Global Security in the Age of Hacking and Information Warfare: *Is Democracy at Stake?*

PROCEEDINGS OF THE 34*th* INTERNATIONAL WORKSHOP ON GLOBAL SECURITY

Mrs. Florence Parly
Minister for the Armed Forces and Workshop Patron

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

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: 1-890664-24-3

34th International Workshop on Global Security

Workshop Proceedings

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

WORKSHOP PATRON
Mrs. Florence Parly
Minister for the Armed Forces

THEME
Global Security in the Age of Hacking and Information Warfare
Is Democracy at Stake?

WORKSHOP CHAIRMAN & FOUNDER
Dr. Roger Weissinger-Baylon
Co-Director, Center for Strategic Decision Research

PRESENTED BY
Center for Strategic Decision Research (CSDR)

AND
Institut des hautes études de défense nationale (IHEDN)
within the French Prime Minister's organization, including
the Castex Chair of Cyber Security

PRINCIPAL SPONSORS
French Ministry of Defense

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

North Atlantic Treaty Organization
Public Diplomacy

Cisco Systems

MAJOR SPONSORS
Fujitsu · McAfee · Area SpA · MITRE · CISQ

ASSOCIATE SPONSORS
NCI Agency · AXA

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

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE
DE LA DÉFENSE

DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA
UNITED STATES
DEPARTMENT OF DEFENSE
Net Assessment

NATO
OTAN
PUBLIC DIPLOMACY

Center for
Strategic
Decision
Research

IHEDN

CISCO™

MAJOR SPONSORS

FUJITSU

McAfee™

SINCE 1996
AREA
INTELLIGENCE MINDSET

MITRE

CISQ

ASSOCIATE SPONSORS

NCI
AGENCY

AXA

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

Patron of the 34th International Workshop

Mrs. Florence Parly
Minister of the Armies

Table of Contents

Welcoming Remarks

Lieutenant General Bernard de Courrèges d'Ustou

Director, Institut des hautes études de défense nationale

Excellencies, Mr. Chairman, Dear Roger, fellow officers, and ladies and gentlemen,

Welcome to this grand salon of the Hôtel National des Invalides, one of our greatest historical monuments in the center of Paris.

As the Director of IHEDN, the Institute for Higher Defense Studies, and also as Director of Advanced Military Education, I am very pleased to welcome this International Workshop on Global Security for the eighth time in Paris, and here for the fourth time, and under the patronage of the Minister of the French Armed Forces, Mrs. Florence Parly.

IHEDN is an inter-ministerial and inter-departmental institute, which conducts 60 seminars or sessions each year and educates 2,200 attendees, who are civilian and military leaders, on defense and security issues at international, national and regional levels. It is particularly dedicated to European and national affairs. IHEDN is also honored to participate in the organization of this workshop in close cooperation with the Center for Strategic Decision Research. We have been accustomed to listening to several invited addresses at the beginning of these workshops and, in a few minutes, we will listen to Ambassador Tacan Ildem, NATO Assistant Secretary General for Public Diplomacy, and General Olivier Bonnet de Paillerets, Cybercommander of the French Ministry of the Armed Forces. But, first, I have the pleasure and honor to present Mounir Mahjoubi, who is the Secretary of State in Charge of Digital Affairs. In 2016, Mr. Mahjoubi was President of the Conseil National du Numérique[1] (the French Digital Council) and at the beginning of the year he joined the team of Mr. Emmanuel Macron in charge of digital issues for the Presidential Campaign. In May, he was named as the Secretary of State in Charge of Digital Affairs.

Mr. Minister, we are very pleased and proud to welcome you. Monsieur le Ministre, je vous cède respectueusement la parole.

[1] The Conseil National du Numérique is an independent advisory commission. The Council issues independent opinions and recommendations on any question relating to the impact of digital technologies on economy and society. The government can consult the Council on new legislation or draft regulations.

Workshop Findings and Recommendations

Dr. Roger Weissinger-Baylon,
Workshop Chairman and Founder

> *"I expect the Russians to meddle in the upcoming European parliament elections in spring 2019…and do all that they can" to intervene in the next 20 NATO and EU elections before 2020.*[2]
>
> - Anders Fogh Rasmussen, former Secretary General of NATO

The *34th International Workshop on Global Security* was held in Paris in December 2017, with the Patronage of the French Minister of the Armed Forces. It was presented in partnership with the French Institute for Higher Defense Studies (IHEDN), within the Prime Minister's organization, as well as the NATO Public Diplomacy Division, the NATO Communications and Information Agency (NCI), the U.S. Department of Defense (Net Assessment) and Cisco. Additional sponsorship[3] was provided by Fujitsu, McAfee, Area SpA, and CISQ. The workshop theme was "*Global Security in the Age of Hacking and Information Warfare: Is Democracy at Stake?"*

The keynote speakers were Minister Mounir Mahjoubi, the Minister of State for the Digital Sector, attached to the French Prime Minister; Ambassador Tacan Ildem, NATO Asst. Secretary General for Public Diplomacy; General Olivier Bonnet de Paillerets, Cybercommander, French Ministry of the Armed Forces; Mr. Anthony Grieco, Chief Trust Strategy Officer, Cisco; the Rt Hon. the Lord Browne of Ladyton, former U.K. Secretary of State for Defence, and The Lord Harris of Haringey. Major General Tatsuhiro Tanaka was the Fujitsu key speaker. Among the NATO speakers were Ambassadors Jiří Šedivý (Czech Republic), Michael Zilmer-Johns (Denmark), Luis de Almeida Sampaio (Portugal), and Mehmet Fatih Ceylan (Turkey); Dr. Jamie Shea, Deputy Asst. Secretary General for Emergency Security Challenges; Mr. Kevin J. Scheid, the General Manager of the NATO NCI Agency; Ms. Merle Maigre, Director of the NATO Cooperative Cyber Defense Center of Excellence in Estonia, and Mr. Jānis Sārts, Director of the Strategic Communications Center of Excellence in Latvia.

Principal findings and key concerns. Although cyber threats are growing rapidly and terrorism is a vital concern of many NATO countries, the most immediate danger is the ruthless and highly effective cyber and information war that Russia is waging against the United States, as well as other NATO countries and partners. Russia's political intervention is a grave danger since it represents a threat to our democracies.

This situation leads to the following rapidly evolving considerations:

- According to the U.S. National Security Advisor, Lieutenant General H.R. McMaster, and joint testimony by the directors of all five U.S. intelligence agencies (FBI, CIA, Director of National Intelligence, Defense Intelligence Agency, and the National Security Agency), Russia intervened in the 2016 elections and is certain to do so again.

[2] https://www.msn.com/en-us/news/world/russia-will-target-european-elections-in-2019-former-nato-boss-says/ar-BBKqVTx

[3] Given the serious harm caused by Russia's ongoing hacking and cyber influence operations, and after consultation with workshop advisors, we did not invite the Russian cyber security company Kaspersky to sponsor the 34th International Workshop. We hope that there will be a way to permit Russian participation again at a future workshop.

- President Trump has been reluctant to punish Russia with sanctions or effectively block Russia from continuing its cyber influence operations and other hostile activities.
- With such strikingly weak resistance from the U.S. President, Russia is currently winning the war and this means that the democracy of the United States is *absolutely* at risk.
- Once U.S. democracy has been weakened, and given that the U.S. military budget represents over 70% of NATO's collective capability, will NATO have the will or resources to protect other members and partners from a similar fate?

Additional findings, recommendations, and questions arising from the workshop presentations and discussions include the following:

1. *According to the French Minister of State for the Digital Sector, Mounir Mahjoubi, "the [cyber] threat has never been as high as it is today," because of the broad-based movement to digital together with an unprecedented diversity and range of interactions among private, state, and ideological cyber actors*.

   The legal structures that are essential to deal with these new threats and the actors behind them are evolving far too slowly. In the past, "...it was much easier to understand how a state could threaten another state in the digital space," but, now, victims of cyberattacks can number in the millions. This means that millions of judicial processes would be needed. Such challenges require a complete re-thinking of the judicial process, and this is complicated by the reality that experts in digital issues are extremely rare and political leaders with the necessary level of relevant experience are even rarer.

   On the positive side, the EU General Data Protection Regulations GDPR) which start in May could help by creating a double revolution: first, it will bring "...a revolution in terms of the diffusion of cybersecurity," and in addition "…people will have more awareness of their own data" and will better understand how to enjoy their benefits and protect themselves.

   Above all, we need to have more thinking on the subject:

   > "...There are not enough think tanks working on this subject worldwide. There are not enough governments… investing on this subject, and there are not enough public servants working on the subject worldwide…This is the year when we need to find a common ground on the subject. "

   Countering Terrorism

2. *Ambassador Tacan Ildem, an opening keynote speaker, recognized that "...the recent wave of terrorist attacks has changed perceptions. In France it is now the first concern of the population."*

   In addition to terrorism, another main threat is cyberattacks—including attempts, presumably by Russia, to "undermine our democratic processes" with disinformation which is "part of the hybrid toolbox. Russia's cyber influence operation:

   > "…targets not just our institutions, but our way of life. They are an attempt to divide our societies from within, and we must respond by continuing to raise awareness."

   Since Russia's illegal annexation of Crimea in 2014 we have significantly enhanced our defence and deterrence. At the same time we are open to periodic and meaningful dialogue with Russia. This is not easy, but it is important because, especially when tensions are high, such dialogue can help us reduce risks and increase transparency.

3. *Terrorism is likely to worsen with "electronic Jihad." According to Lord Harris of Haringey, Daesh uses "cyberspace and social media to radicalize, recruit, fundraise and train" and represents a danger that could be almost as serious as the cyber threat to infrastructure.*

   An example is a single Jihad rap video that was downloaded millions of times, which is the kind of thing that makes even self-radicalization possible (sometimes in as little as four to five weeks). Thanks to the "Dawn of glad tidings," an Arabic language application that allowed ISIS to take control of the social media of their followers before its attack on Mosul, "tens of thousands of messages were posted saying that an invincible ISIS Army supported by God was arriving." Not surprisingly, many of the Iraqi soldiers defending Mosul decided to flee after seeing the messages. According to Lord Harris, it is "only a matter of time before terrorists use cyber as a weapon itself, not just in terms of propaganda or recruitment or training."

4. *In order to counter such terrorist threats, should NATO play a larger role? Portugal's NATO Ambassador Luis de Almeida Sampaio agrees that NATO is already doing a great deal, but he asks, Is it enough? Can NATO do more?*

   NATO has been involved in the fight against terrorism since the invocation of Article 5 after the 9/11 attacks on New York's World Trade Center. More recently, NATO joined the coalition against Daesh. Nonetheless, countries like Portugal, Spain, or possibly France and Italy wonder why the fight against terrorism should be concentrated in the Middle East? Shouldn't terrorism be a 360-degree concern that would also deal with the threat from North Africa and the Maghreb? It is also necessary to consider the tools for dealing with terrorism, which NATO is lacking. And there should be cooperation with the EU, but in a recent agreement with the EU, very few of the 74 measures have anything to do with the fight against terror. In order to preserve the future unity of NATO and encourage its cooperation with other International organizations, these issues need to be discussed at the coming NATO Summit.

