selling them on the street or on the Dark Web? You still have to find the bad guys, where the weapons are coming from, and who wants to buy them. Usually, we can do it easily. As cops, law enforcement agents, or intelligence officials, we try to buy them—and be the first to buy them. Sometimes, we are going to be the sellers. These are classic games that everybody plays on the web.

Millions of people are using the dark web, where it becomes common and normal to be fully anonymous. This is like walking down the street wearing a balaclava without having to worry about being stopped by the police or being required to show an ID. So, we will have to work hard to develop methods to de-anonymize—technically, tactically, covertly, or openly—in order to find ways to get the bad guys. Sometimes, there are very simple methods.

Nicknames are very important to hackers. Perhaps they used the same nickname 10 years ago on Facebook, giving us a way to find them.

As to hackers, their nicknames are very important to them. They often cherish them so much that they keep them for years. Perhaps they used the same nickname10 years ago when they created an account on Facebook. Hurrah! This is not rocket science, but it is a way to find hackers. As to more advanced techniques like the anonymization of hidden servers, some of them are badly configured so finding them is a piece of cake; but, of course, some of them are really difficult to find. Doing so is kind of fun, but you have to buy Zero Days and they cost a fortune. That is going to be a problem for enforcement officers outside the US.

The Dark Web is already changing, for example by providing super secure means of communication. Some companies are selling secure phones for criminals. Perhaps you have heard of PGP encryption (Pretty Good Privacy) on Blackberry phones with 70,000 users. Users encrypt to communicate among themselves. What can we do? You cannot infect them. This is very complex when you do not have access to the server. You cannot monitor the communications, because they are just SMSs.

There will be more and more tools that criminals can use, and we will have to adapt, which is just the daily job of law enforcement officers. It is relatively simple, but you need to have adequate budgets because otherwise, you are very much in the dark. For me, dealing with the Dark Web is also a daily job. This morning, we arrested seven people in two cases. One is a child abuser, which is horrible, and he was using Tor. Of the six others who have been arrested, we are sure that three of them were using Tor daily. I am not blaming Tor; and I am certainly not blaming the US Navy for inventing it. This is our new environment; we have to deal with it.

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

Mr. Andrea Formenti
Founder and Owner, Area SpA

Since we are just a short distance from Notre Dame Cathedral where a tragic fire broke out yesterday, I would like to express our sympathy to France and to the French people. We are neighbors who have been very close for centuries, and let me even say that we are brothers.

I would also like to say a few words about our company, Area SpA, which is an Italian private company with some multinational operations. Since 1996, we have been developing our software-based solutions for cyber intelligence. We work exclusively for government entities, by which I mean national intelligence and law enforcement. We have a solid background in lawful communications interception and communication data retention systems. 100% of our portfolio, and I am saying this in response to Colonel Nollet's remarks, provides forensic proof to our governmental customers. This facilitates attribution in the judicial sense, by generating information that may be used as evidence in a court of law. Of course, in many countries and even European ones, lawful interception of the contents of communication may not be part of the judicial process, but this depends on the country.

In some countries the creation of botnets is not only a crime but even using one is criminal.

We are cultivating strong cooperation with academia and, of course, primarily with our customer community. That's why I tend to understand and agree with the previous speeches. However, I would like to add that in the legal framework of some countries the creation of botnets is not only a crime but even using them is criminal. The trading of hacking expertise can also be a crime; using the Dark Web to buy, exchange, or trade certain hacking techniques can be a crime; even bulletproof hosting and creating counter antivirus services can be cybercrime.

Trading on the Dark Web can involve online payments, social engineering, sexual exploitation of children, forged documents, and the sale of weapons (even nuclear materials). Fortunately, an important Finnish marketplace on the Dark Web, Valhalla, has now been shut down. According to the available public information, it had been in the control of the police for one or two months—permitting the police to collect valuable information on the addresses of the buyers and sellers before closing the site.

Researchers discovered that the internet plays a key role in the smuggling of migrants. This is the so-called White Web.

As to the trading of nuclear materials, it appears that the costs to acquire uranium or plutonium through a Dark Web marketplace are so high that it would be financially impossible to obtain enough to present a threat. Most likely, sites offering such materials are honeypots designed to attract potential criminals rather than real trading posts.

The Dark Web is not the only concern. There is an important report by some academic researchers, including Italians, working in cooperation with European law enforcement on a very sensitive matter: the smuggling of migrants and human trafficking. After a great number of interviews and infiltration activities (both physical and cyber infiltration) about the smuggling of migrants, researchers discovered that the internet plays a key

role. Social media is important in the decisionmaking processes of potential migrants. This is the so-called White Web, not Deep, not Dark.

Social media facilitates the advertisement of smuggling services. Pictures and profiles run by smugglers on social media provide information on ways to travel. Information linked to migrant smuggling services on social media websites are easily accessible and give detailed information via mobile applications. Social media websites are used by migrants to post feedback about smuggling services and rank them, with comments such as, "It was good, it was effective, it was according to what they promised me," and so on. These social media profiles and information on markets are very effective. The internet is also used during and after the journey, of course, through very common encrypted communication applications. In the smuggling of migrants, the Dark and Deep Webs seem to play only marginal roles—mainly the sale of documents, passports and IDs. All the other activities are run on the normal internet.

Photos and profiles run by smugglers on social media provide information to migrants, who can even rank smugglers.

Of course, there are new challenges: you have read about cryptojacking, which means infecting people's devices in order to get control over their bandwidth and processing power for the purpose of mining cryptocurrency. It appears to be an emerging threat, according to European law enforcement authorities. Cryptocurrency also needs to be investigated since crypto wallets are vulnerable to attack. Of course, the normal financial services are attacked as well.

The new 5G technology for the mobile network is an important area of concern. It appears to significantly inhibit the attribution of suspects for law enforcement and security researchers, because 5G makes it harder to identify individual users. As an industry, we are very active in the European Telecommunications Standards Institute (ETSI), and the 3rd Generation Partnership Project (3GPP). Yet there are only about six countries that have been significantly active since the very beginning of the design of the 5G network. These countries defined all the network elements, including the software, the financial and the virtualization of the network function, with attention to security by design.

When buying on the Dark Web you need to understand that you are on the menu. You will very probably be exploited by a seller.

Education of the public is vital, but even industries and operators have been victims. Law enforcement needs to be involved, but it is not common in many countries. We need to cultivate deep technical education and awareness. And it is important to build relationships of trust with any cryptocurrency related businesses. Member states should increasingly invest or participate in appropriate specialist training and investigative tools.

From our point of view, when buying on the Dark Web you need to understand that you are on the menu. You need to know that you will very probably be exploited by a seller. You will get some malware on your computer as a result of your transaction, some of your information will be stolen, or your money will simply be taken without any results, without getting what you ordered on the dark web. Dealing with this reality is our role. There is no rocket science; there is no magic. It is hard work every day, but with great cooperation. That is why sharing ideas at events like this one is important, and to be one of the technologically trusted advisors of our customer community. We try to listen, to understand, and to transform needs into solutions that are useful to all relevant authorities. We always involve network operators and communications service providers. In this way, we try to make cyber and lawful interceptions provide a return on investment.

Geopolitical issues are important, especially in the coming 5G network. Some say that it will not be totally trustworthy. Network monitoring intelligence needs to be relevant, not just to help law enforcement in their investigations. It is also important for the network as an infrastructure to be less dependent on technology vendors and more autonomous. We have seen some installations where the operator was happy to learn that his network was working in an unexpected way, because the network was making excellent decisions. That is why introducing a lawful interception system into a network gives added value that will make the operator more aware of what is happening in his own network.

Monitoring the network passively reveals new trends and we are able to provide our customers with so-called content derived metadata. We have technology that is able to classify the layers of all the traffic. Of course, we have no access to the content, because everything is encrypted, but we do have information about the kind of traffic that is running on your network, the digital behaviour of your network, the behaviour of every subscriber, and of course the use of Tor and other kinds of services for the Dark Web.

And then there is the possibility of going active, perhaps through cyberweapons, or simply by enabling manipulations of the network session or infiltrating digital agents into the community. In other words, it is the digital way to do the second oldest profession, as some may say. The goal is to support link analysis and produce valuable evidence because, even if countries have different needs, it is best if information obtained is bulletproof from a forensic point of view, especially for attribution including geopolitical issues.

In closing, I would like to say that training is a very important part of what we need to do, and above all, we need to have cooperation and dialogue between all of us.

Invited Address

Mr. Jose Sancho
Chairman, Panda Security
Technology Partner

Since I am not a researcher and I do not belong to a defense institute, my view on cyber security comes from the perspective of an entrepreneur in a cyber security company.

First, the origin of cyber attacks has to do with digitization. Digitization is everywhere. As individuals, companies, or states, we all use it. The only difference is in its applications. Individuals use it for digital cameras, maps, alarm clocks or newspapers; companies use it for marketing and sales and for customer support; states use it, for example, for tax collection or elections.

So, everyone—people, enterprises and states—utilizes digital applications and these entities compete against each other: people compete against people for promotion in a company, for wealth, or for vanity reasons; enterprises compete one against the other for market share; states compete for gross domestic products and income per capita.

Since all compete for wealth, who wins the competition? Those who have more productivity. In the past 20 years, 80% of the productivity increase has had to do with IT, meaning hardware, software or communications. Although these seem like three very different things, all are based on software and, by definition, software is vulnerable. Even the most powerful computer, a quantum computer today, cannot thoroughly test just one program with 1,000 lines of code.

There are freelancers in the market who seek bugs in the software. They sell the bugs they discover on the free market.

If you think of an IT application, such as autonomous cars, they have 100 million lines of code. It is impossible to thoroughly test that software, which is the reason why software production companies have more people in quality assurance than in software development.

As part of the software ecosystem, there are freelancers in the market who seek to find bugs in the software. These freelancers sell the bugs they discover on the free market and some of them are even listed companies. Zerodium is one of them. It is listed as a Nasdaq company and is a market place for holes in the software. Quite often, the software producer, like Microsoft or Cisco, will plug the bugs, but at other times, companies or states will use these bugs to implement malware.

Malware and hacking are the sources of cyber attacks which are the criminal way to get wealth in a digital world.

Another source of cyberattacks is theft of identity and impersonation. Malware and hacking are the sources of cyber attacks, which are the criminal way to acquire wealth in a digital world. It is a new type of delinquency that has appeared because of digitization.

Who are the attackers today? There are three different families of attackers. The two biggest ones are the U.S. and China, because they have the most resources. Cybersecurity service companies in the U.S. that are listed on the Nasdaq employ 250,000 people that are dedicated on a full-time basis to U.S. intelligence agencies.

In China, the situation is less transparent but taking into account only what listed companies report, we can guess that China has even more people than the US who are dedicated to cybersecurity and with a more blurred line between state and enterprise.

Countries like Russia, Iran, or North Korea have an interest in influencing swing voters in elections.

The key point is that you need cooperation between governments, enterprises and industries. In the military, there is a similar situation for combat aircraft that are produced by engineers and operated by soldiers and for cyber weapons that are produced by hundreds of thousands of engineers. Of course, other actors can also buy cyber weapons on marketplaces. These marketplaces include stable countries like Russia, Iran, or North Korea that have an interest in disturbing other countries—for example by trying to influence swing-voters in their elections. Because of all the information available to them, they know exactly who the swing voters are and what kind of messages they are sensitive to.

Those states attack others. Actually, a major target is Europe which has the second largest concentration of wealth in the world, and is not well organized and structured. To give you an example: last year, one European country suffered 110,000 attacks as reported to its national CERT. Of those 110,000 attacks, 1,000 came from the intelligence services of other states and they were directed to very specific public administration or defense institutions. Some of these attacks have been reported in the media.

Many attacks are based on cheap weapons, like WannaCry or Petya that have been stolen from the biggest states.

So, out of the three types of actors, the two biggest ones are states using cheap weapons. Other actors, enterprises or individuals, are the authors of these 110,000 attacks that I mentioned above. The vast majority of these attacks are for profit and many of them are based on cheap weapons, like WannaCry or Petya, which have been stolen from the biggest states.

What is the defenders' landscape today? Since attackers have a huge advantage, what can defenders do on their side? We have products like the ones my company produces, but the typical software development takes at least three years and our laboratories detect more than 100,000 new malware samples every day. That means that every day, the malware producing industry is growing faster than the speed at which we can produce software. The other characteristic of these products is that they are global. Once you have a product, you have the means to defend against all the malware coming from that source at that time. This market is worth $35 billion per year in revenue.

Before 9/11, it seemed impossible to fight against money laundering because people were behind rogue states.

The other side of the industry is services. As it takes three years to develop a new product and new attacks come daily, we need services based on people in order to prevent and defend against those attacks at the local level. Globally, that market is about $45 billion, which is larger than the products' market. In terms of people, it means 600,000 people working in services. I think that China has more than that and the U.S. is probably on the same level as China. We know for sure that it is at least 250,000 people. This gives you an idea of why we have attacks, what the landscape is for attackers, and what defenders can do.

How can we progress towards making that situation more controllable? An analogy should give us an idea on how to proceed. The analogy is money laundering. We need a trigger and the trigger for dealing with money laundering was 9/11. Before 9/11, it seemed impossible to fight against money laundering because people were hidden behind fake enterprises and theoretically resided in rogue states. If you have access to the whole chain of money, however, it seems impossible for one autonomous state to go to war against another.

In response to money laundering, the key words became "last beneficial owner." The tax authorities want to know who is the last beneficial owner, who is behind the enterprises, who is behind the states? The last beneficial owner is the one getting the money and putting it into his pocket. Who is the last beneficial owner of Facebook? Probably Mark Zuckerberg. Even if you buy 99% of the shares of Facebook, the one who will give the orders at Facebook will be Mark Zuckerberg because that arrangement was established at the time of the IPO. Who is the last beneficial owner of Google? Larry Page. It is very clear in the by-laws of the company. If you can find the last beneficial owner and follow the chain, you will find the enterprise, the IP address, the telco operator and the state. This chain in cyberattacks is analogous to the money laundering one. Of course, we will need specific legislation to make it possible to follow the chain and the capability to enforce those laws.