5. *Ambassador Fatih Ceylan, Turkey's ambassador to NATO, warns that—despite great success against Daesh in Iraq—the threat is not over, since we must now deal with Daesh version 2.0. We must face the root causes of Daesh, namely "a breeding ground [with] distortion of facts, economic factors, and ethno-sectarian or political grievances". Above all, we must achieve a "genuine political transition in Syria and political recalibration as well as reconciliation in Iraq."*

   In Iraq, the government's priorities must include:

   > "…reforming the political and economic system and rendering it more inclusive and transparent, empowering local communities, devolving more authority to the governorates and starting a genuine campaign of national reconciliation, in tandem with efforts on reconstruction."

   This also means consolidating the ceasefire, revitalizing the Geneva talks, and recognizing that " …collaboration with a terrorist organization to defeat another one, even for tactical reasons, is a grave mistake." In particular, YPG/PYD groups, which are closely related to the PKK, should not be receiving our support. Ultimately, the goal must be the reconstruction of Syria, "…with a governing authority that is seen as legitimate by all elements."

Threats of Cyberwar

6. *The former U.K. Secretary of State for Defense, Lord Browne of Ladyton, warns that the cyber threat has changed the nature of warfare and global security priorities. Critical infrastructure and the command and control of nuclear weapon systems are now at risk of attack by well-resourced state actors including Russia, China, and even North Korea and Iran.*

A 2013 U.S. Defense Science Board study on the resilience of the Department of Defense of systems found that "security practices have not kept up with cyber adversary tactics and capabilities" which means that:

> "…the United States cannot be confident that our critical information technology systems will work under attack from a sophisticated and well-resourced opponent using cyber capabilities in combination with all of their military and intelligence capabilities."

Moreover, a complementary report by the U.S. Defense Science Board in 2017, found that:

> "…major powers—specifically Russia and China—have a significant and growing ability to hold U.S. critical infrastructure at risk via cyber-attacks and an increasing potential to also use cyber to thwart U.S. military responses to any such attacks."

Lord Browne suggests that the solution is "…to develop a clear understanding among the key players not to interfere with the nuclear command and control systems of their adversaries and to work together to protect all nuclear weapon systems from non-state actors."

7. *The new "cyber powers," according to Major General Tatsuhiro Tanaka of Fujitsu System Integration Laboratories, present a new challenge: Just as the potential for conflict among the traditional nuclear powers has led to international agreements for managing them, there is a "need for cyber weapons to operate within an international framework as well." A new international framework would require a "clear understanding of what raises a cyber-attack to the level of an armed attack."*

For example, "…there are many instances where private industry has discovered and actively shut down malicious attacks passing through their networks. What is their responsibility when one nation is conducting a cyberattack against another and where private industry has the capability to stop the attack?"

In order to deal with the issue, General Tanaka has proposed the creation of two internationally-sponsored centers:

- The *Watch and Warning Center,* which would be possibly chartered by the United Nations and funded by many member countries, and
- The *Cyber Capability Center,* which might assist countries that lack the necessary cyber capabilities themselves.

Trust and Resilience

8. *To be effective, a global approach to cyber security must be built on "trust" and "resilience," according to Anthony Grieco, Cisco's Chief Trust Strategy Officer.*

"A fundamental premise... is that the world is going digital." Eighty percent of business leaders want to transform their organizations digitally, which is impossible without cyber resilience. Cyber resilience depends on evidence, because it is the evidence of resilience that permits Trust. In turn, the only way to achieve that resilience, evidence, and trust is through a secure product development life cycle.

As the U.S. State Department's Chris Painter mentioned, the U.S. Vulnerability Equities Process (VEP) provides a way for the government to disclose vulnerabilities that it has learned about so that vendors can fix them. Cisco goes a step further by arguing that "it is critical for all of us to know about [such vulnerabilities] as soon as anyone—government, private or other entities—discover them so they can be fixed." For the private sector, this also means figuring out how to best partner with the public sector.

Russia's New Generation Warfare and Cyber Influence Operations

9. *Dr. Jamie Shea, NATO's Deputy Assistant Secretary General for Emerging Security Challenges, called attention to Russia's "New Generation Warfare" as described in the new U.S. National Security Strategy whose announcement by General H. R. McMaster coincided with the workshop.*

According to Jamie Shea, new generation warfare means that the "home front is now the new center of gravity for strategic competition." In Russia's new generation warfare, fake news, botnets, and aggressive propaganda take advantage of our "cultural hacking," which is characterized by:

…more fragmented and more polarized societies where the mood is anti-establishment, anti-elite; fed by anger, passion, and a voluntary acceptance of misinformation provided that it feeds one's own emotions and prejudice.

In both the U.K. and the U.S., some of our government leaders have gone so far as "to actually describe journalists as enemies of the people." Russia is exploiting this situation with large investments including the RT and Sputnik TV channels. In the face of this tremendous threat, Dr. Shea makes a very strong recommendation concerning Russia, which needs to be taken seriously:

> "…when we give RT or Sputnik a license to operate in NATO countries, we need to demand equal access for Voice of America, Radio free Europe, BBC World Service, or CNN International in their markets."

10. *As Director of NATO's Cooperative Cyber Defense Center of Excellence in Estonia, Merle Maigre reminds us of Russia's cyberattack on her country ten years ago: the "…first time that cyber was used in a*

coordinated manner against another state." A key lesson was the importance of keeping the public informed by maintaining transparency and information-sharing in real time during a cyberattack.

A more recent concern is for "election hacking," which covers "phenomena ranging from email leaks and website defacement to compromising voter rolls or attempts to penetrate campaign finance or voting systems." For liberal democracy to defend itself and survive, a broad and comprehensive approach is necessary:

> "This encompasses strategic communication, democratic education, and securing the technology… improving the cyber hygiene, awareness, capacity building, and the operational security of political actors and candidates…Covering the basic cyber hygiene means changing default passwords and making passwords hard to crack, not using the same password for different systems, making sure that all systems are patched and up-to-date... ensuring that systems are only connected to the internet if necessary and making sure that essential data is backed up securely."

"Every military operation in any foreseeable military mission of NATO will have a cyber component. Therefore, "…we are also struggling with how to convince nations to move cyber assets out of the status of national strategic assets…[which are] difficult to deploy because of their classification and the high-level approval necessary to deploy them.

How can we make a case that cyber assets should be operational assets whose effects can be understood and utilized by operational commanders, as is the case with the air, sea, and land domains?

11. *Russia is an immediate danger because it threatens not only our economies and the safety of our citizens, but it imperils our democracies by attacking our culture and our elections. Should countries that are being attacked by Russia in this way ask for NATO support by invoking Article 5?*

The leaders of all five U.S. intelligence agencies—FBI Director Christopher Wray, CIA Director Mike Pompeo, Director of National Intelligence Dan Coats,[4] Defense Intelligence Agency Director Lt. Gen. Robert Ashley, and NSA Director Adm. Michael Rogers—testified unanimously to the Senate that Russian intervention is certain to continue through the 2018 elections.[5] Unfortunately, President Trump has refused to implement the sanctions[6] against Russia that were imposed by a law that he himself signed in August.

Ambassador Jiří Šedivý, Permanent Representative of the Czech Republic to NATO, cited Russia's implication in an attempted assassination of the Montenegrin Prime Minister, in order to block its entry into NATO. According to a minority staff report[7] of the U.S. Senate's Foreign Affairs Committee, Russia is targeting many of NATO's partners and allies. It intervened in the Catalan referendum; and

[4] According to Director of National Intelligence Dan Coats: "Frankly, the United States is under attack. Under attack by entities that are using cyber to penetrate virtually every major action that takes place in the United States."

[5] Full testimony of U.S. intelligence leaders: https://www.npr.org/2018/02/13/584672450/intelligence-leaders-testify-about-global-threats-in-senate-hearing

[6] https://www.reuters.com/article/us-usa-russia-sanctions/trump-administration-holds-off-on-new-russia-sanctions-despite-law-idUSKBN1FI2V7

[7] "Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security." Minority Staff Report for Committee on Foreign Relations, U.S. Senate: https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf

it has attempted to influence voting in France, Germany, the Netherlands, Italy.

The U.K. Foreign Office's Head of Cyber Policy, Paula Walsh, warned of Russia's efforts to undermine institutions and the rules-based international system.

12. *Without its clever manipulation of Twitter, Facebook, Google and other social media accounts, Russia's intervention would have had far less impact. As Dr. Jamie Shea points out, however, "our [Russian] adversaries have become more and more skillful at exploiting the political domain."*

    It is vital to stop Russia from intervening again. Yet, this will require cooperation from social media companies that made significant profits at the expense of democracy during the 2016 election period. While these companies do seem to be making certain efforts to reduce the risk of another Russian intervention, the companies fear that corrective measure could impact their business models. *Boston Globe* writer Ty Burr says that since the interests of social media companies "…run counter to those of their users…it's probably useful to think of these companies as passive collaborators (at best) until proven otherwise."[8]

13. *According to Dr. Frédérick Douzet, the Castex Chair at IHEDN[9] in Paris, "Russia wants to restore its great power status." Putin's end goal is to shore up internal support by demonstrating that Russia is strong, a great power, and morally superior to the West.*

    Russia seeks to demonstrate the weakness of the U.S., as well as NATO itself, by sowing discord and deepening divisions within and between member countries. In this way, Russia hopes to convince its citizens that western countries are economically and politically corrupt, too—with the same extremes of inequality and injustice, and with unfair or rigged elections, while Russia, unlike the West, has a strong leader in President Putin.

How NATO Can Respond

14. *France, Germany, and a few other countries were able to foresee the threat of Russian cyber influence operations and were able to block or limit the Russian influence. This suggests that Russia's influence can be delayed or minimized whenever countries are willing to push back.*

    According to Denmark's Ambassador to NATO Michael Zilmer-Johns,

    > "Attribution is a powerful political deterrence tool but [it is] rarely used and definitely not used by NATO. Shouldn't it be our first response to any attack in order to publicly expose an adversary? Currently, perpetrators of cyberattacks act with seeming impunity. We must be in a position to act swiftly and take Joint action against nations that conduct attacks under the threshold of an armed attack. If we do nothing, we invite further attacks against ourselves and NATO.

[8] https://www.bostonglobe.com/arts/2018/02/21/their-bots-your-response/Y4lFwBUOhJhTVUchXlXpAN/amp.html

[9] Institut des hautes études de defense nationale (IHEDN)

Surely, NATO can help its members and partners to resist and fight back!

As General Jean-Christophe Cardamone cautioned in his closing remarks, "*To be beaten is excusable; to be surprised is unforgivable."*[10] Since the evidence of Russian cyber influence operations in the U.S. and in Europe is now clear, there is no excuse for not taking action. If Russia is able to successfully impose its will on the U.S. administration in particular, NATO will have lost the benefits of a country providing over 70% of NATO's capabilities. In that case, will our European and other allies sbe able to resist the push of Russia's hybrid warfare in Eastern Europe?

General Tatsuhiro Tanaka warned, "We have a shared responsibility to avoid the tragedy and destruction that uncontrolled cyberattacks could cause to our civilian population and our way of life."

Postscript:

Since these workshop findings and recommendations were drafted, the following significant developments have occurred—involving broad Russian attacks against the U.S. critical infrastructure, Russian nerve-gas poisonings in the U.K., and an inexplicably weak U.S. response:

- *Russia is successfully targeting U.S. critical infrastructure.* According to the U.S. administration, Russian cyberattacks "targeted American and European nuclear power plants and water and electric systems, and [they] could have sabotaged or shut power plants off at will."[11] Russia seems to have left tracks deliberately, as a strong signal that its hackers have the ability to shut down our critical infrastructure if they so wish in case of a conflict.