If you can find the last beneficial owner and follow the chain, you will find the enterprise, the IP address, the telco operator and the state.

So, in my simple view, what is the way ahead? It is again based on another analogy which is deterrence in nuclear weapons, which is achieved by global cooperation among states. We have to uncover the delinquent IPs behind the companies and behind the last beneficial owner. For people, there are laws, penal laws and criminal laws; for companies, there are mercantile laws; and for states, international laws. Adequate laws need to be applied in each case. We also need to regulate telcos and social and advertising companies related to security or manipulation issues. I do not think it is easy, but it is feasible with today's technology.

We need to regulate telcos and social and advertising companies related to security or manipulation issues.

To continue with this analogy, we need global cooperation, mutual reciprocal monitoring surveillance and we need to enforce the laws. How long will that take? Over the last five years, every Sunday's *Financial Times* has advertised houses for sale in the Isle of Man or in the Bahamas. The reason for that is very clear: the Bahamas and The Isle of Man require physical residence over 50% of the time to benefit from the laws that shelter their residents. So, this shows what tax evaders have to do. And is there is legal enforcement to prevent it? How long will it take for us? Fifteen or 20 years? Of course, we need a trigger and WannaCry was big but not big enough to provide the necessary trigger. I am not saying that we need an equivalent to 9/11 but we do need a trigger. If we have that trigger, we will probably be there in 20 years.

The EU is important, but the big states in it are probably more important: Germany and France, as well as, Italy and Spain.

To conclude, what should Europe do in the meantime? First, in Europe today, we are probably without influence because the biggest actors, China and the U.S., can act with one single voice. In Europe, that single voice does not exist. First, we need that cooperation between states and enterprises. The EU is important, but the big states in it are probably more important, they are the tractor ones. By that, I mean Germany and France and, on a secondary level, Italy and Spain. As to the UK, let's see what happens with Brexit: the UK could be very important for cooperation between states and enterprises.

As point number two, we need to achieve leverage through our products. Of course, the U.S. has more people than the whole services industry together, and in products, they have 80% of all the product revenue. And the last beneficial owners of these companies reside in the U.S. and they are governed by U.S. legal rules. So, we have no equivalent to the level of strength that the U.S. or China have with Huawei or Qihoo. We need leverage for our products.

Another point is that, in Europe, we need to lift some constraints that we have on budgets. If a company wants to win a bid to supply a public administration, it probably has to fight on the basis of price against American companies who will know better than us how to win in this context. So, we need cooperation. There is a clause that can be used for cooperation, a national security clause, but it is very rarely applied in Europe. We need to fight for it to be used, because you have to keep in mind that the root cause for cyber-attacks lies in a human condition that will always be there. Because software will be there, hackers will be there. That human condition is greed, and the only way to counterbalance that greed is to be linked to another human condition, which is fear.

In Europe, there is a rarely-used national security clause that can be used for cooperation, and we need to fight for it to be used.

Invited Address

Mr. Emmanuel Chiva

Director, Defense Innovation Agency, French Ministry of Defense

I am here to talk about innovation and to explain to you what the national strategy is in terms of the French National Defense Innovation Agency. Although I am not a science fiction writer, I would like to do a little science fiction with you.

Let us project into 2050, for example. Let us imagine that governments have disappeared. They are replaced by social networks, sovereign social networks governed by artificial intelligence using deep fakes techniques to impersonate their leaders. Each citizen needs to communicate his personal data. Those who do not are considered to be criminals. Some countries such as China, the U.S. or France are trying to resist and are developing new means. For example, China has decided to prohibit entry to its naval domain by deploying hypersonic missiles able to prohibit entry at range of 2000 kilometers.

In 2050, let us imagine that governments have been replaced by sovereign social networks run by artificial intelligence using deep fake techniques to impersonate their leaders.

Space is constantly monitored using constellations of nanosatellites manufactured by private companies without any government link. Space is weaponized by using directed energy weapons able to neutralize any incoming threat. In addition, quantum computers are operational. Cryptographic codes are not secure any more, except for those who use post-quantum cryptography. Nice future, right?

All those examples could feel like science fiction but, actually, it is something that we need to prepare for. It is very serious and could be a foreseeable future. So, we need to anticipate. There is a sentence that I like from Woody Allen: "We are all interested in the future, for that is where you and I are going to spend the rest of our lives."[4] That might seem like a joke, but he ponders the question of choice. Do we have choice? Do we have the luxury of trying not to anticipate? Could we consider that innovation is not a priority?

Actually, the Minister of the Armed Forces, Florence Parly, recently gave the answer in a conference organized by the IHEDN in the French parliament. She said that innovation is not a question of choice. It is a question of survival. So, we need to anticipate. We need to innovate. We need to imagine beyond the present. We need to break through the "wall of imagination," which is very difficult to do because technology has invaded our everyday life in such a way that it becomes very difficult to anticipate, to project into the future. Flying cars are already there. Artificial intelligence and robotics are invading the defense industry. Laser weapons are not science fiction anymore. But what will security be like in the future? What will be the art of war in 2050? I do not know if you can answer this question, but I cannot.

The French Minister of the Armed Forces, Florence Parly, said that innovation is not a question of choice. It is a question of survival.

[4] Originally from the 1959 film, "Plan 9 from Outer Space."

So, we are trying to organize our innovational efforts in response to the reality that our world has changed. I would like to spend a few minutes on that before describing to you how we are organizing and our way of dealing with this new situation.

First of all, what was once sovereign no longer exists. Twenty years ago, communicating on the battlefield was a military privilege. Today, on each and every battlefield, you can see ISIS using networks and smartphones. Who could have imagined ten years ago that you could build your own satellite and task an Indian launcher to put it into orbit for hundreds of thousands of euros—which is an insignificant expense by past standards? At the same time, we see the emergence of new economic giants that transcend governments, that transcend entire countries.

If I ask anyone in the street, "Who is the worldwide champion in artificial intelligence?", they will not tell me it is the French Inria, which is the national lab for research on artificial intelligence. They will tell me Microsoft, Google, Facebook, or Apple which is normal because those companies are putting incredible amounts of money into their R&T. I have tried to find out how much a company like Huawei is spending every year. The answer is around $20 billion, and it is $11 billion for Apple.

What keeps us awake at night is that we could miss the next technological revolution. If we wait too long, innovations become accessible to our opponents.

This is concerning but, at the same time, it creates opportunities because those companies invest in domains that are of interest to our minister. We can certainly benefit from this incredible push for R&T: Civilian virtual reality, augmented reality, artificial intelligence, and cyber technologies are pushing the market. One problem, however, is the fact that these opportunities are available to everybody, including our opponents. So, what keeps us awake at night is that we could miss the next technological revolution and our enemies could capture it before we do. If we wait too long, all those innovations become accessible to our opponents. If we look at what is happening in the Sahara/Sahel today in the Mali region, we see weapons printed using additive manufacturing techniques; we see the use of UAVs with explosive payload; we see cyber-based attacks on our forces. So, this is a main concern. Those new opportunities come along with new threats.

Since the world is changing, there are technological disruptions that can foster strategic disruptions: I am talking about quantum technologies; hyper-velocity, high-energy weapons; biohacking; and, of course, cyber technologies. However, I am not convinced that everything is disruptive. There is a sort of myth about disruption. Artificial intelligence is not a disruption, and it has been known since the year 1950. What is disruptive about AI is that it works today because it can take advantage of data, because of computing power, and because of new algorithms. The real disruption is that it works. Quantum technology is also a real disruption, but hyper-velocity is not. So, there is a sort of myth about disruption that says it will shake the entire landscape and all the traditional actors will disappear. I do not think so. Instead, I think they will adapt. In Paris for example, there are taxi cabs and there is Uber. There are restaurants and there is fast food. Not everything is about disruption—This is just a small observation that I wanted to make.

Therefore, in France, we need to imagine, accelerate and anticipate. We need to organize ourselves, hence, the inception of this new National Defense Innovation Agency that I have the honor of managing. This agency, in French “Agence de l'Innovation de Défense (AID)” is a national service attached to Mr. Joël Barre, the head of the Direction Générale de l’Armement (DGA).

We are not a huge number of people—around one hundred approximately—because our goal is not to generate innovation. Our goal is to organize the innovation. Our personnel comes from the DGA, from the joint staff, and from the SGA, which is the General Administration Directorate of the Ministry of Armed Forces. We have approximately 40% women and we are based in Paris in the Ministry of Defense. Our budget is €1.2 billion per year, which is the necessary funding for the studies that will develop our future capabilities. It includes the financial mechanisms that we have developed to support both innovation and capture innovation from the civilian world.

It also includes the funds that we inject into national operators: We have the governance of the ONERA, which is the French National Center for Aerospace Studies. We have the governance of the ISL, which is a joint German and French research institute. We also have the joint governance of the CNES, the National Center for Space Studies and the CEA, which is the Atomic Energy Directorate for dual-use research. And last, this budget also includes what we inject into the MOD-governed schools. We have four schools under the governance of the Ministry of Defense.

Our new mission is to capture short-cycle innovation, that is, civilian innovation that we can inject into our armament programs.

So, €1.2 billion to do what? Well, our missions are to orient R&T, to decide what will be the allotment of finance and the national priorities that we want to push forward. Today, we have clear national priorities such as artificial intelligence, cyber technologies, intelligence and space. Our goal is to be able to propose to the minister the yearly orientation of the military R&T. We act as an orchestra conductor to be able to ensure the consistency of all the mechanisms that support innovation. But we have a new mission: to capture short-cycle innovation, that is, civilian innovation that we can inject into our armament programs. And our main goal is to accelerate innovation. What we target is the rapid deployment of innovation for the benefit of our operational users. In order to complete this mission, we have organized the Agency in four divisions.

The first one is called "Defense Technologies and Strategy." The goal here is to prepare the technologies that will ensure our future capabilities. They are our next big armament programs, our next aircraft carriers, or the next future air combat system. This division is also focused on international cooperation. I was in the U.S. one month ago and I was very surprised to see that all the agencies like DARPA, DIU (Defense Innovation Unit), the Marine Corps Logistics group or the armies labs are all ready and eager to cooperate with us (as we are open and ready to cooperate with them). I will go to Germany, to Sweden, and I went twice to the UK: We are trying to develop an international network of cooperation. We will also integrate with the NATO innovation hub to be able to benefit from this network.

The goal of our Innovation Defense Lab is to be able to accelerate projects by providing resources—in order to rapidly have a minimum of viable products that can be tested by the armed forces.

The second division is called "Open Innovation." Open innovation, for us, is everything that is external to the ministry: How to capture innovation, how to ensure that the innovators come to us. Our agency is a Single Entry Point for all innovators who want to work with the French MOD. We have gathered in one single entity all the support mechanisms that we use to be able to accelerate innovation.

We are also developing new tools. The first one is called the Open Innovation Cell, which is a dedicated team, something a little bit comparable to what the US is doing with the DIU. The goal is to go “hunting and fishing”.

Hunting is, "You know the game. You know the target. You are looking into the eco-system to see if there are some civilian innovations that can answer that need." Phishing means that you just launch a net and you see what comes to the surface. For example, we sent a team to the CES show in Las Vegas to be able to identify the innovations that could be useful for us.

Also, we have a new tool called the Innovation Defense Lab, which we decided to build primarily to speed up experimentation. It was inaugurated by the minister last November. The goal is to be able to accelerate the projects by providing resources—it can be experts, it can be financial support, it can be experimentation facilities—in order to rapidly have MVPs: minimum viable products that can be tested by the armed forces. We also host the DGNUM (MoD digital command) : a digital factory that is embedded within the Innovation Defense lab. We are working with the labs within all armies—cyber, space, land, sea and air—and we have a new place that is open to the public. This means that if we want to capture civilian innovation, you will be able to come to us without giving your proposal three days in advance and going through security guards. We have an office within Paris, 10 minutes from the ministry, in which we can organize hackathons, launch challenges and organize international meetings.

Our third division is finance and acquisition. To do all this, we have developed this division because we need to be able to accelerate our contracting mechanisms and we need to take risks. However, we know that buying and taking risks is something contradictory in the Ministry of Defense. This will require a change of culture. At the same time, we are conceiving a *contract factory* in order to imagine new contracting tools to speed up innovation.

The fourth division is focused on communication and also on valorization. The main idea: to act as a trusted party and build business models with the innovators. They need to know how they can make money with the ministry of defense, otherwise, they simply will not come. The Agency needs to work with the innovators to protect them, to make sure they will have a viable business case with the MoD.

We are on a fast track. The agency was created in September and it was fully operational in December. Last November, we organized the Defense Innovation Forum which was open to the general public for the first time. Next week, we will give to the Ministry of Defense our strategic plan, targets, priorities and the underlying mechanisms.

We already have some results. In January, we launched an accelerated call for projects in the field of artificial intelligence. The candidates only needed to give us a one-page proposal to enter this competition. We selected 163 projects for review; after a one-week selection process, eight of them have been selected to be accelerated and are now funded. We have organized a robotics challenge in the urban environment and made it possible in one month instead of the 18 months this would have taken in the past. And we have organized a space and artificial intelligence challenge which we will talk about at the coming Paris air show in June.

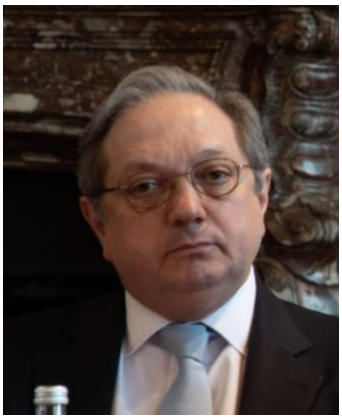
We are here to dare, to accelerate and to imagine the future. We are supported by a strong political will because we do not have a choice.

To conclude, I will leave you with three important words. The first one is *to dare.* During the Defense Innovation Forum, we managed to make a soldier fly over the river Seine using a flyboard. This was very difficult to organize because everyone had a good reason to say, "It is not possible to let one guy fly in Paris over the river." So, this helped change the regulations. Today, we are writing a new regulation allowing for innovative systems to fly, which is a nice achievement. Innovation is not only about technology.

The second word is *to accelerate*, and the third one is *to imagine*. If I ask for example, "What will be the future main battle tank?" you will tell me, " it will be a battle tank with new armor, new camouflage capabilities, or a new weapons system, new optoelectronics." In summary, the next battle tank is… a battle tank.

There are some people who do not think that way. Just to give you an example, we are working with science fiction writers and science fiction authors to be able to think outside the box and to help us imagine the future innovations and future threats we will face. So, science fiction is something that we want to develop into the Defense Innovation Agency.

We are here to dare, to accelerate and to imagine the future. We are supported by a strong political will because our soldiers rely on us, and because we do not have a choice. If you allow me one last sentence, I would say that "Ships in the harbor are safe but that is not what ships are built for."



In Democracy We Trust?

Russian Cyber Influence Operations: Finding Ways to Secure our Electoral Systems and Defend our Democracies

Ambassador Luis de Almeida Sampaio
Permanent Representative of Portugal to NATO

The title I chose for my intervention is "In Democracy We Trust?"—with a big question mark! This is indeed a key question for our public opinions.

To make my case let me start by making a parallel with a very important lesson I learned from General Denis Mercier, the former Supreme Allied Commander Transformation (SACT), the first time I visited him at his headquarters in Norfolk, Virginia. He told me that every military wartime commander's worst nightmare would not be to look at the computer screens in his command post realizing the enemy had succeeded in turning them off or making them blank. That would be grave but not catastrophic, provided back-up systems could be made available at short notice. However, the real catastrophic situation, every military wartime commander's worst nightmare, would rather be to look at the screens of his command post and see a "reality" that would actually not reflect reality—in other words, that particular commander would be making decisions based on information that he should not have trusted; he would be taking action based on information designed to deceive him. Now, imagine for a moment the implications of cyber or hybrid attacks designed to make elections and polls unreliable so that what you see would not be true. Imagine that you could no longer trust your country's electoral process and its results. The electoral systems would be in jeopardy, democracy would no longer be possible.

Trust is the most important commodity that exists anywhere in the world, including trust in the voting process.

Indeed "Trust" is an extremely important commodity. If "Trust" would be rated in a stock exchange, it would be more valued than gold, or oil, or Google, or Microsoft. For our democracies, "Trust" is really the most important commodity. To be able to trust the voting process—and not just to be able to trust the mechanical voting system—depends on being able to be sure that the results reflect truly the voters' choices: protection of the voters' lists, information about candidates, and awareness must support the decision-making process.

This is already a lot, nevertheless it is not all. In fact, there is also the need to trust our critical electoral infrastructures. We need well-protected and very resilient systems in support of the electoral process. Thus the need to invest evermore in cyber security, specifically to invest in the ways and means that are key to the protection of those critical electoral infrastructures. In the meantime, maybe we would even need to consider going back to paper backups. It would be lengthy, but feasible and affordable. What we cannot afford is the loss of confidence in the mechanisms of the electoral process, the loss of trust in our democracies. It is also vital that we trust the information space. Accurate and reliable information is an indispensable guarantee to permit a conscientious choice by the voters. If they do not have accurate and

We must reflect on the eventual need to go back to paper backups for voting systems.

reliable information, how could we claim that they are making a conscientious choice? How to can we achieve that? How to can we protect the "Trust in our Democracies"? This is the most difficult to achieve. Most likely, no one has all the answers on how to do this today. Nevertheless, let us try at least some preliminary thoughts:

For starters, we need a holistic approach. Different agencies and entities need to be involved in a very well-coordinated manner. What I mean by this is *international* coordination. Which doesn't exist as we speak.

Freedom of speech, open societies, and open internet are at the core of our way of life. Because of that, our democratic systems have, inscribed in their DNA, an "Achilles' heel" when it comes to protecting what trust in the information is about. We will need to balance protecting freedom and fighting disinformation campaigns. We need to assure the blockage of fake news and at the same time, we need to protect vital data and their dissemination.

Trust in the information space is the Achilles's heel of our democratic systems.

Again, we can only do this in a very coordinated manner, involving the private sector, social media platform holders, journalists, analysts, think tanks, and academia. We need to agree on international norms of State behavior. We need to legislate inside our national cyberspace. Where do we place the threshold between controlling rules and preserving freedom? For autocratic regimes, many, if not all, of these concerns do not apply. The example of Russia immediately comes to mind. It is a fact that Russia is becoming very prominent in controlling rules without caring about preserving freedom. Moreover, Russia is not the only case.

So what can we do? What can NATO do? We need to protect ourselves; we need to protect our open societies from their enemies. In addition, we should aim at deterring them from messing up with our democracies. Moreover, in the event deterrence does not work, we need to be ready, politically and technically, to retaliate.

Is it possible for everyone to abide by the minimum requirements that would make all of us safer and more secure?

We also know that, in the cyber threat domain, we are as strong as our weakest link. This is an observation that is very often repeated by experts, by people that dwell daily with cyber security and cyber defense related matters; but, if it is true that we are as weak as our weakest link, then the question of benchmarking immediately comes to the forefront.

Is it possible to establish benchmarking in cyber defense? Is it possible to ensure that, in the context of a defense and political security Alliance, like NATO, everyone abides by the minimum requirements that would make all of us safer and more secure? Could those benchmarks be included in the NATO defense planning process? Could we establish capability targets for the NATO nations that would oblige them to meet those minimum benchmark-related requirements?

That is one of the many key questions that we are starting to address at NATO, and it applies not only to cyber but also to hybrid threats. For the time being, I hope that these short remarks of mine will contribute to prompt an interesting debate.

The Imperative of Societal Resilience

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

Efforts to manipulate and influence electoral processes are aiming at the heart of democracy. Elections are not only at democracy's core, but elections occur at a concentrated moment in time when large numbers of people are declaring their political priorities. Therefore, elections naturally invite this kind of activity.

Of course, democracy is about much more than just elections—it is about the division of powers, about the rule of law, about checks and balances, about the rights of minorities, about solidarity in society, and so on and so forth. But elections are also some sort of milestones that impute legitimacy to power for a certain period in the future. These are additional reasons why elections are very sensitive targets.

Now, concerning Russian influence attempts and other activities, we have heard a lot of examples, but only in general terms. Therefore, I hope that Janis Sarts will describe them in more detail, because his NATO Center of Excellence is dealing with them every day. It seems that we have learned to a certain degree to live with the assumption that, whenever there is election, we should expect manipulation. And it also seems to me that Russia's effectiveness has been diminishing. In fact, there have even been elections where we expected Russian manipulation and it did not happen. Perhaps it is possible that the mere fact that there were preparations for Russian intervention—and that there were warnings in advance of the elections—could have had a sort of a demotivating effect.

Russia's effectiveness in cyber influence operations has been diminishing. In some elections, their expected manipulations did not happen.

There are talks about how to deter these kinds of activities. However, I actually believe that in the realm of political processes and societal resilience, it is very difficult to deter. We now have rather well-developed procedures for deterring cyber operations that could potentially result in massive physical disruption. In NATO we have even agreed to the possibility of activating Article 5 if necessary. But in the much more ephemeral and much less material realms of electoral processes and democratic institutions, deterrence does not work.

We have not identified outright efforts by China to manipulate our electoral processes, but they might have interest in European Parliamentary elections.

I am deeply convinced that what actually works, beyond short-term measures, is being prepared to disclose, to attribute, to name, and to shame those attackers. The long-term remedy or mitigation lies in the area of *societal resilience.*

While we have been speaking about Russia, I would like to also mention another adversary that is emerging very rapidly: it is China. We have not yet identified outright efforts by China to manipulate electoral processes. Nonetheless, there have already been indications that they might have some special interest in the context of the coming European Parliamentary elections.

But why is China more of a concern than Russia in the long-term? Russia is relatively straightforward; Russia is more opportunistic; Russia is also more brutal. We should not forget that as a result of Russian hybrid warfare there are actually thousands of people who have been killed, be it in Ukraine or elsewhere. Russia does not hesitate to use terrorist methods: I have in mind the Skripal affair in the UK.

China has a much wider variety of instruments to weaponize information, investments, education, and even entertainment.

China is much more sophisticated: They have a long-term strategy; they have long-term thinking; and, indeed, China has a much wider variety of instruments available to weaponize information, investments, education, and even entertainment. This means that China is a really big threat, and I am worried about the day when it enters another much more open and blatant phase of hybrid warfare against us. This concern is especially worrisome because of the technological dimension: China is now testing a whole new system of societal control in its country and, indeed, all these technologies, all the instruments that one can imagine and that China is developing for manipulating its citizens could also be used for manipulating our own processes, our societies, and our cognition.

***Societal resilience* is the key. We see in Europe societies that are resilient, and resistant to the efforts of Russia or other external actors.**

To come back to my initial points, *societal resilience* is the key. We can actually see in Europe that there are societies that are homogenous, that are coherent, that are resilient, and that are resistant to the efforts of Russia or other external actors. For societal resilience, the main aspects or values are indeed trust in society, trust in institutions, trust amongst people, solidarity, a sense of belonging, the fight against exclusion, etc. These are the positive elements that prevent fragmentation, polarization or exclusion without society.

The Future of Russian Digital Influence

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

Why are we having this debate about problems with elections and election influence? After all, the subject as such is not new. It has been around for quite some time, but it has not been a major issue for the last 20 to 30 years. One of the key reasons for the current debate is that there has been a change in the patterns of information consumption in our societies.

In any given NATO country, between 60% to 80% of the citizens consume information digitally. This is a very sizable number. Of course, TV is still important, but the social media and the online environment are what shape the emotional landscapes. In fact, when we look at recent elections—and I am referring to some in our region, the Nordic Baltic—we see that the political players who develop successful digital strategies are the ones that have the winning hand.

Checks and balances that were developed with traditional media and within democratic environments are not working.

In fact, sometimes even very established political players who have relied on traditional ways of campaigning lose heavily. So, you can see that this digital space is an increasingly important element in the framing of people's perceptions and their behaviors. Unfortunately, this shows that a lot of the checks and balances that we have developed in a normal information space with the traditional media and within democratic environments are not working.

At our NATO StratCom Center in Latvia, we recently released a study that is called the "Black Market of Social Media Influence." What we found was really shocking: As an example of one of the points that we were able to make, and in course with the agreement of a U.S. Senator, we were able to buy, from a Russian company, custom made comments on the Senator's Facebook feed and Instagram page. They were delivered in 15 minutes for $10. We reported that to Facebook. At first there was no response from Facebook, but at the end, we were able to meet face-to-face with their security team, and then they finally started to scramble to understand how it happened.

For a very cheap price with social media, you can manipulate individual threads, manipulate algorithms, and you can trick algorithms.

This is just a simple example, but all the infrastructure necessary to do such things is available at a very cheap price in Facebook, in Instagram, and in YouTube. You can deliver manipulations as you wish: You can manipulate individual threads, you can manipulate algorithms, and you can trick algorithms.

Do you want your YouTube video to trend? That is a service you can buy. Do you want your hotel to be very highly reviewed? You can buy it. Do you want to influence the way a newspaper writes? You can do that, too. Just think about this a little, and you can see how it is possible: Most of the big newspapers rely on their web pages to determine what people are interested in. These web pages give you the means to game what they

think most of their readers are interested in. This permits you to actually lead the *New York Times* in the direction you wish it to go. And that service is available and it is cheap.

Unfortunately, the infrastructure that permits such manipulations is vibrant. It is present all over the world, and these well-established ecosystems are available all the time. Of course, companies like Facebook and YouTube are trying to build safety mechanisms, but our observation is that it only takes about two weeks to circumvent them. And there is another very interesting fact that we have discovered concerning the future of Russian influence operations: All of the software that is necessary to create these bot systems is Russian made. There are even Indonesian bots or Indian bots that rely on Russian software, and this is important to understand.

Companies like Facebook are trying to build safety mechanisms—it only takes about two weeks to circumvent them.

A second element that I want to quickly touch on is data. We have all heard about the importance of data, including the story of Cambridge Analytica, which in my personal perspective has been overblown. From my perspective, they were not able to deliver as they claimed. But I think that data is the way that human behavior is going to be influenced in the future. Marketing companies are doing that all the time, and, yes, we accept that as part of the game as it currently exists. But then, where are the limits to what is acceptable? Is it all right to trick people to influence their behavior in the political and election contexts?

Data is the tool that will be used to influence human behavior in the future: where are the limits to what is acceptable?

As a small illustration of what data can deliver, we recently teamed up with one nation's armed forces during a military exercise. By using only open source data that is freely available, we attempted to see whether we could tell who was participating in an exercise, what was taking place during the exercise, whether we could use these datasets to shape the behaviors of the soldiers.

As to these three goals, first of all, we were able to discover almost all the details of an exercise, including classified ones. We were able to identify about 15% to 20% of all the participants by name. Finally, we were able to do searches on the kinds of data that you might normally be able to find on those individuals. The results of these searches were very rich and that enabled us to make soldiers disobey their orders, or leave the positions that they were supposed to defend in the framework of the exercise.

Our concerns are actually not about the military, because I trust that, one way or another, the military will find ways to secure the access to these individual soldiers at critical times. But our greatest concern is about the society, about our electoral commissions, about municipal officials, and about people within the government that can be really susceptible to these behavioral manipulations.

Our greatest concern is not about the military but about our societies that can be really susceptible to these behavioral manipulations.

When we think about the manipulation of behavior, it is easy to forget the fact that we act for the most part instinctively and emotionally when we develop our points of view and make decisions. Since we very rarely

act on a purely rational basis, when somebody uses neuroscience research methods, it is very easy to achieve behavioral changes. We will have to deal with systems that automate these database-influenced campaigns *en masse*, with 10,000 people on areas that are specified by geolocation, etc. In my view, this is what is coming.