- *Russia is testing the U.K. government—or trying to send it a message—by poisoning a former British spy, Sergei Skirpal, and his daughter with a military-grade nerve agent.* In addition, Russia likely murdered with impunity over a dozen other Russians living in the U.K., with Nikolai Glushkov being the most recent. Speaking to Parliament, Prime Minister Theresa May called the poisoning a "direct act of the Russian state against our country" (unless it is a dangerous loss of physical control over the nerve agents).[12] Like cyber, political corruption, money laundering and blackmail, murder is part of the Russian tool box.

- *Despite the above threats, the U.S. State Department is responding with unusual passivity to Russian interventions.* According to the *New York Times*, "not one of the 23 analysts working in the department's Global Engagement Center — which has been tasked with countering Moscow's disinformation campaign — speaks Russian," the department has imposed a hiring freeze, and it spent $0 of the $120 million budgeted by the U.S. Congress to respond to Russian interference. [13]

- *During the 2016 Presidential campaign, Facebook allowed a Trump consultant, Cambridge Analytica, to exploit 50 million Facebook accounts without users' knowledge*.**[14]** The impact on the election may have

[10] Attributed to Napoléon Bonaparte.

[11] https://www.nytimes.com/2018/03/15/us/politics/russia-cyberattacks.html

[12] In recent years, Russia has been suspected of murdering over a dozen Russians living in the U.K. including Alexander Litvinenko who was poisoned with polonium-210 in 2006. Most murders were made to look as if they were due to natural causes or suicide.

[13] https://www.nytimes.com/2018/03/04/world/europe/state-department-russia-global-engagement-center.html

[14] http://www.bbc.com/news/world-us-canada-4344479

been significant,[15] and Facebook may have limited ability to prevent similar data misuse in the future. This situation highlights the importance of European Union efforts to regulate data privacy.

- *Under a tightening investigation by Special Counsel Robert Mueller, President Trump is viciously attacking the investigation as a "witch-hunt." It is also attacking the Justice Department and especially the FBI, its former director James Comey and its former deputy Andrew McCabe.* In response, former CIA Director John Brennan tweeted:

  > "When the full extent of your venality, moral turpitude, and political corruption becomes known, you will take your rightful place as a disgraced demagogue in the dustbin of history… you will not destroy America...America will triumph over you."[16]

  According to U.S. retired four-star general Barry McCaffrey:

  > "Reluctantly, I have concluded that President Trump is a serious threat to U.S. National Security. He is refusing to protect U.S. vital interests from active Russian attacks. It is apparent that he is for some unknown reason under the sway of President Putin."[17]

[15] "In secretly recorded conversations, Cambridge Analytica's CEO, Alexander Nix, claimed he had met Trump 'many times.'" https://www.theguardian.com/uk-news/2018/mar/20/cambridge-analytica-execs-boast-of-role-in-getting-trump-elected

[16] Tweet by former CIA Director John Brennan in response to the firing of Deputy FBI Director Andrew McCabe hours before his planned retirement.

[17] https://twitter.com/mccaffreyr3/status/974748724176941056

Keynote Address

Mr. Mounir Mahjoubi

Minister of State for the Digital Sector, attached to the Prime Minister

In the government of President Macron, I am responsible for digitizing the economy, helping startups to grow as fast as possible and digitizing the small and medium-size enterprises (SMEs). A second objective is to digitize the state itself. These two key objectives are built on two pillars: the first one is digital inclusion—how to bring people who do not digitize to use a digital format and help them do the conversion; the second one, which is what we are talking about today, is cyber security. There can be no digital transformation of the state and no digital transformation of the economy without cybersecurity. This is why both state and economic transformations are under the same ministry because we believe that these issues need to be treated together. So, thank you for letting me open the seminar on this subject and give a perspective on what we are doing, how we see the threat and how we politically envision how to act in the coming year.

There can be no digital transformation of the state and of the economy without cybersecurity.

I will start with the perception that the cybersecurity threat has never been as high as it is today. There are multiple reasons for that:

- First, we tend to measure more what is happening in the SMEs (small and medium-sized enterprises) and in the decentralized administration; and because we have been advocating for cyber security, more people talk about the risks and problems they have been confronted to.
- Second, there has been a diversification of the cyber threat. There are new types of actors and new dynamics between actors. In prior years, it was easier to understand how a state could try to threaten another state through the digital space. Now private organizations seeking to destabilize other private organizations or other states are being paid by private organizations or states. So, the dynamics between private actors, state actors, public actors, ideological actors, has never been as diffuse and agile. For example, a country may join forces with an ideological group from another continent and, together, pay a private organization to attack a network of private companies. There is no name for this, but it is a new type of attack and a new way for our states to look at the cyber threat and organize against it.

This raises multiple questions concerning operations and states and what we can do as we confront this new type of threat. Today the social structure, the judicial structure, the international judicial and legal structures have not been built at the same pace as the pace of the threat that we are facing. If we look at the international judicial process, we see that cyber criminality is in fact never sanctioned, or only in very few cases. In the case where one attacker would attack one single French citizen, an international judicial structure would not act on it because it would be too expensive and too small a case, but if you look at the numbers and sums involved, almost one million people have been attacked individually. So, this million does not fare well in a judicial procedure but it is nonetheless one million judicial procedures and we need to keep this in mind. On the contrary, when a large organization or state is attacked, it is quite easy for the international judicial process to act on it because it is like in the past and like a physical attack. A digital attack does not have the ability to refer to what was happening before in the physical world since no process and tools are available on the subject.

Another question concerns international law and the applicable texts and agreements on the subject. For the past five years, Ambassador David Martinon, who is here today, has witnessed the failure to reach a common view on what the applicable rules on cybersecurity should be. The most important issue is perhaps the level of understanding of the people who are the deciders. At international conferences on cybersecurity and digital topics that are not specifically specialists' conferences, you can observe that political leaders do not have the level that would be necessary for competent discussions and negotiations. This is why we mostly end up with solutions from the physical world or from the past because these are solutions that current political leaders can refer to through their past experience. There is not enough experience in the digital world yet. Although we are experts, the subject is too young and has changed too much over the past fifteen years. Likewise, it is probable that the dynamics over the next twelve months will be equivalent to the ones we witnessed over a period of ten years and this will go even faster in the future.

There is not enough experience in the digital world...The subject is too young and has changed too much.

These different considerations are completely changing the way we think about geostrategic and judicial subjects. At an operational level, we know how to act and make a decision within one hour; we know how to make decisions in a few days and we know how to organize ourselves. But at the geostrategic and political levels, we do not have this same capability. So, it seems to me that there is something in the operational mindset that is applicable to the political mindset. All the successes of startups, all the success of digital transformation come from organizations that introduced the values and speed of digital into the thinking of their specific domains.

We are now at a crucial moment and, by using pedagogy over the coming months, the French government wants to take every opportunity to incite French and European citizens, as well as SMEs, to raise their level of thinking on issues such as the Directive on Security of Network and Information Systems (NIS). This directive, which sets out the first EU-wide rules on cybersecurity, needs to be transposed into French national law and I am currently discussing it with parliamentarians. It is an excellent occasion for pedagogy because today you cannot be the leader of an organization or a company CEO without asking yourself about the cybersecurity question.

The other subject is the EU General Data Protection Regulation (GDPR) that will start in May and we will begin discussing it with the Parliament in a few weeks. This could be a revolution in terms of diffusing cybersecurity in the civil space. Because of GDPR, SMEs and large organizations will have the responsibility to protect the personal data and privacy of EU citizens but, as most of them already have some personal data systems, it will mean that we will have legal and economic tools that will allow us to give them better protection. We will also have sanction tools to make sure that they do protect these personal data. Currently we have no capacity in France to audit the network of SMEs and companies on the territory and no tools to ask them for more investment, more responsibility and more awareness of the subject. With GDPR, we will have the investment, the communications and the tools that are necessary to increase the level of security of our economic network. GDPR's positive effects will be to spread cyber security and give people a greater awareness of their own data.

GDPR's positive effects will spread cyber security and give people a greater awareness of their own data.

At the EU level, we are having difficulties finding common ground on definitions, on the processes, and on how to protect ourselves. These difficulties are not coming from large threats but from daily ones concerning certification and how to tackle the subject of diffused security in our country. At the international level, we are facing an impossibility. During the last few international assembly meetings, France has offered to start a new process to discuss cybersecurity. I believe that there has never been a better moment than 2018 to start this new round of discussions. The government truly needs a place where cybersecurity can be discussed at both operational and political levels. It is urgent to act on this and we need to have the same ability intellectually as we have operationally. There are not enough think tanks in the world working on cybersecurity, not enough governments investing in it, not enough public servants working on it—I will do my best to have more in France—not enough at the EU policy level where you can count on the fingers of one hand people who work specifically on cyber security, and some countries only work on operational subjects. So, this is the year to find a common ground on cybersecurity. Our program for 2018 will be to organize ourselves at the international level, help SMEs and the economic world, help our citizens understand the importance of cybersecurity, invest nationally to protect even more elements, and raise GDPR and the NIS directive to a higher level of awareness.

There are not enough think tanks working on cybersecurity, and not enough governments.

NATO in the Current Security Environment

Ambassador Tacan Ildem
NATO Assistant Secretary General for Public Diplomacy

It is a pleasure to be here in the former council chamber of the Sun King in the city of light. Paris is a true beacon for the world, not just for its history, art and culture, but also for its democracy. Just over two years ago, however, the city's lights were dimmed by heinous terrorist attacks. Briefly, the lights of Paris's most famous landmark, the Eiffel tower, went out. Today, I come with a simple message. French people are not alone and together we can—and will—overcome this threat. The specter of terrorism confronts many of our countries: Spain, Belgium and the U.K. have had similar experiences. So has my own country, Turkey, and the tentacles of terrorists have stretched far beyond Europe's borders. But it is our unity that is our greatest weapon, a unity that comes through Alliances like NATO. The recent wave of terrorist attacks has changed our peoples' perceptions. In August, public opinion polls of the French Ministry of the Armed Forces showed that terrorism has become the first concern of the French population. Now, more than ever, we need to respond.

The recent wave of terrorist attacks has changed our peoples' perceptions—In France, it is the first concern of the population.

One of the best tools in fighting terrorism is training local forces and building the capacity of local institutions. So, what is NATO actually doing? In addition to having every member of the NATO Alliance being part of the Global Coalition against ISIS, the Alliance itself recently signed up, too. This means we can bring not only our knowledge and experience to the battle, but also our equipment. Our work to fight terrorism involves many different lines of effort and type of activity, ranging from our Resolute Support Mission in Afghanistan to our training of Iraqi forces. We are also working on improving our awareness and the way we share information, so that Allies can take swift preventive actions against the threats we face, including terrorism. However, NATO's decades of experience, from the Balkans to Afghanistan, have taught us that one of the best tools in fighting terrorism is training local forces and building the capacity of local institutions. This is what we call Projecting Stability.

One clear example is in Iraq, where NATO is ramping up its efforts to provide training and assistance to Iraq in multiple areas. These include training for counter-improvised explosive devices and de-mining, military medicine, and assisting the country in reforming its security institutions. This year, we launched in-country training, as well as training personnel in neighbouring Jordan. We deployed a team to Baghdad to facilitate NATO's training and capacity-building programmes to support Iraq's fight against terrorism and instability. Projecting Stability is a way of providing more security for ourselves by having more stable and secure neighbours. It is an investment in others that benefits all. This will remain a focus for us next year, as well as exploring what more we can do together to support the fight against terrorism.