On top of that, we have to be aware of the devastating effects that deep fakes are going to have on political discourse, and it may be only two years away. Think about what will be possible with deep fakes—faking audio and everything else—without any technical means to tell the fake from the real. Well, that is going to be a significant blow to trust and to our democratic processes.

Think about the future of bots in the online environment, the marriage of a typical bot with a Siri or Alexa type technology. That is going to be really, really tricky to deal with. And think about the merger of Big Data, AI, and the recent research on the human decision-making processes. Along all of these lines, I see actors like Russia developing their capabilities.

Nonetheless, I think that China will be the really big actor down the road. Their social scoring system, for example, is basically about combining Big Data, AI, and surveillance technology to influence and control behaviour. Think about the capability they are going to develop! At this point, China is using these capabilities internally, but they will have the capability to act internationally if they decide to do so.

So, there are growing risks for our democracy. It is partly because of the way the environment has changed and partly because it is now easier for malign actors to operate in this new environment. The actors with the technological capabilities will be really the ones that we have to really consider.

What should we do to fix it? First, self-regulation is not working. If it only costs the price of a hamburger to manipulate a U.S Senator's newsfeed, that is not acceptable. So there has to be some kind of regulatory framework. Hopefully, the new EU Commission is going to start working on this. I also hope that the U.S. Senate will consider some of the issues. In any case, we have to find a way to implement transparency, accountability and oversight of the Big Data companies.

We need to develop data awareness: Do governments know where the data from within their societies are going?

The second thing we need to develop is data awareness, both by individuals within our societies and by governments. Do governments know where the data from within their societies are going? They certainly need to know if it is going to China or to Russia, although I think it is far more complicated than that. But, at least we need to know. Personally, I believe that we should act as if we think the data is going to some of the most harmful places, which might not be based on market logic, but which may very well be the case. And lastly, we need to develop the capabilities to achieve the necessary control over our data.

We used to be concerned only with cyber security, but a Pandora's Box has been opened. New threats and developments are emerging all the time, and we have to keep abreast because, next year, we may face new vulnerability that we have never considered. This approach has to be built into our DNA.

Digital Elements of Converging Technologies—Some Security Implications of the Fourth Industrial Revolution

Dr. Linton Wells II

Executive Advisor, C4I and Cyber Center and Community Resilience Lab, George Mason University; Former acting US Assistant Secretary of Defense for Networks and Information Integration and Chief Information Officer

In the context of the World Economic Forum's Fourth Industrial Revolution concept, I would like to address some of the digital elements of converging technologies. The basic premise of the Fourth Industrial Revolution is that a combination of accelerating and converging technologies is blurring the boundaries between the digital, the physical and the biological spheres. What does this mean from a security perspective?

Cyber resilience recognizes that your networks are vulnerable, and may be penetrated, but you have to keep operating.

The digital sphere, includes developments like artificial intelligence and machine learning, "big data" analytics, cloud computing, and automation. If you have not seen it, I recommend the US Defense Science Board report on automation. It is unclassified and it makes a very interesting distinction between autonomy in motion and autonomy at rest, which is worth looking at. From a security perspective I prefer to think in terms of cyber resilience as opposed to cybersecurity because security has an implication of locking down and trying to keep bad things from happening while resilience recognizes that your networks are vulnerable, and probably will be penetrated. Yet you have to keep fighting after you have received damage. How do you do this? These are core questions that need to be adapted not only to today's networks, but also to advanced mobile wireless, 5G, the Internet of Things (IoT), distributed ledger technologies such as blockchain, the whole world of financial technologies and, eventually, quantum information science. All these fit into the digital sphere.

Intersecting with the physical world are approaches such as advanced manufacturing, including 3D printing, various kinds of new materials that lead to all sorts of new antenna technologies and related things, and then autonomous systems as I mentioned earlier.

Linking the biological sphere with the physical and digital worlds are areas like synthetic biology, the ability to print artificial organs, which are already being implanted, and genetic engineering. The point is that there are many security-related technologies that are wrapped up in the Fourth Industrial Revolution construct.

All of these are going to be affected by accelerating and converging technologies. If you pick some parameter, say computing power per unit cost, and it doubles every 18 months, which is about what it is doing now, in a year and a half you have 100% more capability. But in five years, it is 900%, in 10 years, it is 10,000% and in 15 years, which is only to 2034 now, you have 100,000% more capability. I have no idea what 100,000%

more capability means for an iPhone, but I am sure I am not going to be carrying a brick like the present device around with me.

These curves may continue to accelerate, they may level off, or there may be step function jumps in capability, like quantum computing. The point is that we cannot rely on linear projections from where we are today. The future is going to be very different. This is what Tom Friedman has referred to as the "Age of Accelerations." In addition, these technologies are interacting. I like to think in terms of BRINE: bio, robotics, information, nano, energy, and how they work. If you add in artificial intelligence and advanced manufacturing, it is a very interactive, complicated world. Again, we cannot expect that linear projections will provide an accurate reflection of the future.

A British company, HawkEye 360, is selling maritime signals intelligence all over the world.

So, what does this mean from a security perspective considering the area of command, control, communications, computing, intelligence, surveillance, reconnaissance (C4ISR)? An explosion of information assets is coming from non-governmental sources: Just think of open source geospatial information and also of the fact that multiple commercial satellites are selling sub-meter resolution imagery. A British company, HawkEye 360 is offering maritime signals intelligence all over the world and a U.S. company, Capella Space, has joined several others in launching radar satellites. These are capabilities that once used to be the province only of governments.

In terms of unmanned aerial systems (UASs), the U.S. Defense Department operates something over 10,000 UASs. Beginning in 2015, however, our Federal Aviation Administration began to register drones in private hands. By early 2018 more than 1 million private drone operators had registered, and many may have more than one air vehicle. The number of drones in the private sector dwarfs the number operated by the Defense Department. In sum, the amount of information—we call it IV4: information volume, velocity, veracity, validity—generated by such systems and the 24/7 news cycle, plus social media overwhelms traditional intelligence collection methodologies.

Cellphones also are almost completely outside the control of governments. To this must be added the whole area of the IoT and all the information it is generating. None of this fits the traditional, structured, intelligence model of "task (a sensor). process (the inputs), exploit (the information), disseminate (the report)" (TPED). How do the pieces fit together today? The point is that our decision support systems for governments, and other functions, need to recognize that these assets that are out there in open sources and learn how to make better use of them.

The center of gravity of future wars may not be tanks and troops…but the minds and resilience of the populations.

Trust has been talked about a lot. What are the checks and balances in the digital sphere and how will they change in this "age of accelerations?" Consider a concept I'd like to call "cognitive-emotional conflict." Suppose that the center of gravity of future conflicts is not tanks, troops, artillery and command posts, but the minds and resilience of the population of the engaged states. Are our defense expenditures actually making us more secure in this space?

I think we need to pay much more attention to bio, not only bio-hacking but also synthetic biology, physical and cognitive augmentation, and neuroscience—the whole question about how our brains are responding to the diverse, sophisticated stimuli coming from social media. Information providers are very skilled at making us want to keep clicking in areas that generate revenue for them. How do we maintain some control in the face of this sophisticated manipulation? Also, how do our militaries actually take the extraordinary amount of research and development that has been done in these areas and transition it to acquisition and sustainability in ways that will match the velocity of the innovation, compared with our present structured, slow, acquisition of defense systems?

I think these developments present enormous opportunities, as well as challenges. The democratization of technology can make it hard for democratic governments to control information flows, but also can give small states a way to acquire very effective defense capabilities much faster than they could in the past. Put together, these could provide deterrents, particularly for the smaller, front line members of NATO.

Essential Collective and Individual Cybersecurity Components

Ms. Merle Maigre
Executive Vice President, CybExer Technologies

I will look at cybersecurity from the perspective of both the government, where I used to work, and the private sector, where I work now. I can say with absolute certainty that, in today's world, there is no way to understand security without understanding cybersecurity; and, in today's digitally dependent societies, people are the most important link. The role of people has a collective component and an individual component, and they are both equally essential.

It is a mistake to regard cyber technology as a support function rather than a core business instrument.

My first point is about collective decision-making in cybersecurity, that is, about boards of directors, managements, task forces, national governments and so on. It is essential to make the argument that cyber really is strategic and not technical. The principal mistake that I have seen so far, where the thinking goes off on a wrong track, is when cyber technology is regarded as a support function rather than a core business instrument.

This approach, for both the governments and the enterprises, leaves technology and security as something that the others—the techies, or the IT department—must fix. Thereby, it is a slippery slope because it hands off this critical responsibility to an IT department that in most organizations is really strapped for resources. I would claim that technology issues need to be management decisions, in order to avoid delegating everything as technical details down to the lower levels.

We need to train strategic-level decision-makers to solve a major cyber crisis without turning them into security engineers.

A related point is that collective decision-making at the top level is crucial. This is where things often get stuck—or, sometimes, even blow up. We need to train strategic-level decision-makers and provide them with the experience of having to solve a major cyber crisis without necessarily turning them into security engineers. We need for them to keep in mind the bigger picture and not get lost in the small technical details. One good example, where this notion was well understood by the EU and the Estonian Minister of Defence, was back in September 2017 when EU defence ministers gathered in Tallinn for the first ever cyber security table-top exercise, called CYBRID 2017. It included EU defence ministers and the NATO Secretary-General.

The key questions that the EU defence ministers asked evolved around four modalities: timeline, transparency, authority, and cooperation.

- "Timeline" was about how much time do you need to make decisions in a cyber crisis, and how far ahead can plans be made during a cyber incident or a cyber-attack?
- "Transparency" deals with the questions about public and media exposure of the decision-making during a crisis.

- "Authority" is about who in your organisation, be it an enterprise or a government, can execute decisions during a cyber conflict, in what circumstances should authority be delegated up or down, and whether you have the supporting procedures and legislation ready for it.
- And, finally, "Cooperation" deals with questions like, "Who are your necessary partners and allies? How can government and industry work together, and how much international cooperation is needed?

The goal of this wargaming-like simulation is to illustrate the set of decisions that the leadership or management of a fictitious country or a fictitious enterprise needs to take after becoming a target of a large-scale cyber-attack. The participants take part of this wargaming individually and respond to incidents individually. During the exercises, differences of opinion and suggested courses of actions are highlighted and addressed during the simulation instantly.

The aim is to create discussion and highlight different ideas and approaches, providing a realistic and engaging experience, but the strategic-level cyber exercises should not, surely, be only for the defense ministers. This should go beyond the defence community and include other areas—in national governments, among other public officials, and as well as in private enterprises, with supervisory boards, and executive directors—because raising awareness of decision-makers about cybersecurity is essential. A good way to start is to demystify cyber for the top leadership.

We have a cyber hygiene platform for all government institutions. There is a 45-minute online course for individual users.

I would also maintain that even the strongest and best coordinated collective and organizational response is not enough without effective individual response. This is because in today's digitally dependent society, people are the most important link. Here the rule is simple: independently of our jobs, our age, our level of responsibility, we all need some technical literacy at our own individual level to function well and not to pose threats to those around us.

Two years ago, the Estonian State Information Authority launched a learning platform for all government institutions. This is what we in Estonia call 'cyber hygiene.' At the level of individual users, a 45-minute online course is a key tool. It serves as a means to map individual risk behaviour in cyberspace. It includes questions like: "What do you do when you find a flash drive in the parking lot? Do you login into open Wi-Fi networks? How do you protect yourself from shoulder surfing?" So, it is very simplistic and really basic stuff.

To get people genuinely worrying about their cyber hygiene, you need to change their attitudes and mind-sets.

It is targeted towards people who really do not have prior experience with cyber security. Each individual online session provides a personal matrix, showing specific risk areas in different categories in interaction with cyberspace, such as: (a) personal attitude (b) knowledge about security and technology (c) exposure to social media and the internet, and also (d) corporate culture. It captures each dimension, from the individual to the corporate level. The most important feature of this game-like course is the fact that the test is not built on the classic 'pass or fail' principle, but comprehensively captures various risk areas, because you could get 80% out of 100% and feel secure, but that fails to address the 20% where the risk lies.

Summing up, the Estonian approach to cyber hygiene is that you will go nowhere if you keep on repeating the same dry warnings and instructions. If we want the people to start genuinely worry about their cyber

hygiene and, in addition to that, raise cyber awareness, you need to change their attitudes and mind-sets. Finally, I would repeat that the heart of technology is the human factor, and I think that will remain true until 2040—or even beyond.

NATO's Digital Endeavour—Facing the Future Cyber Threats

Captain Philippe Charton (French Navy)

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

I would like to say a few words on what NATO is doing in terms of our digital transformation and preparations for the future. The future has to be built today, because NATO's process for defining and developing capabilities is very long. In fact, Allied Command Transformation (ACT) in Norfolk is at the origin of every new development and innovation.

According to Wikipedia, digital transformation is "a novel use of digital technology to solve traditional problems." NATO has been facing traditional problems for 70 years, and we are used to facing them. What do we want to achieve with the digital transformation? Our NATO Communications and Information Agency (NCIA) has the role of delivering critical technology to enable the 29, and soon 30, NATO nations to communicate with each other.

This role is deeply rooted in the Washington Treaty with a focus on both Article 4 of the treaty, which is the consultation process, and Article 5. In support of Article 4, we provide communication information systems so that nations can collaborate and discuss together. Under Article 5, which is the agreement for collective defense, we support operations and exercises. For example, we are currently involved in seven NATO military operations where we are providing communication and information systems to allow the soldiers, sailors and airmen to do their job. That is the basis of our work in the NCIA.

We want the NATO workforce to be highly effective and to be able to use mobile capabilities.

We are the NATO technology hub. This means that we want our workforce, the NATO workforce, to be highly effective and to be able to use mobile capabilities. This could seem very basic and simple, but it is not at all obvious in an Alliance how to provide simple IT assets, laptops, tablets and cell phones in a way that is secure. And they need to be secure. We also need secure workstations in the offices. So, assuring the security of these networks and assets is our core endeavor.

We are facing adverse cyber threats that other large organizations are also facing. Activism is usually not our major concern, but certainly espionage and advanced persistent threats (APTs) are much more of a concern for all NATO networks. NATO networks are quite numerous because, as you know, we have many different classification levels: NATO unclassified, NATO restricted, NATO secret, mission secret. In short, secret everywhere, which are spread over many different countries and NATO places, and must be protected. That is quite a difficult task.

We need to have a clear and effective NATO digital journey. That is why we are currently developing projects to modernize NATO forces. For example, we will inaugurate this year the new NATO academy in Oeiras, Portugal. Recently, we also moved into our new offices in The Hague. We are renewing the new satellite ground stations and we have a very important program called Polaris to improve and upgrade our

infrastructure on a cloud-based model. We also want to reduce the number of server rooms centralizing them in three data centers that are redundant in order to increase resilience and reduce the cyber-attack surface and have safer NATO networks.

Innovation is one of our key NATO objectives as mentioned very recently by Deputy Secretary General Rose Gottemoeller. In the key five objectives for NATO to move forward, she mentioned first unity, two, burden sharing and three, innovation; so, innovation is at the heart of our actions. The other two objectives deal with difference of norms and new opportunities to the Alliance collective security. That is an important feature, and with innovation, we still need to absorb the new impact of artificial intelligence, big data, and cloud computing.

Our progress depends on NATO technologies developed by the NATO nations and their industries.

Here, there is no secret: the basis of our action and progress is the fact that we are closely related to NATO industries. We have a very effective NATO industry/cyber partnership and the new technology is not developed by NATO but developed by the NATO nations and NATO industries. We have many industry partnership agreements that are really effective. In the cyber domain, the information exchange via these industry partnerships is an important resource that we are taking advantage of.

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

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

I am honored to be here and would like to present a slightly different angle concerning our digital future. In Japan, a new society is arriving and 2030 is its target year. It is called "Society 5.0 and the digital twins." The European Commission calls it the "5th Framework Program, DG XIII," which was started in 1999 in Europe. In Japan, it is "Society 5.0" and in the US, it is "Digital Twins" but all describe the same new digital society.

The definition is a human-centered society that balances economic advancement with the resolution of social problems using systems that highly integrate cyberspace and physical space. The military talks about kinetic and non-kinetic, but it is a little bit different with Society 5.0. This Digital Twins definition is more about society and social environmental transition. It integrates the Internet of Things (IoT), artificial intelligence (AI) machine learning (ML) and softer analytics with spatial network graphs to create living digital simulation models that update and change as their physical counterparts change.

With Society 5.0 and digital twins, new bodies created through innovation will eliminate regional age, gender and language gaps.

In Society 5.0 and the digital twins, new bodies created through innovation will eliminate regional age, gender and language gaps and enable the provision of products and services finely tailored to diverse individual needs and latent needs. In this way, it will be possible to achieve a society that can both promote economic development and find solutions to social problems. The beauty of this case, which is the destiny of our new society, is that humanity can, via cyberspace, go to the past, present and future. It can feed back to enhance and extend society and our lives and the convergence to a new humanity.

I mentioned that it is a little bit different from kinetics and non-kinetics. It is not a complete separation, it is synchronized cyberspace, and although the concept is man-made, digital cyberspace is just conditional, like gaming, and only side by side or just on the outside. It does not feed back to the real world, although we can introduce damage to the real world from cyber if we do not connect properly.

The new risks and the key issues are that physical evidence or object incidents and cyber digital must be twins, which have integrity, data digitization liability and service availability with trust and the synchronization of feedback with mission assurance.

And AI, artificial intelligence, will assist humanity to make decisions. There is a risk of being hacked or manipulated and current major AI services are already hacked. Lots of engineers have said that AI will "eat" the data, statistical data and evidence. And the data must also be healthy, like food. AI should not eat junk data.

And the complexity of mission assurance that can be supported by advanced computer technologies and resilience is very important, more than just security.

Next, what is the image of a human-centered society, in contrast to Society 5.0? Digital twins achieve advanced convergence between cyber space and the physical space, enabling AI based on big data and robots to perform or support other agents that free humans from everyday cumbersome work and tasks that they are not particularly good at. And through the creation of new value, it enables the provision of only those products and services that are needed by the people and thereby achieve optimization of the entire social and organizational system.

AI based on big data and robots can free humans from everyday cumbersome work and tasks that they are not particularly good at.

Also, the system is for the people, and this is a society centered on each and every person and not a future controlled and monitored by AI and robotics.

We have lots of good cases and movements of recent convergence. Why did the European Commission start over 20 years ago DG XIII? In England, two years ago, they started this activity again because DG XIII was slowed down. It was because computer technology was not good enough 20 years ago. But now that computers have enough power to do this, DG XIII is now being reborn or restarted.

In Europe, you also have epSOS, which provides smart open health services for European patients. This is a medical system and the cross-border sharing of certain health data. Japan started Society 5.0 and the US started digital twins. A concept demonstration of digital twins will come during the Olympics in the near future, hopefully by 2020, but we are not sure we can finish it. It will just be a concept demonstration. But by 2022 and 2024, you will see something from the Olympics. Olympic people are going to Society 5.0 and digital twins, and you can see lots of YouTube or TV information about the digital twins by Olympic people.

Finally, the US is working on community resilience**.** In an age of accelerating technologies a virtual electric hospital service with AI is already implemented, as in Kosovo and Georgia and some countries (10 countries, including the US in Arizona and New York City); have already implemented it for medical services.

Basically, we are now back to a simple humanity so our life should be simpler.

Artificial Intelligence and the Cyber Threat: The Role of New Technologies and Artificial Intelligence

Mr. Maurice Cashman

Principal Engineer, McAfee

AI in cybersecurity is both a very interesting topic and an extremely important one. I will give you a couple of perspectives on this: One is just from a context perspective. Having been in the industry for some time, I think that we are in a third generation of cybersecurity architecture, defence of architecture, and capability. I call it the analytics-driven layer. Most of the customers that I work with today understand the need for threat intelligence, they understand the need for defence in depth. They are struggling with a lot of the challenges that some of the larger enterprises may have addressed over the years.

Some of the leading-edge customers that I work with are thinking about how analytics can help them in their cybersecurity capability. I am going to use the term "advanced analytics" as an overall term here but, within that, there are a number of layers from basic statistics to machine learning to the top of this pyramid of complexity which is AI. So, be careful of the terminology.

In some of the major attacks that have taken place, the average time of effect is about four minutes.

We are definitely leaning towards that third level of capability where the majority of our conversations are pivoting towards how to use analytics at various levels, versus just threat intelligence. That is the evolution that we have seen. I believe that a fourth layer, more human centric and more driven, is coming, but it will be for next year's conference.

A couple of things have driven the evolution and the speed at which the evolution is happening: One is the speed of impact. In some of the major attacks that have taken place, there is an average time of effect, which is about four minutes. And today's attacks are not just one or the other, they are not just ransomware, they are not just targeting certain systems, certain vulnerabilities; they are thinking on their own and they can move and adjust based on what the targets are doing. Those kinds of attacks—I would not even call them sophisticated—are a lot more prevalent. Their speed of impact is really quick, so there is not a lot of human interaction that can happen. The systems themselves have to be quite adaptable.

Cloud computing platforms can be stood up and stood down very quickly—in the millisecond range.

Another element that has driven this evolution towards analytics in our architecture is operational complexity. A good example could be that of a billing cycle within Amazon, which is about 100 milliseconds, so the operating speed in Cloud, the proliferation of Cloud computing platforms and the fact that those platforms are stood up and stood down very quickly—in the millisecond range—mean that you cannot have a lot of humans in that loop and you have to think about a more analytics-driven capability.

Finally, as a kind of generic example, everyone knows that there is a shortage of people. According to the Frost & Sullivan survey that I am using here, there is a shortage of about a million and a half cybersecurity experts. Are we ever going to fill that? I do not think so. So, we have to look at ways to better use our people and also figure out other ways to train and recruit within our business.

Those are the key macro trends that have driven this evolution. Now, when it specifically comes to AI, Gartner says that by 2020, 85% of every customer interaction will be driven without a human, only driven by AI. Think about that in the retail space, digital marketing: these are where things are starting, but they are also in other areas. According to Forbes, $30 billion are being spent on AI and we have heard similar numbers today from the other panelists concerning the investments that are being made. Another statistic indicates that there is a lot of venture capital investment with over 3,400 AI companies, mainly in the US, China and Israel. There are also other hotbeds and other reasons why countries that you might think should be on the list are not there. So, a real explosion is happening.

The pyramid of complexity includes machine learning—training your algorithms to recognize patterns. AI is at the top of the pyramid.

From a CSO perspective, I operate mostly at the level of engagement with our customers, and one of the key things is to understand the terminology. There is a market fear, uncertainty and doubt (FUD) that comes out. According to The UK National Cyber Centre, out of all the cyber companies that claim to use AI, over half did not actually have any AI inside their technology. Nonetheless, it is being used to solve every issue.

There are really three levels there. We call it the pyramid of complexity—that is an industry term and we use it within McAfee—machine learning, which is training your algorithms to recognize patterns; deep learning, which is kind of a system of nodes working together, again, to do learning and pattern recognition. It is more complicated and faster. And then, we consider AI to be at the top of that pyramid, where you have reason and decision making, mimicking human decision making and learning capability.

The first two levels are quite prevalent in all kinds of layers, whether it is in an end user device protection or network, or in your behavioral analytics. Those techniques have been around for a number of years. They are embedded in almost every sort of technology that might be in your architecture. Some other AI ones are also in use, like natural language processing, which is recognizing patterns in unstructured data. It is very effective in dealing with phishing and spam and it is getting more sophisticated because phishing is actually quite sophisticated. It is not the user's fault when he clicks on a link because it is fairly easy to get someone to do that. But the systems have to catch up. Another one is in computer vision: you see it a lot in photo recognition in social media and other technologies. From a cyber perspective, detection using computer vision AI capability is happening now. It is a practical application for AI in cyber.

Chief Security Officers need to ask "How are you defending against adversarial machine learning?"

If you are in an enterprise, what are the things that you need to consider if you are a security leader inside your business? One area that I feel will have an impact is in acquisition strategy. Today, if you wonder "How do I measure the effectiveness of a piece of technology or system that I am buying or want to build?" you will have to test it. So, the questions may change. I ask vendors or I ask other providers, "How effective are you against said attack," or, "How effective are you against said framework?" We were having that conversation last night about MITRE Att&ck framework as a way to measure your whole architecture effectiveness.

AI is also going to add another level of complexity in the acquisition discussion or in understanding what adversaries are doing to affect training models and training datasets that companies like us are using. There is a dearth of the training data that is needed for many AI systems. It is weird that in the data explosion we have, there is a lack of good training data but that is a risk and adversaries can poison those things.

I think CSOs have to think about how to ask the right questions of their providers, not just, "Are you really using AI?" but, "What about an adversarial machine learning and how are you defending against that?" How are you securing your own algorithms?" In acquisition discussions, again, the CSO must ask the right questions of his security technology providers, "How are you using Analytics in your technology? What type of machine learning? Is it in development, is it in training, is it in classification patterns? Is it to improve prevention, detection, investigation or response? So, there are lots of different areas within acquisition that, as a buyer of the technology, I need to be better informed.

Thinking about it from a resilience standpoint, I have been a believer in that philosophy or that strategy for some time. If I am in an enterprise and AI is now my intellectual property, I have to think about that as one of my crown jewels and figure out how am I going to defend it.

According to Gartner again, by 2020, 60% of digital commerce companies will use AI, so it is a huge business driver and it is driving 30% of the revenue growth and profitability. It is just like Cloud was a few years ago and it is where the business is going to move to. Therefore, as a leader or designer of security solutions, you have to think about, "How am I going to defend that?" Just know that it is coming and don't avoid it or do not be slow in defending it like we did sometimes with Cloud.

I think that a new training and recruitment problem might be arising. So, today, if we are looking for example for analysts or trained engineers, they could be quite scarce but think about the requirements for developing AI inside your business that might require data scientists and other types of skill sets. Maybe this is worth another look at your recruitment capability. Also, think about not just training your people but think also of the data training that is required to build the AI within your own corporation. So, you have to defend it but you also have to think, "How am I going to get the right data and train that data to make my systems more effective?" I think those are key things within the resilience discussion.

From an architecture point of view, one of the things that we advise is thinking about analytics as part of your layered strategy, therefore as defensive capabilities at various layers. But, more importantly, today is in the detection and the investigation fields. There is new technology on the market that helps analysts make better decisions as they go through an investigative process and that is purely driven by AI capability. The biggest application of AI, right now, is in the detect and investigate phase, and in helping reduce mean time to respond, which is a key metric, but also address the people problem and helping to make our analysts smarter as they go through such systems.

If cameras are going to be everywhere, with the ability to do facial recognition, will there be a duty to have a responsible ethics policy?

Looking at it from threat intelligence, adversaries obviously use advanced analytics against our data, against our systems and they are also using it to test and understand where they should be attacking. New kinds of intelligence might not just be on the actor groups that we are used to today but also on loose affiliations of actors coming together and on what kind of AI techniques these different actor groups are using? That is going to be a new layer, perhaps within the STIX framework.

Looking at the ethics and liabilities in the governance area. If you are an AI company or a company that is dependent on AI, what sort of responsibility does the CSO have? Application security was always very important, privacy by design is one of the later topics and now, ethics by design, which is a great term. For ethics and liability, what is going to be the responsibility of the CSO or the security leader?

And finally, back to the computer vision piece of privacy versus surveillance. If cameras are everywhere, if there is the ability to do facial recognition, is there going to be a duty for our security architects and CSOs to have a responsible ethics policy within that construct?