While terrorism involves high-profile attacks on our societies, we must also confront the more subtle ones every day.

Terrorism involves high-profile attacks on our societies and values but we must also confront the more subtle attacks on us taking place every day. One of the main ones is cyberattacks. The French Ministry of Defence, NATO and the EU have all recognized that even the largest international corporations or government branches are highly vulnerable to cyberattacks. We do not need any more convincing after seeing attacks that have targeted organisations ranging from Baltic governments, to European banks to the UK's National Health Service. We have also seen attempts to undermine our democratic processes, including here in France. Disinformation is not a new technique. But today it is part of the hybrid toolbox. They target not just our institutions, but also our way of life. They are an attempt to divide our societies from within. And we must respond, by continuing to raise awareness. NATO does not respond to propaganda with propaganda. We do so with facts, based on our values and from a position of strength. We are confident that the truth ultimately prevails. We also know that we respond to these challenges by strengthening our cyberdefences, as NATO has been doing.

We have seen attempts to undermine our democratic processes, threatening not just our institutions, but our way of life.

A number of Allies have identified Russia as one of the main sources of such attempts – but let me be clear: NATO does not seek conflict with Russia. Indeed, prior to its illegal annexation of Crimea and its continued destabilization of eastern Ukraine, NATO was working towards a strategic partnership with Russia. But, faced with a dramatically changed security situation, NATO had to respond.

A number of Allies have identified Russia as a main source of cyberattacks.

NATO's Dual-Track Policy towards Russia: Strong Defence and Dialogue

Defence. We have significantly enhanced our collective defence and deterrence. Since 2014 we have implemented the biggest reinforcement of our collective defence since the end of the Cold War in response to a changed security environment. NATO's four multinational battle groups in Estonia, Latvia, Lithuania and Poland are now fully operational. We are also making progress in strengthening our presence in the Black Sea. Our response has been defensive, proportionate, and in line with our international commitments.

We remain open to periodic and meaningful dialogue with Russia. It is not easy, but it is important.

Dialogue. At the same time, we remain open to periodic and meaningful dialogue with Russia. This year alone, we have held three meetings of the NATO-Russia Council with Ukraine as the main item of discussion. But we have also discussed transparency and risk reduction in Europe, as well as the situation in Afghanistan. Our dialogue is not easy, but it is important because, especially when tensions are high, such dialogue can help us reduce risks and increase transparency. However, we must not forget that Russia's illegal annexation of Crimea was the first time since World War II that a European country had attempted to change borders unilaterally. That goes against the international rules that Russia itself agreed and signed up to. The international community could not accept that. There could be no 'business as usual'.

Strengthening NATO’s Network of Global Partnerships

NATO-EU improved cooperation. With the array of challenges facing us, NATO is strengthening its network of global partnerships, first and foremost with the European Union. We have made major progress in doing so since the NATO Secretary General, Jens Stoltenberg, signed a Joint Declaration on NATO-EU Cooperation together with Presidents Juncker and Tusk in Warsaw last year. We are already implementing over 70 measures across many areas, including maritime exercises, defence industry and research, defence capabilities, and hybrid and cyber-defense measures. Now we need to harness this improved cooperation in new areas. We can provide for more coherence in developing capabilities, avoiding unnecessary duplication and making capabilities available to both NATO and the EU. It is also extremely important that this cooperation should proceed in full transparency with non-EU NATO Allies. This has become even more important with the advent of Brexit. If that proceeds as planned, by April 2019 80% of NATO defence spending will come from non-EU Allies, and three of the NATO battlegroups deployed to Eastern Europe will be led by non-EU Allies. The EU’s role in European defence is set to increase with the launch of the Permanent Structured Cooperation, in which 25 EU member states agreed to cooperate on defense and security policy. This has the potential to provide new capabilities and improve burden sharing within the Alliance. It could also help drive increased defence spending, which leads me to my final point: We need to invest more for our armed forces to function effectively.

First and foremost, we must cooperate with the European Union—a new agreement implements over 70 measures.

Boosting Allied Defence Investment. It has been one of the top priorities of the NATO Secretary General. In 2014, NATO Allies agreed at our Wales Summit to stop defence cuts, gradually increase defence spending and move towards spending 2% of their GDP on defence by 2024. In 2017, we estimate a real defence spending increase of 4.3% in Europe and Canada—a third straight year of accelerating increases. This translates into an additional $46 billion in spending over the past three years. Along with five other Allies, Romania has announced the intention to reach 2% in 2017, and Latvia and Lithuania have indicated they will do the same in 2018. France is also close to 2 %. So while we still have a long way to go, we are going into the right direction.

It is a necessity to defend our systems, people and values. As the city of light knows well, democracy dies in darkness.

For nearly 70 years, NATO has helped keep the peace in Europe by investing in defence and deterrence. It is the most successful Alliance in history because we have adapted as the world has changed. This is not a luxury, it is a necessity to defend our systems, people and values. As the city of light knows well, democracy dies in darkness. But together, we can ensure that our countries, and especially France, remain a beacon for the whole world.

The Ramifications of War in Cyberspace

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

Introduction

The ramifications of war in cyberspace could induce one to think that war in cyberspace is as codified and legible as in the land, air, and sea domains. Allow me to present several indicators showing that we are entering a Copernican revolution which will force us to think and act otherwise. Essentially, in what way is this space militarized? What are the military's responsibilities? Has the art of war been truly revolutionized? I believe part of the answer can be found in two major characteristics of the cyberspace, which is both a theatre of innovation and transformation but also an ever-growing space of conflict. The digital space forces us to rethink the way in which we manage this conflict and, as a result, the level of coercion that we must accept or not accept in this space.

Our British friends are right to say that the cyber weapon is a weapon of mass disorder in its potential.

The Two Characteristics: Conflict and Innovation

First, the Digital Space of Conflict. It is a grey zone, a fog, where this rather immaterial space, led by hidden actors that are increasingly numerous, actually has effects that are extremely concrete. Our British friends are right to say that the cyber weapon is a weapon of mass disorder in its potential. What are the threats that we perceive?

The first threat, the mafia crime, is at the lowest level of this space of conflict. It is a new form of crime that does not depend specifically on defence or national security, but it is a weapon that produces disorder and, depending on its sites, has generated 41 billion euros worth of damages last year.

When the electoral process is attacked, have we not also attacked the very existence of our democracy?

The second threat is attempts to penetrate the strategic digital networks of the state or state-owned businesses. We can think of the attack on TV5 Monde which falls under the sabotage category and, in that case, does not fall under national security anymore.

- It can also be a weapon of global disruption which makes us think existentially about the vulnerabilities of democracies—when the electoral process is attacked, have we not also attacked the very existence of our democracy?
- There is of course the cyber weapon that has become a spying weapon and is widely used by certain states. I am thinking of the leaks, Vault 7 and Vault 8.
- It is also a renewed propaganda weapon for the Jihadist groups. Even if the threat they pose has been minimized in the Levant, they are still pursuing their destabilization campaign—especially with the emergence of a professionalised propaganda in Africa and in the Sahel. We

can only fear that these relocations, whether in the Sahel, the Balkans or in Asia, will lead jihadist groups to perpetuate the use of the cyberspace as propaganda and threat tools against Western interests.

Our adversaries, whoever they are, are exploiting these grey zones perfectly and are finding digital sanctuaries.

As you can see, our adversaries, whoever they are, are exploiting these grey zones perfectly and are finding digital sanctuaries inside a zone of quasi-trust, freedom and progress that the internet has created. So, we must face these threats and actors, and we must rethink the way we manage this space of conflict in an area that is escaping any kind of framework and whose borders between crime and state actions are porous, where everything mixes. In the end, these actors are also pirates. They are at the same time state-like organisations and pirates and it is sometimes quite hard to differentiate them.

The question of how to manage this space of conflict has become an element of a strategic nature for states. What tolerance threshold can we accept? How should we respond? What are the organizational mechanisms, the doctrines? Our Anglo-Saxon friends are putting forward dissuasion, which France does not wish to endorse – because in our culture, dissuasion is eminently related to the nuclear area. I must admit that I prefer the concept of dissuasion over the concept of coercion, which leads us to believe that there is an acceptable tolerance threshold for states, and a threshold for what is unacceptable. This process of reflection is led today by the General Secretariat for Defence and National Security (SGDSN). I wanted to share it with you through the French cyber publication that the Prime Minister requested and that will give its conclusions at the start of next year.

Second, Cyberspace as a Zone of Innovation. This innovation constitutes a permanent change in an almost physical sense and it requires from us an adaptation that we are not necessarily prepared for. We must adapt to the arrival of artificial intelligence in our weapons systems, in the daily administration of the Ministry of Defence, but also in our military staff, and in the capacity to manage information and decision-making. It is also innovation in the art of war: How do we integrate this weapon with our conventional weapons? We have to combine them. It is innovation in our integration of technologies that are constantly renewed inside our operational structures. It is rethinking our procurement process. And it is rethinking this integration within our agencies.

Cyberspace is a zone of innovation and we must adapt to the arrival of artificial intelligence in our weapons systems.

The Ministry of the Armies (which is the old Ministry of Defense) has delivered a response to this new form of combat and threat by deciding to create a structure at the level of the Chief of Staff of the Armed Forces, which is the ministry's Cyber Command, and regroups three missions:

- The first mission is the classic protection of the systems, whether they are in France or on operation sites.
- The second one is a defense mission that can intervene against digital attacks or neutralize them, and also in the field of propaganda, which is a new mission for the army.
- The third mission can intervene in the action, which allows for the integration of the planning and operation management channels to gather response elements from attacks or to be substituted to conventional weapons.

Today, these three pillars of cyber defence depend on a rather strong and coherent focus on the entire continuity of the cybersecurity. Informing, anticipating, protecting, defending, and acting constitute the entire spectrum of my mission and its continuity. Behind it, I would say, are essential characteristics of this responsibility: One is operational, because I am in the field of protection, defence and action—an eminently federative characteristic. Second, what I do for the Ministry of Defence, I also do at the inter-ministerial level—today, I am practically co-stationed with the National Cybersecurity Agency of France (ANSSI) and I only exist by delegation of this general directorate. The third one is profoundly technical in nature: it links back to the innovation process and my capacity to integrate this renewed technicity within the ministry.

As Cybercommander, I am practically co-stationed with the National Cybersecurity Agency of France (ANSSI).

in the end, for what kind of war is all this organization? We could of course think that this digital space generates effects where remediation has to be within a short timeframe, where measuring the effect is complicated. However, I think our responsibility is double, coming from two angles. The first angle is the angle of action and the second angle is the strengthening of the relationship between the army and the public authority. If Marshal Foch's war principles, which he held dearly (freedom of action, concentration of efforts and economy of means) do not seem to be questioned, this space nonetheless establishes the superiority of having the initiative. In the cyberspace, the offensive will always be superior to the defensive. All of that is only a matter of time.

In the cyberspace, the offensive will always be superior to the defensive. All of that is only a matter of time.