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

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

Last year, I spoke about the need to develop new military concepts to address cyber warfare and for the international community to come together to develop norms of behavior and international cooperation mechanisms. These would include confidence-building measures such as an international cyber watch & warning center, and the international cyber capacity-building center. I referenced the Tallinn Manual 2.0 and introduced what I called the "grey zone" of this new type of warfare. I stressed the urgency of addressing these threats. These past two days, we have heard from experts about new forms of hybrid warfare and cyber conflict, about what the future landscape of hybrid warfare and cyber conflict may look like.

This year, I would like to discuss non-kinetic threats: Non-kinetic means mainly cyber electronic warfare (cyber EW) and information operation or information warfare, asymmetric or hybrid warfare using cyberspace and the challenges that this type of warfare places on militaries and governments alike. Today, asymmetrical hybrid warfare not only poses dynamic new military threats, but, as we are beginning to see in new military plans and hear at conferences such as this one, today's threats require more holistic or comprehensive approaches to defeat them or to mitigate their effects.

Much of this warfare today is conducted in the grey zone, that is, *warfare in a non-kinetic environment.* The grey zone is a different situation and is all the more challenging for militaries to address. Other forms of emerging warfare such as asymmetric warfare, hybrid warfare, and unrestricted warfare—a type mainly used by China—human-centric and data-centric capabilities, and a variety of other terms describe these new types of warfare.

We are almost always at war within the grey zone…in a state of competition that has not escalated to the conflict or war levels.

My remarks will primarily investigate the grey zone and highlight the fact that military and national defense strategies require new approaches and solutions. We are almost always at war within the grey zone, in other words, we are always in a state of competition that has not escalated to the conflict or war levels. The grey zone has no defined beginning and, perhaps more significantly, no clear ending. Today, grey zone warfare has moved to electronic, data-centric and network-based threats that are integrated within traditional means of kinetic warfare.

Battles within the grey zone include traditional types of cyber warfare, nation-state attacks, data exploitation and surveillance and non-traditional tools for warfare such as the media and social networks. Historically, the grey zone is not a new concept. It has existed for centuries. Networks and worldwide instantaneous communications have made it easier. We are trying to catch up with that threat while distant adversaries,

mostly non-democratic countries, have operated with near impunity within the grey zone for years. For them, crossing between military, civilian and commercial targets is considered normal and appropriate.

These non-kinetic attacks with cyber operations as the primary capabilities or enablers have only increased in intensity and expanded their opportunities. Both an unknown time component and, often, national, political, economic and military objectives that are different from traditional types of warfare mean that grey zone warfare likely leads to truly long wars.

In a sense, a new sort of cold war has re-established itself in this new battlefield where non-kinetic warfare dominates while kinetic warfare is to be used as the last resort. This has caused a shift in the balance of power for entities operating within the grey zone in which raw military power is not the sole factor in determining the winners and the losers. This new paradigm creates great challenges for traditional and national defenses to defend against these "always on" threats. Today's alliances were created to deal with traditional warfare. Current national and international strategies to address these threats are mostly undefined, inconsistent or non-existent. These new strategies will require new partnerships and approaches. Internally, military departments will need to work more closely with other ministries to develop plans and strategies. Externally, it will require both new international partnerships and updates within existing alliances and agreements.

Today's alliances were created to deal with traditional warfare. The new strategies require new partnerships.

Warfare technology is moving to address this new paradigm, but success will not be won by better AI or smarter weapons alone. It will require the integration of national resources that span the spectrum of potential targets to defeat foreign objectives. The planning and the execution of these strategies will require additional skill sets and authorities that reside outside most military institutions, such as economics, diplomacy, or politics.

The grey zone has the potential to become black or white—breaching thresholds for kinetic response.

It is not all bad news, though. The Cold War largely remained cold and there is hope that warfare within the grey zone will have a similar outcome. However, complacency and hope are not what modern warfare strategies and planning are based upon. Whereas the Cold War had the potential to become hot, the grey zone has the potential to become black and white, that is, international standards or norms can be achieved or thresholds for kinetic response may be breached.

We need to plan and organize in order to agree on appropriate international norms or standards before suffering the outcomes of non-kinetic matters and before escalating to kinetic warfare. I have not mentioned AI in detail, though. Artificial intelligence must be a key technology, for both kinetic and non-kinetic measures. As an example of the non-kinetic, AI and new algorithms are being developed to try to identify influence operations and fake news.

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

Mr. Donald Proctor
Former Senior Vice President, Cisco Systems

I was delighted to hear Wolfram von Heynitz from the German Federal Foreign Office talk yesterday about "ethics by design." My fellow panelist Mo Cashman from McAfee and I have been exchanging similar ideas about this in the context of artificial intelligence, and I believe that it is becoming part and parcel of the cybersecurity discussion. Therefore, I would like to dig a bit deeper on the ethics of AI.

You may have read that Google recently announced, with great fanfare, that they had formed an external ethics board for artificial intelligence. Then last week they decided to blow it up, so there is no more board. Amazon has also been in the news because of the prospect that their shareholders may decide to vote on how Amazon can use its AI technology.

So there has been a lot of activity in AI recently. Almost every large country has announced a major initiative in artificial intelligence. At this workshop, we've heard that this is not just for economic advantage, also for national security reasons.

Last year, I talked about what I called the moral compass of software: How do we in the technology sector and in the public sector make sure that we are not only building the right things, but that we are using them correctly?

The example that I gave on AI last year had to do with autonomous systems. We talked about a version of the classic Trolley Problem—there is a trolley going down a track, and it is out of control. An observer has to decide whether to divert the trolley to the left or the right, both of which have people in the path.

Software needs a moral compass: How should it make choices in situations when all the outcomes are bad?

There is no good solution to the Trolley Problem, because all of the outcomes are bad. However, the Trolley Problem permitted us to talk about how industry needs to think about structuring a framework to answer similar questions. Certainly, we cannot have every provider of artificial intelligence coming up with their own version of how to solve this problem.

Interestingly enough, Mercedes Benz ran afoul of this idea a couple of years ago when they gave their answer to the Trolley Problem. They said in the face of an inevitable collision, they were going to protect the passenger first. Well, that did not go over well. It clearly was not always the right ethical choice, so they retreated on that position. Since then, Germany has come up with its own guidelines on the ethics of AI.

And in the military space, the UN First Committee has been working for several years now on exactly what an autonomous system, such as a weaponized drone, can do and how autonomous it can be when making life-and-death decisions. So there are certainly both civilian and military implications.

Facial recognition is another important AI application, and it is getting very good. My new iPad recognizes me, sometimes even without me intending it to do so. It works when the lighting is low, and from many

different angles. The technology has gotten to the point where it does not matter if you age, if you gain or lose weight, or whether or not you are wearing glasses. It can even tell you apart from your twin. Facial recognition is becoming more and more part of the fabric of our lives, but there are some unintended consequences that we need to be mindful of.

Has anybody heard of Sony's friendly-looking robotic dog called Aibo? It is illegal to sell Aibo in the state of Illinois in the United States because it uses facial recognition to identify its owner, and such a use of facial recognition is illegal in the state of Illinois. This shows that technology is running ahead of the law, but here is a case in which the law had an interesting unintended consequence.

Second-order effects of facial recognition are identity hijacking, pre-crime identification, and workforce displacement.

As other examples of unintended consequences, I would like to mention three second-order effects of facial recognition technology: identity hijacking, pre-crime identification, and workforce displacement.

Identity hijacking is just a sophisticated form of identity theft. If you think it might be inconvenient to have your credit card stolen, wait until somebody steals your face. Your face provides access to your personal information, your banking and, in some cases, even your physical assets. There is already an emerging market for your face, you will be happy to know—or maybe not. This market exists primarily for purposes of biometric spoofing. If I can pretend to be you, then I can get ahold of your stuff. Your face is much easier to steal than your fingerprint, and using a hacking technique called a "replay attack," I could use your face for a number of nefarious purposes.

Janis Sarts from NATO StratCom mentioned "deep fakes," which are becoming more and more sophisticated. The definition of deep fakes that I like is, "Manipulating images of real people to make it appear that they're saying or doing things they have never said or done."

One of the ways in which AI technology like deep fakes is getting more sophisticated is through the use of generative adversarial networks or GANs, which work by pitting two deep neural networks against each other.

Another concern is the use of AI for "pre-crime" identification. What if you could predict a crime before somebody commits it? It is an idea from the science fiction story "The Minority Report" by Philip K. Dick written in the 1950s (perhaps you've seen the Tom Cruise movie): If you can get enough information about somebody concerning a crime that they might be likely to commit, you can intervene before they actually do it. Of course, this would be a slippery slope. But it's not far from China's current experiment using facial recognition for "social scoring" in the Xinjiang province.

The Xinjiang experiment shows that triangulation can be a powerful tool. Our world is full of metadata, and triangulating your face, your overall appearance, your gait, and your expression with other digital footprints like banking transactions or retail purchases is becoming easier and easier. But the inferences are not always valid, since the information may lead to false conclusions. For example, racial bias is a problem in many of the facial recognition systems in use today. The Markkula Center for Applied Ethics at Santa Clara University in the Silicon Valley has expressed concern about algorithmic bias as one of the major issues for AI. (In case you do not recognize Mike Markkula's name, he was the third co-founder of Apple.)

And then there is the issue of workforce displacement. The Brookings Institution says that one in four jobs will be displaced by AI. Facial recognition will displace the jobs of security guards, retail workers, hospitality staff, and many others.\ just shift the business someplace else.

But there is a real ethical dilemma here. Even if AI ends up creating new jobs for millions of people, it is not necessarily going to create a job for that delivery truck driver. This is something that we have to take seriously. At the same time, we have a serious skills gap in AI. As General Leinhos from the German Cyber Service mentioned, the military and the private sector are competing for these scarce skills, which we are all going to need going forward.

What are the things that we can do? First, we need to continue investing in technology. Biometric deception and deep fake technologies are advancing much more quickly than our ability to detect them. This means that we need to keep investing in technologies like defacializing, so that we can identify when images are altered or being used in the wrong way.

Second, we must ensure that there is a market for investments in these forensic tools. To be economically viable, there must be customer demand for such technologies. And we have to manage the classic COTS vs GOTS problem (commercial-off-the-shelf versus government-off-the shelf). If you are building aircraft carriers, you may only need to build one; but if you are building a commercial product, you need to build thousands of them for the product to be viable.

Finally, we need industry accountability. We have to establish ethical guidelines, a moral compass. We need to have algorithmic transparency and be mindful of the principle of "ethics by design." This is one of the few areas in which industry is actually asking for a level of government regulation. In fact, there are two places where I see great opportunities for government and industry to partner. One is reskilling of the workforce, and the other is establishing norms of behavior—like obtaining prior consent before a person's image is captured or retained, mandating signage when surveillance is being used, and restricting the use of unaided facial recognition that may result in harm to a human.

These are just a few ideas on how we might go forward in this brave new world of advanced artificial intelligence.

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

I am hoping that this last full panel of the workshop is going to be up to the same standard as the previous ones, if not even better. We will do our level best to go out on a note of *feu d'artifice,* of fireworks. I am also mindful that we are being looked down upon by Louis XIV. It was famously said of the Bourbons in France that they learned nothing, although maybe that applies more to Louis XVI, whose head was chopped off, rather than to the *Roi Soleil* himself. But certainly on this panel, we are going to endeavour to learn something, unlike the Bourbons. And we are going to be looking at crisis management and how you respond to cyber crises.

I feared that after I retired from NATO, that would be the last of my invitations to this workshop, particularly as the advice that I was given when I retired was to do nice things with nice people in nice places. So under that definition, this was the last activity that I wanted to be excluded from. Roger, thank you very much for inviting me back. But I also note that you have downgraded me to be a chairman, rather than a speaker! Ths is to keep me out of trouble. And indeed, it gives me the supreme test of pronouncing everybody's name correctly, because that really is the only task of the chairperson for a panel.

Nonetheless, here are just a few quick words of introduction. What I hope we can do in this session is delve deep and down into the practical aspects of crisis management, because obviously if there is something about crises in the cyber domain, unlike the nuclear domain, it is that they happen every day of the week. This is a bit of a paradox, because if they happen every day of the week, it means that we are constantly being tested and challenged in terms of our intelligence, situational awareness, our ability to respond, our ability to attribute, our ability to recover. But the good news is because this is happening every day of the week, we also are acquiring experience, know-how, and knowledge. So we should be upping our game so that, as the Beatles would put it, "it's getting better all the time." Is that the case or are there crises ahead of us, and are we continuing all the time to make the same mistakes?

Crisis management means that you learn the lessons so that you are going to do better next time.

The first principle is to keep your options open for as long as possible.

Because as all of you know, there are two types of crises – the ones that you are prepared for, and the ones that you are not prepared for. And the definition of crisis management is not only that you do survive the crisis with the minimum amount of damage, but you learn the lessons so that the same thing is not going to happen to you twice, or you are going to do better next time.

So to my mind, as somebody who in his NATO career had to deal with a lot of crises, admittedly not so many cyber ones, but certainly ones involving dropping bombs on other countries, what were the principal things

that were, in my mind at the time, and perhaps would also sort of come across as the key lessons in handling a cyber crisis? Well, the first principle, of course, is to keep your options open for as long as possible. If you are sort of bleeding options with every passing moment, then you are losing your ability to manage a crisis. If you can keep a large number of options in play as long as possible, you are managing the crisis well.

The second principle is avoiding unwanted escalation, in other words, the crisis should not drive you into doing things that you really do not want to do, which could end up making the crisis much worse than it is initially. So avoid escalation. Of course, crises should also demonstrate your strengths, rather than your weaknesses. That is important. And I learned myself that if your management of the crisis actually becomes the crisis—think Brexit, because you simply cannot manage it—then obviously you are in a doubly difficult situation where you have a double crisis—the crisis and your handling of the crisis.

The second principle is avoiding unwanted escalation which could end up making the crisis much worse than it was initially.