The digital space creates for the army new options on the battlefield and on its operation at the tactical, operational, or strategic levels, through what I call the combination of weapons, through the continuity between cyber defense and cyber-attack, and my responsibility is to master this space to fit the exact needs of the management of my operations. Secondly, cyber creates the conditions for technical/operational superiority for the army. By combining the kinetic and non-kinetic effects, it creates a certain psychological superiority over those that do not have those types of capacity. It is also an employment field where clandestine actions and non-clandestine actions mix in an intimate way and which leads us to rethink the border between these two worlds.

By combining kinetic and non-kinetic effects, cyber creates a certain psychological superiority over those who lack it.

And it is most importantly an engagement which produces effects to the benefit of public safety. When I undertake the fight against Daesh propaganda in Syria, I generate elements of intelligence and knowledge of the national territory for the benefit of the action of the armed forces and action of the police, even the action of the judiciary, which is being questioned today.

This new form of combat also creates conditions. You must first understand the adversary's operations. For that, I must at the same time understand the evaluation of aggression, the tools they use. And that forces me to rethink in depth the relationship between the Ministry of Defence, and especially the army and the intelligence world. Today, we cannot decide on a digital action without knowing that there is an extremely strong organisation around its allocation. I am anticipating, but when I am being attacked, I suggest at the political level, if not certainties, at least clues which make it possible to hold the political weight on the allocation level. It forces me to handle the synergy between human intelligence, technical intelligence and the cyber operations of the ministry of the Armed forces. So, this is the first constraint.

My second constraint is that, in order to contest the adversary's freedom of operation, notably by using available tools, I must revise my relationship with other departments of the State. I was talking about ANSSI. Today, there are no threats that are not co-handled by ANSSI and the ministry of the Armed forces. Also, to contest the adversary’s freedom and take the lead, I must be in this innovation cycle for which we are not prepared. I am intimately convinced that the review of agencies, including the military and operational ones, will integrate engineers and data scientists within our operational units to be able to develop in almost real time either algorithms or tools available to decision-makers or to those that use weapons systems.

We must integrate engineers and data scientists within our operational units to be able to develop algorithms and tools in almost real time.

In the destabilization of counter propaganda and disinformation, I wanted to underline that I cannot perform this continuity between the police world and the judicial world. Today, it is this continuity in terms of organization that is being implemented. There is not a week now where I am not in communications with the Interior Ministry.

So, you can see that this new space of conflict imposes obligations on us, and perhaps rights tomorrow. It is a question that was asked before for that matter. But, most importantly, it will require that we rethink in our agencies the level of interoperability, of inter-ministerial cooperation, and also with businesses and globally. I often say that cyber and cyber security are a bit like counter-terrorism. Counter-terrorism took 15 years to shake intelligence services’ traditional culture and organisation vis-à-vis the rest of the State. I think cyber is starting to follow this same revolution.

Cyber is following the same revolution as counter-terrorism which took 15 years to shake the traditional organization.

This is quickly what I wanted to say on the topic, which does not necessarily offer answers on the place of the military in cyberspace but is a substantive issue.

I will finish with a question on our own ability to understand what is happening to us. I think the space of innovation, which is a technical, administrative and societal revolution, is also a space where conflict is starting to take root. Are we making the right choices? What is our leadership today? In any case, I question myself on my ability and that of my deputies to understand this profound transformation which today cannot wait.

Les Ramifications de la Guerre en Cyberespace

Général Olivier Bonnet de Paillerets
Commandant de la cyberdéfense, Etat-Major des Armées

Vous m'avez posé une question de fonds sur la place des militaires dans ce nouvel espace. Parce que la ramification de la guerre, c'est un thème qui pourrait laisser penser finalement que cette guerre dans l'espace numérique est aussi codifiée, structurée et lisible que dans les espaces conventionnels terre, air, mer.

Permettez-moi pour autant de vous livrer quelques pistes qui montrent que nous ne sommes qu'au début d'une révolution qu'on peut qualifier de copernicienne pour les militaires, et qui nous oblige évidemment à penser et agir autrement. Au fond, en quoi cet espace est-il militarisé ? En quoi les militaires ont-ils une responsabilité particulière ? Est-ce que l'art de la guerre est profondément transformé par cette révolution ?

L'espace cyber est à la fois un théâtre d'innovation mais aussi un espace de conflictualité grandissant.

Je crois qu'une partie de la réponse se trouve dans deux caractéristiques majeures de cet espace cyber qui est à la fois un théâtre d'innovation et de transformation, mais qui est aussi un espace de conflictualité toujours grandissant. L'espace numérique nous oblige à repenser à la façon dont on gère cette conflictualité et par là même le niveau de coercition qu'il faut accepter ou ne pas accepter dans cet espace.

Les deux caractéristiques : innovation et conflictualité. Sur la conflictualité, d'abord cet espace numérique, comme vous le savez, c'est une zone grise, un brouillard, où cet espace de conflictualité assez immatériel a pour autant des effets qui sont, eux, extrêmement concrets, qui sont menés par des acteurs masqués et toujours plus nombreux. Et nos amis britanniques ont raison de dire que l'arme cyber, c'est une arme de désorganisation massive dans son potentiel.

L'action mafieuse en cyberespace est une arme qui a généré 41 milliards de dégâts l'année dernière.

Je voulais revenir rapidement sur les menaces que nous appréhendons. La première d'entre elles, évidemment l'action mafieuse, qui est au plus bas niveau de cette conflictualité mais qui est une forme nouvelle de criminalité qui ne relève pas spécifiquement de la défense ou de la sécurité nationale, mais qui est une arme qui génère de la désorganisation et qui, selon certains sites, a généré 41 milliards de dégâts l'année dernière.

Deuxième menace, qui est évidemment les tentatives de pénétration des réseaux numériques étatiques ou des entreprises stratégiques de l'Etat. On peut penser à l'attaque sur TV5 Monde qui relève du sabotage et, là, qui ne relève plus directement de la sécurité nationale. Il y a aussi cette arme comme arme de déstabilisation globale qui nous fait réfléchir d'une façon quasi existentielle aux vulnérabilités des démocraties. Quand on atteint aux processus électoraux, est-ce qu'on n'atteint pas à l'existence même de notre démocratie ? Il y a évidemment l'arme cyber qui est devenue une arme d'emploi pour l'espionnage, qui est devenue une arme de grande prolifération avec des responsabilités de certains Etats. Je pense aux « leaks. » Je pense à Vault 7 et Vault 8.

En tant qu'arme de déstabilisation globale, il nous fait réfléchir aux vulnérabilités des démocraties.

C’est aussi une arme de propagande renouvelée par les groupes djihadistes qui poursuivent encore, même s’ils ont été atténués dans leur menace au Levant, leur entreprise de déstabilisation—en particulier, avec une inquiétude forte sur l’émergence d’une propagande professionnalisée en Afrique et au Sahel. On peut craindre que ces relocalisations, que ce soit au Sahel, que ce soit dans les Balkans, que ce soit en Asie, ne constituent finalement qu’une pérennisation de cette capacité des groupes djihadistes à utiliser le cyberespace comme outil de propagande et de menace contre les intérêts occidentaux.

Le champ de la propagande est une mission nouvelle pour l’armée.

Vous voyez que nos adversaires, quels qu’ils soient, exploitent parfaitement ces zones grises et trouvent des sanctuaires numériques au sein d’une zone de quasi-confiance, de liberté et de progrès, certes, qu’ont constitué l’Internet. Donc nous devons faire face à ces menaces, à ces acteurs, et repenser la façon dont on gère cette conflictualité dans ce domaine qui échappe à tout encadrement et dont les frontières entre criminalité et action étatique sont poreuses et où tout se mêle. Finalement, ces acteurs sont à la fois des corsaires. Ce sont à la fois des organisations étatiques et à la fois des pirates dont on ne sait à un moment donné plus très bien faire la différence.

Ces acteurs sont des corsaires—à la fois des organisations étatiques et à la fois des pirates.

La question de la gestion de la conflictualité devient une donnée de nature stratégique pour les Etats. Quel seuil de tolérance accepte-t-on ? Comment y répondre ? Quels sont les mécanismes organisationnels ? Quelles doctrines ? Nos amis anglo-saxons mettent en avant la dissuasion, ce que la France ne souhaite pas—parce que la dissuasion est éminemment, dans notre culture, liée à la chose nucléaire. Je dois avouer préférer au concept de dissuasion le concept de coercition, qui laisse à penser qu’il y a un seuil de tolérance acceptable pour les Etats, et un seuil d’inacceptable. C’est toute cette réflexion aujourd’hui qui est menée par le SGDSN et je voulais vous le partager au travers de la revue cyber française qui a été souhaitée par le Premier ministre et qui devrait donner ses conclusions en début d’année prochaine.

Je dois avouer préférer au concept de dissuasion—lié au nucléaire—le concept de coercition.

Zone de conflictualité, mais aussi zone d’innovation. Cette innovation constitue un changement permanent quasi au sens physique du terme. C’est un changement, je dirais continu, qui nous demande une adaptation à laquelle nous ne sommes pas forcément préparés. C’est une adaptation à la fois par l’arrivée des technologies de l’intelligence artificielle dans nos systèmes d’armes, dans l’administration quotidienne du ministère de la Défense, mais encore dans nos états-majors, et la capacité à manager de l’information et de la décision.

C’est aussi de l’innovation dans l’art de la guerre. Comment intégrer cette arme avec nos armes conventionnelles ? En les combinant, en nous substituant à ces armes. C’est aussi de l’innovation dans nos processus d’intégration des technologies toujours renouvelées au sein de nos structures opérationnelles. C’est repenser nos processus d’achat. Et c’est repenser cette intégration au sein de nos organisations.

Cette nouvelle forme de combat et de menace, le ministère des Armées (qui est l’ancien ministère de la défense) y a apporté une certaine réponse en décidant de créer cette structure au niveau du chef d’état-major des armées, qui est le Cyber Command du ministère, qui a regroupé trois missions.

La première, une mission classique de protection des systèmes, qu'ils soient en France ou en opération. Une mission de défense, qui permet d'intervenir contre les attaques informatiques ou de les neutraliser, mais aussi dans le champ de la propagande, qui est une mission nouvelle pour l'armée. Et enfin dans l'action, qui permet d'intégrer à la chaîne de planification et de conduite des opérations, de disposer d'éléments de réponse aux attaques ou de se substituer aux armes conventionnelles.

Vous voyez que ces trois piliers de la cyberdéfense aujourd'hui relèvent d'un choix assez fort de concentrer dans un tout cohérent toute la continuité de la cybersécurité. C'est informer, anticiper, protéger, défendre et agir qui constituent aujourd'hui tout le spectre de ma mission et de sa continuité. Avec derrière, il me semble, trois caractéristiques fondamentales de cette responsabilité.

La première, de nature opérationnelle. Je n'existe que parce que je suis dans le champ de l'engagement de la protection, de la défense et de l'action. Une caractéristique éminemment fédératrice. Ce que je fais pour le ministère de la Défense, je le fais aussi au service de l'interministériel. Aujourd'hui, je suis quasiment co-localisé avec l'Agence nationale de sécurité des systèmes d'information. Et je n'existe que par délégation de cette direction générale. Enfin, troisième caractéristique, profondément de nature technique, qui revient au processus d'innovation et de ma capacité à intégrer cette technicité renouvelée au sein du ministère.

Le Cyber Command est quasiment co-localisé avec l'Agence nationale de sécurité des systèmes d'information (ANSSI).

Donc cette organisation, mais pour quelle guerre finalement ? On pourrait évidemment penser que cet espace numérique génère des effets où la remédiation est dans des temps courts, où la mesure de l'effet est compliquée. Pour autant, je crois que notre responsabilité est renouvelée sous deux angles.

Le premier, c'est celui de l'action, le deuxième, celui du renforcement de la relation entre les armées et le pouvoir politique. Si les principes de la guerre de Foch, chers à Foch (liberté d'action, concentration des efforts et économie des moyens) ne semblent pas être remis en cause, pour autant cet espace consacre vraiment la supériorité de l'initiative. L'offensif sera toujours en effet supérieur au défensif dans le cyberespace. Tout ça n'est qu'une question de temps.

L'offensif sera toujours en effet supérieur au défensif dans le cyberespace.

Cela renouvelle pour les armées, premièrement, les options sur le champ de bataille, sur sa manœuvre, au niveau tactique, opératif ou stratégique, par ce que j'appelle la combinaison des armes, par la continuité entre la cyberdéfense et la cyber-attaque, où ma responsabilité, c'est la maitrise de cet espace au juste besoin de la conduite de mes opérations.

Deuxièmement, le cyber crée pour les armées les conditions d'une ascendance technico-opérationnelle. En combinant des effets cinétiques et des effets non-cinétiques, il crée une certaine ascendance psychologique sur celui qui ne dispose pas de ce type de capacités.

C'est aussi un domaine d'emploi où actions clandestines et actions non-clandestines se mêlent de façon intime et qui amènent à repenser la frontière entre ces deux mondes.

Et c'est surtout un engagement qui produit des effets au bénéfice de la sécurité publique. Quand je m'engage à lutter contre la propagande de Daesh en Syrie, je vais générer des éléments de renseignement et de connaissance sur le territoire national au profit de la police et des services de renseignement intérieurs. C'est toute cette continuité entre l'action des armées et l'action de la police, voire de l'action judiciaire, qui aujourd'hui est remise en cause.

Pour comprendre la manœuvre de l'adversaire, je dois à la fois comprendre l'évaluation de l'agressivité et les outils qu'ils utilisent.

Donc cette nouvelle forme de combat, et j'en terminerai là, elle crée aussi des conditions. Il s'agit d'abord de comprendre la manœuvre de l'adversaire. Pour cela, je dois à la fois comprendre l'évaluation de l'agressivité, les outils qu'ils utilisent. Et ça m'oblige à revoir en profondeur la relation entre le ministère de la Défense, les armées en particulier, et le monde du renseignement. Aujourd'hui, on ne peut pas décider d'une action numérique sans avoir une organisation extrêmement forte autour de l'attribution. J'anticipe, mais à la fois quand je suis attaqué, je propose au niveau politique, si ce n'est des certitudes, au moins des faisceaux d'indices qui permettent de responsabiliser le poids politique sur le niveau d'attribution. Cela m'oblige évidemment à assumer la complémentarité entre le renseignement humain et le renseignement technique et les opérations cyber du ministère des Armées. Donc première contrainte.

Il faut des ingénieurs et des « data scientists » au sein de nos unités opérationnelles pour développer des algorithmes en temps quasi-réel.

La deuxième, pour contester la liberté de manœuvre de l'adversaire, notamment en utilisant tous les outils à notre disposition, m'oblige à revoir ma relation avec les autres services de l'Etat. Je vous parlais de l'ANSSI. Aujourd'hui, il n'y a pas une menace qui n'est pas co-traitée entre l'ANSSI et le ministère des Armées. Çela m'oblige aussi, pour contester cette liberté et prendre l'initiative, à être dans ce cycle d'innovation dans lequel nous ne sommes pas préparés. Je suis intimement persuadé que la révision des organisations, y compris militaires et opérationnelles, fera que nous intégrerons à la fois des ingénieurs et des « data scientists » au sein de nos unités opérationnelles pour être capables de développer en temps quasi-réel soit des algorithmes, soit des outils à la disposition des décideurs ou de ceux qui emploient les systèmes d'armes.

Dans la déstabilisation de la contre-propagande et la désinformation, je tenais à souligner que je ne peux pas exercer cette continuité entre le monde policier et le monde judiciaire. Aujourd'hui, c'est cette continuité en termes d'organisation qui est en train d'être mise en place. Il n'y pas une semaine aujourd'hui où je ne suis pas en relation avec le ministère de l'Intérieur.

La cybersécurité, c'est un peu comme le contre-terrorisme—le cyber est en train de suivre exactement cette même révolution.

Donc vous voyez que ce nouvel espace de conflictualité nous impose des devoirs, et demain sans doute des droits. C'est toute une question qui a été posée d'ailleurs précédemment. Mais elle demande surtout de revoir profondément dans nos organisations le niveau d'interopérabilité, le niveau de coopération en interministériel, avec les entreprises mais aussi à l'international. Et finalement, je le dis assez souvent, le cyber, la cybersécurité, c'est un peu comme le contre-terrorisme. Le contre-terrorisme a mis quinze ans à bousculer les services de renseignement dans leur culture traditionnelle, dans leur organisation vis-à-vis du reste de l'Etat. Je pense que le cyber est en train de suivre exactement cette même révolution.

Voilà ce que je souhaitais vous dire rapidement sur la question, qui n'apporte pas encore forcément de réponse sur la place des militaires dans le cyberespace, mais qui est une question de fond.

Je me questionne moi-même sur notre capacité à comprendre cette transformation profonde et qui aujourd’hui ne peut attendre.

Je voulais en finir, et vous le comprendrez bien, par ce questionnement sur notre propre capacité à comprendre ce qui est en train de nous arriver. Je crois que cet espace d’innovation, à la fois de révolution technique, administrative, sociétale, est à la fois un espace dual où la conflictualité est en train de s’installer. Est-ce que nous faisons les bons choix ? Notre leadership aujourd’hui ? En tout cas, je me questionne moi-même sur ma capacité et celle de mes adjoints à comprendre cette transformation profonde et qui aujourd’hui ne peut attendre.

Merci d’avoir accepté que je parle en français pour porter encore plus encore ma conviction sur notre capacité ou pas à comprendre ce qui est en train de nous arriver.

Dealing with Terrorist Groups and State Actors: Cybercriminal Attacks, Active Cyber, and Toxic “News”

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

It is always an honor to be here and a time to be at our best because we are interacting with great experts. First, I could not agree more with general Bonnet de Paillerets about the fact that, when we talk about cyber, we are now in a situation where the lines are completely blurred. Sometimes, we think that we need to fight against conflictuality in cyberspace but also conflictuality involving states. Sometimes, we feel that our enemies are pirates or, at any rate, sub-governmental entities. In the case of WannaCry, we thought that we were fighting cyber criminals, but we may have been fighting states. Petya looked like a cybercriminal attack but perhaps it was an attack launched by a state. So, how do we fight those situations? Sometimes, we may have to confront the states and sometimes, we may have to start a judicial process. This is why we are very much attached to the universalization of the Budapest convention[18] so that we can be in a good position to fight or go after the authors of cyberattacks.

Wannacry and Petya looked like cybercriminal attacks but perhaps they were launched by a state.

My first point concerns where we are in terms of the 2016/2017 UN Group of Governmental Experts (GGE) process. Where do we stand? I believe that we made some significant progress in the last GGE round, notably in terms of norms of behavior, but since we did not arrive at a consensus report, none of this has been notarized. We still need to work on the issue of norms in cyberspace and continue the work of clarification of international law as it applies to cyberspace, even though the format of the GGE may not be the best one anymore. At least, we have to keep in mind that the expectations we had in the past may be too high now. Since the two previous GGE reports have acknowledged the possible application of international law to cyberspace, we need to insist on the fact that International humanitarian law is fully applicable. Other topics may be more nuanced and may require more focus and additional work.

We need to insist on the fact that international humanitarian law is fully applicable in cyberspace.

Second, we need to give a new momentum to the OSCE process. Some great achievements were made last year in terms of confidence-building measures. We need to keep working on them and make them operational so that we can test them.

[18] The Convention on Cybercrime, also known as the Budapest Convention on Cybercrime or the Budapest Convention, is the first international treaty seeking to address Internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations.

Third, we should try other things. Intergovernmental formats will always be necessary if we are to reach the kind of universalization that is required. We must talk directly to industry on several issues and fight the proliferation of cyber weapons, which will rely on a better definition of what a cyber weapon is. And in the field of active cyber defense, we will need to get a better definition of what is acceptable and what will never be acceptable and that is a difficult job.

For active cyber defense, we need a better definition of what is acceptable and what will never be acceptable.

We also believe that we have to work closely with software developers to make sure that they consider the need for better security in their product. Of course, if we have conflicts in cyberspace, it is because there is a digital battlefield and this battlefield is made of all the vulnerabilities that are comprised in the products that are in the mass market. We are currently reviewing a project on IoT that the U.K. has prepared. There is a lot of good in it and it is very similar to the initiative that we launched back in September in New York in the margins of the UN G8. It is important to push on those two topics in order to try to construct a safer digital environment.

Another issue that has already been evoked is fake news. When it comes to fighting fake news, the legal ground seems to be weak. How can we tackle this difficult problem? Fake news and fake news tools are part of foreign policies. It is not a secret that they are an instrument of diplomacy. This has been expressed by General Valery Gerasimov, Russia's Chief of the General Staff, in the description of his Doctrine,[19] so it should not come as a surprise. What is surprising is the level of sophistication of the fake news that we are facing, and I think it is only the beginning. What we are seeing now is very rudimentary, but it will become more and more sophisticated because the technologies associated with fiction and storytelling are getting better and better. In the future, we will be facing a kind of fake news that will be difficult to identify as fake. So, we need to tackle this question now. Last Friday, the French Minister of Foreign Affairs presented his international strategy for the digital economy and has announced that he would launch an event to see how we can make progress in this area.

The sophistication of the fake news that we are facing is surprising—and it is only the beginning.

I am in charge of another issue, which is the use of the internet for terrorist purposes. The problem is how to work with the big and small platforms to make sure that they take down in a short delay the kind of toxic mud that we can see on these platforms. We are currently negotiating with them to obtain a one-hour delay. But we believe that one hour is way too long and that, in a few months, we will have to start renegotiating to obtain a 10-minute delay. In the meantime, we will probably see the kind of progress that will lead us to think that even 10 minutes is too long. This is the same kind of problem that we are facing now with fake news, which is the control by the platforms of what they upload. I am not that keen on giving them the power—they have the technical power, and if they do not have it, they will have it very soon. But there is no legitimacy for the platforms to take down every comment, whether it is fake news, terrorist

We are currently negotiating with the social media platforms to remove toxic content within one-hour—it needs to be 10 minutes.

[19] General Valery Gerasimov wrote: ""The very 'rules of war' have changed. The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness. … All this is supplemented by military means of a concealed character."

content or child pornography, without outside oversight, because then, the power of these platforms would become infinite. This is a question for discussion with them.

We also need to encourage them to keep investing in artificial intelligence and improving their process, but, at the same time, we have to dialogue with them to make sure that freedom of expression is not completely erased from these platforms. We are working on that with them now, trying to reconcile statistics—the ones that they claim they have and the ones that we have—in order to build confidence between us. It is important to work with small platforms too because if you tackle the problem on one platform, the contents will inevitably be posted and disseminated through other platforms. New platforms, such as Snap or LinkedIn, have joined the consortium of the platforms that we are working with and we hope that European platforms can join the same movement because the momentum is on.