And then finally, as I said, being able to learn by doing and being able to improve and draw the lessons. If we have had a crisis, we tend once it is over to heave a sigh of relief and say, "Thank God that's over. Goodbye to all of that. I want to go on holiday." then, we do not really analyze the lessons, the experience. As T.S. Eliot said, "We had the experience, but we missed the meaning." And therefore, we do not put those improvements in place, which are necessary to deal with the next crisis.

So, we are going to talk cyber. But I hope that, in this panel, we are also going to talk crisis management and see how learning and applying the key principles of crisis management, for instance through regular simulations and exercises, can not only improve our ability to deal with cyber security, but also help us to manage crises such as hybrid warfare type crises that we were talking about this morning in a more general sense.

Responding to Cyber Crises: How to Deal with the Challenges

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

When I was asked to be on this panel and after looking at who was going to be in attendance at the conference, I thought I should probably start by setting up some perspective on where I come from. At MITRE, I actually do not do any of the work that we do for the Department of Defense or the intelligence community. I actually support the work that we do related to the US Department of Commerce. And in that role, I work a lot with the private sector. I work with healthcare, the financial services and even industries like hospitality—hotels and restaurants. So, the perspective that I will give will be more related to the way we would interact with those organizations. But when we talk about cyber and cyber crises, we are not talking about whole of government or even whole of nation. We are really talking about whole of world, since there is a need for everybody to come together. For this reason, I do feel like a private sector perspective is a good thing to bring here.

When responding to a cyber crisis, the most important thing is to be ready for it before it happens.

When responding to a cyber crisis, the most important thing is to be ready for it before it happens. If you are responding in real time or after it has already happened, you are pretty well behind the eight ball. So, what does it mean to be prepared for a cyber crisis?

1. You have to have a plan. Your plan should be based on something that is a sort of common lexicon. In the United States, there is a lot of uptake of the cyber security framework for critical infrastructure. It has been translated most likely into several of the languages of those who are in this room and others as well. The reason for using a sort of common framework is that these are risk-based frameworks. They allow you to customise your responses and what you care about, based on your own determination of what your risks are.

When you are dealing with a cyber crisis, the chances that you will be able to resolve it by yourself are pretty small.

2. When you are dealing with a cyber crisis, the chances that you will be able to resolve it by yourself are pretty small. You will have to bring people from other places, maybe outside of your organisation, and having this common lexicon will really go a long way in helping the crisis management process not to become the second crisis that you are dealing with.

These risk-based approaches are important because, in the private sector, you have to get your C-suite on board, just like in the public sector where you have to get your executive leadership on board. These frameworks allow you to bridge the gap between the people who speak the technical language and the people who are dealing with risk every day. Although we like to think that we are special in terms of cyber risk, we

are just another risk. People and executives are dealing with risk every day and they have to be able to communicate. These common frameworks really go a long way to do that.

Being compliant is not having a plan. Compliance and security are not the same things. This was mentioned by previous speakers, and it is another reason why you must be able to talk to that executive level. You have to make everybody understand that checking boxes does not make you secure. The plan that you develop should go beyond that, it should be exercised. You should work through the kinks before doing it in real time.

Part of the exercise should be to define who has decision-making authority. There is nothing worse in any situation, much less in a crisis, than not knowing who can say 'yes' or 'no.' You do not want to be facing that when you are in the middle of a very bad situation. To the best of your ability, you should have those external relationships in place. If you think that you are susceptible to denial of service attacks, but you are not big enough to have the infrastructure in place to deal with them, have those contracts in place and someone on call that you can bring on board if you start to get hit. All of this will lead to the management crisis not becoming an additional crisis. I would like to point out too that, as you do your risk-based approach, you will be able to determine what things you care about most and put high security around them. The other things can be put on a lower tier.

You have to understand the threat landscape as well. It is easy to say, well, this is important and here is a control that I should put on, but you should really understand your adversary. This is where the attack frameworks mentioned earlier can be helpful. For example, there is the MITRE ATT&CK framework (a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations) and the Lockheed Martin cyber kill chain approach (which breaks down each stage of a malware attack in a way that helps you to identify and stop it).

There are things you can do that will not only help you understand your risk but will help you understand what the adversaries are doing. They are not secret. They are done in public and by consensus. You can trust them, and they are open source. So, identify your risks. Take the time to understand what the adversaries are doing that are related to those risks. And have your plan in place and exercise it.

When you look at recent attacks in the U.S. such as the massive ransomware attack of a major US city, the whole city was essentially stopped. For example, hospitals were talking about "having to figure out how to use paper to admit people." So, a fundamental element is to have good backups, to validate the backups and to make sure that the backups are safe, that your critical systems are backed up and that you know how to restore them.

The Importance of Training in Facing Future Challenges: Examples from the CCDCOE Exercises and Training Portfolio

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

We have just had a panel with very smart speakers facing an impossible question: "What will the world be like in 2040?" They did a good job of looking at the question from various angles. Since we are facing a very difficult question as well at our CCDCOE, I was tempted to do the same thing—to tap dance around it. But the discipline that has been instilled in me through military training prevents me from doing that, so I will try to directly tackle the question of "How to respond to cyber crises."

There are multiple areas that we need to work on equally well in order to face the future challenges and crises, but I would like to focus on training. There were mentions of training and human factors many times today, and I will come back to those. Training actually represents two of our three pillars at CCDCOE—since training, exercises, and research are what we do.

Our flagship exercise is *Locked Shields*. Some count this year's exercise as our tenth, but the first two were not called Locked Shields. So, we did not announce the exercise as our big "10." And congratulations to the host nation of this workshop here in Paris: France won the Locked Shields exercise this year. Congratulations as well to the Czech Republic and Sweden for being in the top three. We deliberately do not publicize the remaining places, because this is a training experience. We want to provide the best training opportunities for the nations, and it is their decision on how they use the experience. If they want to send a new and less experienced team, that is their decision. Nobody needs to be embarrassed if they come in last, because training is the place where you should expect to fail, where you should be allowed to fail.

Siemens brought their software and hardware. They set it up as they would actually wire a city's power grid.

Locked Shields is at its core a technical exercise. I am sure that many of you know it very well, but some of you do not. Our technical branch goes through a long, deliberate and detailed process, together with our industrial partners, to set very realistic targets. Here is one example: Our industrial partner, Siemens, brought their software and hardware to the exercise. They set it up in the way they would actually wire and run a city's power grid. It was set up as a target to be attacked and defended in the exercise, and there were several other realistic critical infrastructure targets that the teams also had to defend.

The 23 blue teams, the defending ones, were all elite professionals sent as representatives of their nations. They were fighting from their home stations and they were not in Tallinn, Estonia, with the other players. In order to include the human factor that we spoke about earlier, every team was assigned what we called a "user simulation team." (I played with the letters and called it the "stupid user team.") It introduced into the

simulation such issues as, "What do you do with a thumb drive that you find in a parking lot? How do you handle a suspicious email? When can you click on a link?" These inputs simulated things that normal users do. Even if national elite warriors do not make those mistakes, then somebody in their nation probably does. Giving realistic training is our goal with *Locked Shields.*

We added to the simulation such challenges as "What do you do with a thumb drive that you find?

We also have another exercise called "*Crossed Swords."* We have now run it for the fifth time, but the first time, we had called it an "openly offensive cyber exercise." In the previous years, we could not announce this openly because some of our member nations would not want to be associated with offensive operations. Now, as a result of some political statements early this year a few weeks before the exercise, we found out that it is okay to call it what it is: an "offensive cyber exercise." Another interesting and important improvement this year was the addition of a command layer. This year, it was an Estonian cyber commander in order to simulate a cyber-heavy task force. He had special ops units under his command for kinetics if needed, so he could choose which tasks to do with cyber and which with kinetics. He had actually both of those options in the scenario.

I would also like to discuss our training courses. Our training portfolio is about 20 courses, which we teach with two iterations per year. This means we are presenting 40 courses per year. Half of them are our ten technical courses that develop purely technical skills. However, being the home of the Tallin manual and Tallinn manual 2.0, a strong part of our portfolio is the international law course. We have operational courses, and a course on cyber planning at the operational level, which is not for cyber people. Mistakenly, organizations and nations send cyber experts there, but it is not for them. It is designed so that military campaign planners can understand how cyber works in collaboration with kinetic combat, the normal, conventional means of modern warfare. A cyber threat intelligence course is another new pilot project that we ran.

With our strategic level courses, it gets interesting. Our Critical Information Infrastructure Protection course is always a very popular course which kind of matches the theme of *Locked Shields*. We have been running our highest-level course, the Executive Cyber Seminar, for three years. We have been trying to get higher level people there, and I think we have succeeded because a couple of weeks ago, we had a room full of general officers and their civilian counterparts from defense and other ministries. Finally, in the third year, the message got through that this is the place to learn about cyber, and I now think it is one of the most important courses that we teach. A spin-off of that course was at the EU ministerial meeting, where we offered a half-day condensed version for the military committee with TTX in the end.

In summary, the training of people of all levels is key, and this is what we refer to in Estonia as basic cyber hygiene. I think the term is spreading and I do not even know if it is an Estonian term. But from the ordinary user level to everyone else, we need to have more appropriate levels of knowledge, because the human being is likely to be the weakest link.

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

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

After thinking long and hard about how to discuss ways to deal with cyber crises, I think that the best approach is to give a worked example. Some years ago, I became involved with cyber security issues and crisis management in a battle space, actually in a theatre of operations.

We are now in an environment of digital smog—a combination of volatility, uncertainty, complexity, and ambiguity.

The first challenge was getting people to understand that the dynamic has changed, so we came up with the term 'digital smog.' Just as von Clausewitz talked in 1817 about 'the fog of war', we are now in an environment of digital smog—a combination of mission tempo and the coming together of all these digital assets. And that means that we have greater complexity and greater uncertainty, which is what we used to term VUCA – volatility, uncertainty, complexity, and ambiguity – which came out of the US War College in 1987.

So recognizing that dynamic, we thought that we should replicate what we see in aerospace in terms of "fly-by-wire:" it brings greater levels of automation, which offer greater agility. In other words, you can adapt faster than with a conventional aircraft.

The first step was an agile operating model, so the command flattened its structure considerably. It went from seven to five to ultimately three levels of operations. Another concern was that the technical side and the war fighter side were disconnected, so we went out to them, we used things like design thinking principles and agile delivery principles. And we finally arrived at the concept that "there is one single team."

The other thing that we noticed was that the feedback cycles, especially during operations, were too long, so we had to shorten the feedback cycles considerably. In many cases, the feedback was long only because there were so many manual processes, but they could be automated. Also, the feedback cycles were lengthened by many steps that were just there for historical reasons.

Since the permissions required to counter a threat involved three levels of sign-off, we got that down to one level of sign-off. And we employed a concept that David Marquette used in his book, *Turn This Ship Around*:

> Do not move the information to the authority; move the authority to the information.

During the training exercises, we quite often found that there were high levels of technical debt in legacy systems.

Another thing that we realized was that the decision-making process provides feedback, but you have to orient it to the decision-making process. This meant moving toward an autonomous approach to enable the guys on the ground to react much, much faster. All this was a good start, but then we got into the nitty-gritty. During the training exercises, we began to find weaknesses in our existing systems, and we quite often found that there were high levels of technical debt in those legacy systems.

We started an exercise to remove that technical debt and improve the quality of those legacy systems, including their suppliers—both external suppliers and internal ones. For example, there was a UAV that was

supposed to fly up in the air and provide EW (electronic warfare) for about half a mile, under the assumption that the quality of that UAV was already checked by the relevant ministry that purchased it. Since we did not agree with that assumption, we had our own people look at the quality of that system to see whether it was fit for purpose. We also audited our suppliers to make sure they were using the relevant standards that we had agreed to, and as far as possible, we wanted heavy automation in the supply chain.

An interesting concept was that of "digital twins." Since we did not like the phrase, we called it "model-based systems engineering" which made it easier for people to understand what it was about, but it actually came down to digital twins. We built a digital twin of our battle space environment, and we then applied artificial intelligence to that environment and it ran through multiple attack scenarios. What is interesting, but it is still in its very early days, is to build a digital twin of your opponent in real time while the attack is going forward. This means that you can have people on the ground countering an attack, and in parallel, their wing man is a virtual digital environment using AI, which is suggesting the best counter measures, even suggesting how to get forward to go on the offensive if needed.

We also recognized that this is a *system of systems* world. And if it is a system of systems world, politically, from a command perspective, and from a systems perspective, do we believe in the trust network? And the answer was "no." This means that we operate in a "system of systems" world under the assumption that the trust network is already compromised.

Now that assumption changes the dynamic, because it means that you have to think about other nodes in your network, and whether they are actually acting in your best interest. And if they are not acting in the best interest of the system of systems, how would you know? And what could you do about it?

We also have to deal with the human element, since human beings have this great ability to be irrational. We all have countless biases that we use every day (which fortunately makes the difference between a human and a machine). This meant that we needed to augment the human decision-maker. Since we discovered that there was a strong need for emotional support in particular, we talked to crisis managers involved with Hurricane Katrina. They said that their biggest problem was in making decisions that could lead to loss of life. In such cases, the decision-making cycles increased, because the crisis managers started to get emotionally attached to their decision-making.

In such cases, AI and other techniques give that decision-maker more confidence about their decisions. These techniques can speed up the decision-making, and make it more accurate, while also improving the intelligence and emotional quotient of the decisionmakers and giving them greater confidence.

As my final point, I would say that in the case of this particular command, the most important thing was actually getting the necessary support from the top. That is often the difference between organizations that have tried and failed, and organizations that have been really successful. For this particular organization, the stars aligned, because there was a new uniformed commander who was very open to these ideas. There was also a deputy director who had come from the banking world, and who was used to these ideas. Between the two of them, they opened the doors for us to be successful.