Algorithmic confinement must block toxic "news" from being applauded widely on the internet in minutes following a terrorist attack.

We also need to work on algorithmic confinement so that, in the case of an attack such as the ones that happened in London, Paris or other capitals, we do not see toxic mud being applauded everywhere on the internet in the minutes following the attack. In such circumstances, we must make sure that the platforms can push positive contents for the duration of the period during which the perturbation or destabilization of our societies is particularly high.

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

Mr. Conrad Prince

U.K. Cyber Security Ambassador, Defence and Security Organisation

I would like to focus on where we are in the U.K. in terms of developing our national capability and strategy on cyber. Just over a year ago, we published our Second National Cyber Strategy (2016 to 2021), a strategy backed up by 1.9 billion pounds of investment in transformational activity in cyber security. This is not business as usual, such as funding conventional information security work for departments. This is money that is invested in transformational change, and that strategy builds on the modernization and change that was produced by our First National Cyber Strategy in November 2011.

There are three pillars to the strategy:

- How do we defend ourselves in cyberspace?
- How do we deter people from attacking us? That is really about how we make the U.K. a hard target, a less appealing target.
- How do we develop our cybersecurity ecosystem—our industry, our skills, our science and technology, and our research base to the level that we need for national security purposes as well as for our prosperity purpose?

Defending Ourselves in Cyberspace

Let me talk about what we have done in this first year and identify a few lessons from a personal perspective. If you look over this last year, a key striking point for us has been the issue of scale, the intensity of the cyberattacks that we have faced and, in particular, the extent to which we are seeing a rise in hostile nation-state activities. There is a lot of material and very good analyses in the private sector about where these attacks are coming from, with a surprising number of them coming from hostile nation-states. Our prime minister, Theresa May and my friend Ciaran Martin, the chief executive officer of our National Cyber Security Centre (NCSC), have publicly commented recently about the attacks from Russia in the U.K. against our media sector, our Telco, our energy sector. There is a significant increase in nation-state activity, possibly a change in risk appetite, and quite a breadth in the nature of the attacks. This is a noteworthy development.

The U.K. has observed a significant increase in cyberattacks and a rise in hostile nation-state activities.

On the cybercrime side, we have observed in the U.K. that the criminal networks are becoming increasingly aggressive and focused. We are all very familiar with the growing commoditization of cybercrime, the ease of use of cybercrime techniques, and the increasing availability of those techniques. There is a refining of tradecraft, though not necessarily with particularly sophisticated techniques, but simply getting clever at deploying those attacks. As to ransomware, we have probably seen a doubling of it in the U.K. in the last year. Just to give you a sense of scale, in its first year, our new National Cyber Security Centre handled around 590 serious cyberattacks on U.K. soil. These were very significant attacks where the National Cyber Security Centre has had to swing into action. We saw the first deployment of our national crisis management capabilities that we would use in a

There is a refining of tradecraft and ransomware has doubled over the last year.

significant terrorist cyberattack and both our Home Secretary and our Minister of the Interior used the national crisis methodology to deal with the WannaCry ransomware attack.

How Do We Deter Attacks?

What have we done to tackle this? A key development has been the creation of our new National Cyber Security Centre. It brings together a number of different government bodies that had grown up over the last five years to handle different aspects of cyber, pulling them together into one place—a single 700 person center designed to manage national level incidents to protect our core services and core infrastructure and to increase the levels of the U.K. cyber defense. It is part of GCHQ, our national Intelligence and cyber agency. That link with the Intelligence and cyber dimension is very strong, and it is also a very public-facing organization. A lot of NCSC has been about how to engage publicly, how to demystify cyber, how to respond to attacks, and how to develop our technical responses. It has been a significant step forward for us.

Our new strategy is much more interventionist and now takes active defense measures.

Our new strategy is much more interventionist and we are taking another step forward with active defense measures. We have a program called "Active Cyber Defense." This is not hacking back, this is not offensive cyber, it is a different terminology. Our active program takes measures to minimize the impact from a high-volume commoditized cyberattack on individual users, using an automated way that is effectively invisible to the user. How do we, as government, working with industry, take these measures to block commodity attacks? There are a number of things that we are experimenting with now:

- We are using Domain Message Authentication Reporting and Performance (DMARC) to block fake emails, emails that are spoofing U.K. government addresses—particularly around our customs excise taxes and so on. Using the DMARC protocol, we blocked a hundred fifty thousand emails from one spoofed government address.
- We have developed our DNS service, developing data on bad websites and using that in an automated way to block users from going to bad websites with malware.
- We are working with a U.K. Company called Netcraft which provides very effective anti-phishing services. The average phishing site's duration in the U.K. has been reduced from 27 hours to 1 hour.

We are blocking fake emails with Domain Message Authentication.

This is the start of our experimentation with programs that do these sorts of automated national level activities to block users from large-scale commodity threats and it is an important part of our strategy. At the moment, this is all focused on the public sector and public service users. An interesting challenge for the future will be how we will roll this out to the country as a whole.

Our Work on Developing the Cybersecurity Ecosystem

Finally, I will touch on our work around the growth of our ecosystem and around skills. We have approximately 800 cyber companies in the U.K. and the market is worth around 22 billion pounds a year. We absolutely depend on the industry sector to provide the products and services that we need for our national cyber capability. As a government, there is no way we can deliver this alone. So, it is in our national security interest to have a very viable cybersecurity industry. We are investing in it and in particular in the startup sector. We have created a new Cyber Innovation Centre close to GCHQ, the NCSC in Cheltenham, and we are about to invest 14 million pounds in a London Cyber Innovation Center. We are working to support our startups in cyber with a program to identify startups that have a capacity to grow into larger scale companies. For all these projects, the government is working with industry, industry experts, and with academia to promote and develop an ecosystem.

We have a £20 million program to identify 5,000 promising children for increased mentoring and schooling in cyber.

On the skills side, we have a major skill shortage in the U.K. Thus, we are now investing about 20 million pounds to identify 5,000 school children, from age 14 years and up, and to give them significantly increased mentoring, summer schools, and online work in cybersecurity. It is a kind of elite program, not a general awareness program in schools. This means identifying school children with real aptitude, bringing them into cybersecurity and getting them hooked on cyber to help provide the cyber workforce for the future. It is an important program that builds on what GCHQ has been doing for a number of years and a major investment. So, we are standing up our national response, making it more coherent and creating new ways of protecting the individual and investing in our ecosystem.

What Lessons Have We Learned?

The government role is to be active. We continue to have faith in the core approach that we are taking, which is a more active and interventionist role for our government. This means not simply gathering intelligence and information or criticizing people for not having good basic cyber security but actually being quite active across the ecosystem to improve our protection.

The basics remain our core vulnerability. In terms of the threat that we have seen from Wannacry and from most other attacks that we have seen, one lesson is still about the basics. Many of you here are probably familiar with the issues around Wannacry and the National Health Service. They were about basic information insurance, failure to understand and manage networks properly, failure to keep patching up-to-date, failure to keep the antivirus up-to-date and lack of single central control networks. These basic things remain our core vulnerability and addressing them is critical. How can we address them? We can do two things: Incentivize behavior change and take the active measures that I talked about earlier. We still have major challenges around how to incentivize behavior change and how to incentivize our citizens, small businesses, large businesses, to improve their cyber security.

We need to incentivize behavior change and take active measures to improve cyber security.

Clarifying responsibilities. We need to do more in the U.K. to clarify the role of government, the role of the private sector, the role of civil society. Who is responsible for doing what? What is the balance for the government between encouraging people to change behavior, incentivizing them to do so, and compelling them to do so?

To adapt our strategies, we need to get better at measuring the harm caused by cyber.

The importance of data protection and measuring the harm from cyber. Minister Mahjoubi talked earlier about the NIS Directive in the General Data Protection Regulation (GDPR). We are very focused on those as our regulatory response in this arena and it will be an interesting exercise to see the impact of this regulation. If we want to adapt a strategy for the future, we also need to get better at measuring the harm caused by cyber. Our current ways of measuring it are not necessarily giving us the best insights into how we shape our investment and how we shape our responses.

Developing skills and encouraging the ecosystem. Finally, we must do more to develop skills and encourage that ecosystem because we depend on a strong industry base, a great research base, and skilled workers for us to deliver the protections that we need.

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

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

Roger asked me to address the question of how governments can help protect countries from hacking and cyber influence operations. I may have a surprising response to that question. We need to take hacking and cyber operations very seriously but there are responses that governments can take and, perhaps intentionally or somewhat unintentionally, we have been doing a fairly good job at that. I am not saying that we can all go home and rest, but we may be doing better than we think. Let me begin by slightly lowering the excitement of the discussion. In what sense would I expect cyber capabilities to be used in international conflicts?

Hacking and Cyber Influence Operations—Four Kinds of Scenarios

The first scenario is an all-out cyber war where a malicious state actor has compiled highly skilled capabilities for years and is using them for an all-out cyberattack against an enemy. Alternatively, it is a 16 year-old-teenager sitting in the basement of his parents' house who is doing the same thing. As you can see, these two scenarios are very different, and neither are probably entirely realistic. For the time being, I think that a cyber war where an international conflict is exclusively fought with electronic warfare means is an unlikely scenario. So, I am putting it aside.

Any warfighting effort will be accompanied by some form of cyber action. That is the reality.

In the second scenario, cyber capabilities are used in a larger conflict that is also being conducted with conventional warfare means. This is something that we have seen for years, at least since 2007 and possibly earlier, and we must realize that any warfighting effort will be accompanied by some form of cyber action. That is the reality.

Multi-layer efforts can destabilize a state, polarize societies, direct influence operations at the public and key policy makers.

The third scenario is the use of cyber capabilities as part of a hybrid conflict. This is where it starts to become interesting, because hybrid conflicts are difficult to deal with. They involve multi-layer efforts to destabilize a country and state, polarize societies, use influence operations directed at the public and at key policy makers, and the aggressor often resorts to clandestine actions in order to avoid attribution or retribution. This very much sounds like cyber capabilities have been designed for these types of conflicts and cyber capabilities do form a key element of hybrid conflict situations. These conflict situations remain below the threshold of all-out war, according to article 51 of the UN Charter, but they are nonetheless a considerable security and political risk.

Where preexisting tensions exist between countries, cyber can be the spark that blows up the powder keg.

Finally, in the fourth scenario, a military crisis develops from an apparently minor cyber incident. In 2017, an incident in the Persian Gulf area that in itself was not all that significant—a website was defaced and fake news were spread—turned into a political crisis. The incident picked up on preexisting tensions, almost spun out of control and developed into a political crisis that has not been entirely settled yet. These types of scenarios are imaginable in areas where preexisting tensions exist between countries and cyber is the spark that makes the powder keg blow up.

How Do We Respond to these Kinds of Scenarios?

The first response is to realize that cyber is an international security factor and security experts and diplomats need to take it seriously and think of how to respond. However, cyber capabilities do not fit well into our established security thinking. Some people believe that we have to rethink the entire world and completely start anew. I am not fully convinced of that because I learned a lesson some thirty years ago when I was in graduate school and became interested in how to prevent a nuclear crisis. Our teachers made us read Thucidides, Klausewitz, Sun Tzu and others. None of those military strategists had any conception of a possible nuclear age and nuclear confrontation but they developed strategic thinking ideas that actually proved very valuable in the age of nuclear confrontation. So, maybe we should not throw out the baby with the bath water but also think about some established and successful international security strategies.