State Responsibility in Dealing with Cyber Threats

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

I will talk at a slightly more strategic level about what regulations look like, what they need to look like, and what we are expecting them to look like. But first, let me mention that I was part of the Estonian team at the *Locked Shields* exercises that Colonel Tarien discussed. We did not get one of the first three places, but it was a very interesting experience since it was my first time. You are put in the middle of a crisis and, for two days, you are working with a team of 40 or 45 people who are managing the crisis with you. The crisis is manufactured, of course, and you know that nobody is actually getting killed, but you have the feeling that you are going through the real thing.

Eventually some teams contained those attacks better than others, some not as well, but everyone got hit. These two days of *Locked Shields* were a sort of reality check for most of these teams: even if you win, like the French team which did win, you are probably still going to be hit by an attack on the water purification system, somebody is going to change the level of chlorine in the water, and the water is going to be tainted. That is the reality even if you are the best of the 23 teams. You have to understand that you will be hit. In any case, congratulations to the French team for winning, and we will see how we can do better next time.

Estonian institutions that deal with data must follow baseline standards on how they lock their doors, computers, and servers.

Other panelists here have talked about how to managing crises. In Estonia, we do a whole lot of these same things and we put them into law because it is a necessity. We tell Estonian institutions that deal with data that they have to follow certain baseline standards on how they lock their doors, lock their computers, lock their servers, etc. We have requirements for critical infrastructure on how to analyse their risks and mitigate those risks. This is not just an Estonia thing since the NIS Directive has done this for the whole of Europe. This is something that everybody has already done.

However, a crisis may come from a very unexpected place. In Estonia, we had a weird crisis about a year or so ago: it was a supply chain crisis. We have an ID card that we use for basically everything. We use it to log into our banks, to log into the system to pay taxes, and to log into our health records. Of course, we use this for voting—this is something that most countries do not do. Fortunately, we found out before an actual crisis that this card was not performing encryption properly. Nobody actually said, "I was able to vote instead of you." Nobody actually said, "I got into your records." It was a firmware error in the chips. We tested one card and saw that it was not just a theoretical threat, there was a real risk.

Unexpectedly, we had a weird supply chain crisis—our national ID cards were not performing encryption properly.

We created new keys for about 700,000 people, and they were able to upgrade their ID cards. All this happened just two months before our elections, however, which raised the question as to whether we could

safely continue with the elections. Finally, the electronic voting or I-voting, as we call it, did go forward. We had technical advisors for the politicians who took the decision to go ahead with the voting, and there was record setting participation in the actual electronic voting at that time. Still, this shows that the next crisis may come from a very different place than what you would expect. At the Estonian Information System Authority, we look at a wide variety of cybersecurity questions, from the ID card to the 5g technology we all will rely on in the future.

I will just throw them out to you for your comments. There are no solutions here, but just a couple of questions.

- As a society, we have decided that we do not usually require people by law to keep the doors to their houses locked. If somebody does break into a house, it may be handled by an insurance company, but people are not required to lock their doors. Should they be?
- As European countries, we have actually decided that we are proactively defending our citizens from unsafe cars on the road and from unsafe food in stores and in restaurants. Therefore, should we have regulations to protect our citizens from unsafe applications on their phones or devices? And if so, how do we approach that? Should there be a certification authority for all of Europe? Or should it be country by country?

Do we need regulations to protect our citizens from unsafe applications on their phones or devices?

While preparing for potential crises or incidents, lawmakers in our parliaments usually raise questions about proposed regulations from the perspective of human rights, freedom of speech, and other sorts of liberties. Perhaps they will ask privacy or security questions as well. In fact, some lawmakers may use the law to block new innovations such as, "We should not have self-driving cars until we get certain things in place, or we should not have 5G operated by a company that we do not trust." They feel that they may save lives in the future with such approaches. This raises another question: Given that we have scholars and experts looking at freedom of speech and liberties, should we have the same sort of discussions on future technologies? We already do that to some degree, but should we do that a little bit more?

Should we have discussions on the possible dangers of future technologies?

Over the past two days, we heard in this forum about the infamous red flag laws of the United Kingdom of 1865, which required a person to walk in front of the autonomously moving locomotive. It does sound weird. You can understand that it may have hindered some innovation. But let's just take a moment to think about what the lawmakers intended. What was their positive intention? Perhaps, they were seriously concerned for the safety of people, and for the horses too and they decided to do something about it. They decided to put this concern into law.

If we now understand that these sorts of restrictions may hinder technological progress, let me just ask, "Should we actually do it again knowing that regulations may impose costs? In the AI panel just before ours, there was a good example concerning the displacement of workers in Palo Alto. A goal was, "We don't want to stop innovation. We just want to slow it down a bit."

These are the kinds of questions that we have to ask as a state regulating authority. We know that these regulations may have a cost. How much taxpayer money are we, as a society, willing to put into building a 5G

network in order to have trust in its provider? How much will the discussion around Chinese technology delay this deployment of working 5G technology in Estonia, or elsewhere in Europe? Is there going to be a difference in African, Asian, or South American countries? Are some regions going to be advancing more rapidly than Europe because they are not having these discussions around the privacy and the question about 5G and Huawei?

This is something that we are discussing with our European partners. We are not doing this alone, fortunately. In a small country like Estonia, we may not even have the expertise to do so. We rely on our partners and allies including the United Kingdom which hosts the Huawei Cyber Security Evaluation Centre where they have the technical expertise regarding these products.

After the European Commission's recommendations to ensure a high level of cyber security for 5g networks, all EU members are now actively engaging in this 5g security question. We are working on our national threat assessments on this 5G question, and, by the end of the year, the European Commission will have minimum requirements worked out in the European Union. This is how we, as a state, as a regulating authority, are working together with our people and our European partners as well.

Concluding Remarks of the 35th International Workshop on Global Security

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

Thank you for your kind words about the Notre Dame disaster. Whether you are Christian or not, part of our history has gone up in smoke and there is a feeling of total sadness and also anger. It is a real tragedy—it is not only our heritage, but it is yours as well. Yet the phoenix always rises from its ashes: It will be a long-term obstacle course, but we will achieve this major goal.

As the Deputy Director of the institute for Higher National Defense Studies within the organization of the Prime Minister, I am pleased that we are meeting together again in the King's Council Chamber of the Hôtel National des Invalides for the 35th International Workshop—at a time when the multiyear renovations of this historic building are nearly complete. This permits us to fully enjoy the beauty of this Council Chamber, the Salle Turenne, and the majestic courtyard in a way that King Louis XIV might have wished for his guests when he built the Invalides for his soldiers and as a Royal Chapel intended for his family and descendants. As we meet here under the watchful eyes of the King, there is perhaps a first lesson to take away from our discussions, which is the unpredictability of the future. This is demonstrated by the fact that the statue standing above the other side of the courtyard is not that of Louis XIV but of Napoleon. And the Royal Chapel contains not the tombs of the royal descendants but that of Napoleon I instead.

Before making a few remarks to close this workshop, I would like to thank all of you for joining us and sharing your wisdom and experience, as well as the Center for Strategic Decision Research, which has been our partner for the sixth time. We also appreciate the contributions of our new partner, the DGRIS (General Directorate for International Relations and Strategy department of the French MoD), as well as the NATO Public Diplomacy Division, and our Technology Partner, Panda Security, together with the cyber security companies whose logos you see before you.

Last year's workshop theme was already a surprise to me because it addressed for the first time the risks of hacking and cyber influence operations not only to our militaries, our economies, or individuals, but also their potential to threaten our democracies by creating divisions within our societies, threatening the credibility of our elections, and even driving a wedge between the nations of our Atlantic Alliance which has kept our countries safe for 70 years.

Since we are meeting in a monument where the spirit of Napoleon is widely present, it may be appropriate to consider a warning which has often been attributed to him and which I have mentioned in the past, "Se faire battre est excusable, se faire surprendre est impardonnable," or, "To be beaten is excusable, to be surprised is unforgivable." So we must not allow the rapid evolution of the hybrid threat to catch us by surprise. Yet, it is

evolving very rapidly indeed. A year ago, some of us were surprised by the success of Russian cyber influence operations in not only creating divisions among our societies but even influencing elections. We also became aware of the unfortunate reluctance of social media companies like Facebook, Google, or Twitter to cooperate fully in blocking or limiting these influences by foreign powers.

Given the harm to our societies caused by such cyber influence operations, it is fortunate that governments are increasingly aware that the danger comes not only from foreign adversaries, but from our own political organizations, private actors, and social media companies. In fact, some of these companies are so large and powerful that a new term has been invented to describe them: quasi-state actors. As one of the first steps, the United Kingdom is expected to announce legislation very soon calling for an independent regulator that will impose a "new statutory duty of care" on media companies and even their executives in order to limit the distribution of harmful content.

In these brief remarks, I will not try to summarize the results of two full days of presentations and discussions, but I would like to draw attention to several points that were made by speakers and which are especially relevant to the workshop's overall theme:

- ***A large-scale kinetic war is no longer the most probable scenario***. Hybridity is playing an increasingly decisive role. In addition to cyber-attacks, other information activities such as fake news campaigns, intended to create 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.[5]

- ***Hybrid attacks are growing and enjoy "near impunity."*** The rule-based international order was upended in Georgia (2008) and again in Crimea (2014) with Russia's highly aggressive use of non-kinetic, asymmetrical, hybrid warfare. These attacks continue "with near impunity" within a "grey zone" that stays below the threshold of what would provoke an armed confrontation. They are increasing in intensity and threaten militaries and governments alike.[6]

- ***Among hybrid threats, psychological effects are the most dangerous***. Hybrid attacks with the potential to cause widespread physical damage can be deterred by NATO's invocation of its collective defence clause. Yet, psychological effects are more damaging because they are less visible, develop over a longer-term, and the attribution of the attacker is likely to be ambiguous.[7]

- ***Disinformation is a weapon.*** At the heart of the psychological threat is "*disinformation*" which is actually a "weapon to influence human behaviour." It is changing how societies perceive and consume news, how they make decisions, and how they respond to foreign interference. We have seen this in recent elections around the globe that have disrupted the international order and continue to do so.[8]

---

[5] Lieutenant General Ludwig Leinhos, Chief of German Cyber and Information Domain Service.
[6] General Tatsuhiro Tanaka, Fujitsu System Integration Laboratories.
[7] Ambassador Jiri Sedivy, Permanent Representative of the Czech Republic to NATO.
[8] Mr. Jānis Sārts, Director, NATO Strategic Communications (StratCom) Center of Excellence

- ***In the Black Sea area, Russia is actively using hybrid tactics***. It is exploiting the specific vulnerabilities of each state in the region to reduce the cooperation and undermine trust. The frozen conflicts in the region fuel organized crime and have significant potential to destabilize the whole region rapidly. Russia also leverages energy security as the Black Sea is a key transit corridor for energy resources.[9]

- ***Digitization, despite great benefits, increases vulnerabilities to cyber and other hybrid threats.*** The "digitization" of governments, militaries, and societies is growing rapidly because of its enormous benefits, but it brings an increased attack surface that increases vulnerability to hacking, cyberattacks, and cyber influence operations.

- ***Artificial Intelligence and other new technologies are now a security issue as well***. As governments adopt new guidelines to regulate the use of AI and other technologies and as industry seeks ways to create ethical guidelines for their development, it is important to understand the unintended consequence of new technologies in our increasingly digital world."[10]

- ***Governments and industry need to be proactive in dealing with the societal effects of new technologies***. The delays of both government and industry in adequately dealing with the advent of 5G technology *(Question: Should Huawei be allowed to play a leading role in 5G?),* as well as the attribution of attacks and the dissemination of false information on social networks, show that their responses need to be more proactive.[11]

Facing all these issues, societal resilience is the best response, rather than deterrence. Societal resilience depends on positive values and characteristics such as mutual trust and solidarity among people, the cohesion of society, and loyalty to the institutions of the state. The way to achieve this in our societies is through good democratic governance, transparency, and accountability of power, a strong and active civil society, as well as well-educated people who can think critically."[12] Individuals must also assume a large portion of this responsibility for defending against hacking, cyber threats, and disinformation. In Estonia, for example, citizen responsibility is actively encouraged as a key element of *cyber hygiene.*[13] With these efforts, we can at least hope that the next generation will be a *cyber resilient* one.[14]

Thank you for joining the 35th International Workshop and for being with us for these final sessions. Since we will be preparing "findings" for our government, NATO, and participating countries for consideration for the next workshop, it would be helpful to know your thoughts on which issues to emphasize. So, will ask as a favor that, if you have suggestions, please help us "rethink our way of thinking" as we prepare for the future.

Editor's note: The above points are based in large part on the preliminary drafts of presentations prepared for the 35th International Workshop. Their contributions are recognized in the footnotes in lieu of specific citations.

---

9 Ms. Simona Cojocaru. General Director for Defense Policy, Romanian Ministry of Defense
10 Mr. Donald Proctor, Former Senior Vice President in the Office of the CEO, Cisco.
11 Mr. Lauri Tankler, Estonian Information Service.
12 Ambassador Jiří Šedivý, Permanent Representative of the Czech Republic to NATO.
13 Ms. Merle Maigre, Executive Vice President CybExer Technologies.
14 Mr. Xavier Carton, Deputy Director of Information Systems, RTE

The *35th International Workshop on Global Security* is presented by the Center for Strategic Decision Research (CSDR), the Institut des hautes études de défense nationale (IHEDN), and the General Directorate for International Relations and Strategy (DGRIS), with the sponsorship of the following governments and organizations:

Center for Strategic Decision Research

IHEDN

DGRIS
Direction générale des relations internationales et de la stratégie
MINISTÈRE DES ARMÉES

NATO
OTAN
PUBLIC DIPLOMACY

UNITED STATES
DEPARTMENT OF DEFENSE
Net Assessment

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE
DE LA DÉFENSE

TECHNOLOGY PARTNER

panda
Panda Security

MAJOR SPONSORS

McAfee
FUJITSU
SINCE 1996
AREA
INTELLIGENCE MINDSET
MITRE
CISQ

ASSOCIATE SPONSORS

NCI
AGENCY
Karakawa
Foundation
Peace
AXA
CYBEXER