When there are doubts about an attribution's reliability, it is difficult to generate the public support to credibly threaten deterrence.

Deterrence by Retaliation. One we always think of is deterrence. Deterrence is serving us quite well in the nuclear age but the narrow concept of deterrence by retaliation—dissuasion—does not work well when cyber is concerned. Why is that? If you are to deter an actor by threatening retaliation, you must be very sure of who you are actually directing the threat of retaliation to. Who do you want to deter? Who do you threaten to punish? You have to make clear to that actor what the consequences of any misbehavior on his part will be. This is very difficult in situations where there is an attribution problem, where the attacker may be hiding behind multiple screens, where you simply do not know to whom to address your threat. There is also the issue of doing this with sufficient public support. When there are doubts about the attribution, it is very difficult to generate the needed public support to credibly threaten deterrence. So, deterrence by retaliation does not work well in cyberspace.

Deterrence by Retaliation with Flanking Elements. However, a wider concept of deterrence has been put forward by people like Joe Nye at Harvard University who says that deterrence by retaliation should be accompanied by other elements of deterrence. One of those elements is deterrence by denial. Deterrence by denial did not work well in the nuclear age because it is difficult to defend against a nuclear bomb. Deterrence by denial implies digging a moat, building a wall, trying to make your side difficult to attack. That is what we have been doing for a while now with cyber hygiene. Cyber hygiene is trying to protect IT systems from malware. It is an important element of cyber deterrence, but it may not be sufficient. Why? Because this is a bit of a rat race. You always have to try and catch up with the innovation on the offensive side.

Deterrence by denial includes Cyber hygiene—trying to protect IT systems from malware.

So, you need another flanking element. It could be deterrence by entanglement. Deterrence by entanglement is the idea that states will behave better and will not even go to war when their domestic societies are entwined through cultural, social and economic ties and the internet is of course a great entangler. It makes it much easier to communicate, it is a great promoter of international trade, of a flow of ideas and therefore, it is an entangling element. States actually go beyond this passive use of entanglement when they also engage in confidence-building, when they actively exchange ideas and information with other governments. This is an element of building entanglement and improving communication between states.

Deterrence by entanglement is the idea that states will behave better and not go to war when their domestic societies are entwined.

Finally, there is another flanking element which is deterrence by taboo. Joe Nye calls that normative considerations that can deter actions by imposing costs to the reputation of an actor's soft power beyond the value he gains from a given attack. Building deterrence by taboo is what we have been doing in the United Nations where we are trying to promote a common understanding of existing and potential threats in the sphere of information security as well as cooperative measures to address these threats. This includes norms, rules and principles for responsible behavior of states, confidence-building measures, issues of non-use of information communication technologies in conflicts and how international law applies to the use of information communication technologies. This has been the mandate of the United Nations Group of Government Experts (GGE) which has been discussing these issues for the past two years.

Deterrence by taboo includes norms, rules for responsible behavior of states, confidence-building measures, non-use of ICT in conflicts.

Specific Levels of Action. Each of the deterrence elements I presented corresponds to issues on the international agenda and to specific levels of action: global, regional, and individual. You can arrange these elements and see that this is all about the rules that apply to state behavior in cyberspace; it is about the links between states and the confidence that states will apply those rules; and it is about the capacity of individual states to engage in rule-abiding and confidence-building behavior. This is pretty much what we have been doing for a while. We have been engaged in defining the rules, in building confidence and in building capacity for states to engage in positive, rule-abiding and confidence building behavior. The issue of information security has been on the United Nations agenda since the Russian Federation first introduced a draft resolution in 1998*.* Starting in 2004, we have had a series of five groups of government experts. Three of those have produced reports in 2009 and 2010, which represented twelve years of negotiations. In 2013, the experts agreed that international law applies and in 2014-2015, they provided detailed insights on how international law applies on the list of non-binding norms of responsible state behavior. In 2016-2017, the 15th group of government experts went further by trying to universalize what had been achieved in the past, but they failed to reach a consensus on one specific point of their mandate which was how international law applies. Interestingly enough, there is wide consensus that the failure of the 2016-2017 GGE does not affect the validity of the previous GGE reports. Our Russian and Chinese colleagues agree and want to continue this work in the United Nations.

The Organization for Security and Cooperation in Europe (OSCE) set the gold standard for regional level confidence building.

Building confidence has mainly been done at the regional level. The leading organization for this is the Organization for Security and Cooperation in Europe (OSCE), which set the gold standard. Other regional organizations are following in the OSCE's tracks—the ASEAN Regional Forum, the Organization of American States—and this has been quite helpful in building confidence in this context. Quite importantly, for two years in a row, the OSCE's ministerial council has issued decisions by the ministers to endorse this work and show the way forward for future work.

Finally, the whole element of cybersecurity capacity-building is mostly done by states at the bilateral level. One reason is that cyber capacity-building requires a lot of confidence between the two parties involved. This is probably a dangerous analogy but cyber security capacity-building is a little bit like marital relations: you only marry someone you really like. This is why cybersecurity capacity-building is mostly done on a bilateral basis and not in international fora. The U.K., the Netherlands, Germany, are quite active in this, and France is doing a lot in North Africa and other parts of the world.

Since it is so dependent on trust, cybersecurity capacity-building is mostly done by states bilaterally.

To summarize, there are things that states can do to counter the threats posed by hacking and cyber influence operations and I think that we have been doing fairly well already. The work is not done. It will never be completely done but I see the glass at least a little bit full and certainly not completely empty.

Multi-stakeholder Cooperation for Cyber Security and Defense

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

Public-Private Partnerships and Multi-Stakeholder approach

I have participated in this forum many times and always find it very elucidating. When we talk about the term public-private-partnership, everyone seems to have a different definition. It is clear that we need a multi-stakeholder approach to a lot of issues, but a multi-stakeholder approach does not necessarily mean that all stakeholders have the same role for every particular issue. As an example, at a time when we were trying to convince India to adopt a multi-stakeholder approach for internet governance, some senior Indian government officials asked, "If India is attacked, does that mean that we would need to consult with a multi-stakeholder group before responding?" We said, "No, you have certain rights and priorities as a nation-state to respond to security incidents—it will be good if you do talk to the private sector and civil society to expand your toolset, but that is not a prerequisite." This shows that there is misunderstanding about what multi-stakeholder means and a lot of misunderstanding as well about what public-private partnership means.

There is a misunderstanding about the meaning of both multi-stakeholder and public-private partnerships.

To me, public-private partnership is defined in terms of what you are actually trying to share. What does each side try to get from the other? Information exchange is one example. It has been difficult to have a good exchange between the government and the private sector. After the U.S. passed some pieces of legislation, there was a concern that sharing information with the government would run afoul of some competitive issues—if companies were to disclose information, their trade secrets would be out. So, a special provision was made to give companies protection under the Freedom of Information Act, but companies still did not share information. They did not share because they were worried about antitrust concerns. Then, the Department of Justice and the FTC inked a letter to say that if companies were sharing for these purposes, there would be no antitrust concerns. Nonetheless, there still was no really robust sharing because industry said that there were still liability concerns. So, about two years ago, some legislation called the Cyber Information Sharing Act (CISA) gave limited liability protection, but all those steps were just hurdles. The reality is that you are still not going to share information unless there is a business reason to do so. There have to be benefits for government and benefits for industry because, ultimately, that is the reason to share information. I think we are doing a better job at defining the criteria and what we are trying to share and that is really important.

Public-private partnerships are not going to share information unless there is a business reason to do so.

Another aspect of public-private partnership or a multi-stakeholder approach is that the U.S. is neuralgic to any kind of regulation. Europe is taking a different tack which reflects its cultural differences. Europe's Network Information Security (NIS) directive is more regulatory than the U.S. approach, particularly for critical infrastructure. In the U.S., the National Institute for Standards and Technology (NIST) has agreed on a number of best practices, working collaboratively with industry. In the long-term, it will help make this area more secure over time by working with the private sector, even though it was not a stated purpose.

As a "recovering lawyer" I am aware that, despite the U.S. being litigious about many things, there are not many lawsuits being brought by individuals for inadequate cybersecurity practices. The reason for that is that no real "standard of care" exists for cyber security and a standard of care, which no one has really defined, is needed to have liability. Likewise, to have a robust insurance market for cyber security, you need to have a standard of care too. Over time, voluntary standards like the NIST approach will create a standard of care that will create liabilities and also lead to cyber insurance. What Europe does in terms of the Network Information Security directive will also create a standard of care overtime. I am not in favor of a hugely regulatory approach on this but, in certain industries, it is going to have more effect over time.

For cyber, there is no real "standard of care," which is needed to establish liabilities or allow an insurance market.

I would also like to mention the Global Commission for the Stability of Cyberspace (GGSC), of which I am a member. It is a kind of public-private group, and it is not trying to compete with the Group of Governmental Experts (GGE) that Ambassador Martinon talked about earlier. In a sense, it is a supplement to the GGE on what the rules of the road are and what the norms in cyberspace should be beyond those that have been defined in the GGE. It is comprised of 27 commissioners from all over the world and from all walks of life, including civil society and the private sector. Its members are technology experts, such as Vint Cerf who helped create the internet, Bill Woodcock, who runs the Packet Clearing House, or Joe Nye, who is a famous academic from Harvard. It is chaired by Marina Kaljurand, a former foreign minister of Estonia and co-chaired by a former high-level Indian official.

We are proposing a new norm which is not to attack the public core of the internet.

The commission agreed on a norm, a rule of the road, that governments and individuals should not try to attack the public core of the internet. Basically, the idea is that nation-states would do certain things with the internet for intelligence gathering, for criminal law enforcement, and for other purposes. However, doing something that would have a general and wide-ranging effect on the internet—the domain name system, the routers—that would actually take down the internet or make it unavailable for a wide group of people, would do such harm that we do not think anyone should be involved in this. Of course, definitions are important, and we need to define what the core of the internet is. This is the first product of the Commission and, as we go forward, we are thinking of other products.

Roger asked me to talk a little bit about the U.S. National Security Strategy that will be coming out during the workshop. It has not come out yet, but I suspect that it will be largely consistent with what we have seen from the Obama and Bush Administrations since there is a lot of consistency on the cyber issues between these administrations. There is now a little more emphasis on deterrence, on bilateral relationships versus multilateral ones, but I also think that a bilateral relationship is a building block for a multilateral relationship. Another emphasis is on having consequences for bad actors, although I do not think anyone has done a particularly good job in that area.

Attribution: An Opportunity for Government and Private Cooperation?

Another area where I can see an opportunity for government and private cooperation is attribution. At the end of the day, attribution is a political issue and not just a technical matter. I was a prosecutor for many years, and I would say that the standard in the U.S. is not to have 100% certainty, but to be "beyond a reasonable doubt." When you look at attribution, you look at the technical evidence, the human intelligence, money flows and motives, and then you can make an attribution decision. When President Obama called out North Korea for being responsible for the Sony Pictures attack, virtually everyone had said that it was North Korea. When we finally made the official attribution to North Korea, however, a lot of people were in doubt because we could not share all the information that we had. We shared more than we normally do, but we could not share all of the sensitive information that told us that it was North Korea.

Assuming attribution is correct, what consequences can we impose on bad actors, especially bad state actors?

Assuming that we get by this attribution hurdle, what consequences can we impose on bad actors, and especially bad state actors? I would say that we must have credible consequences and these consequences must be timely. Doing something six months later is not timely. The actions that we took against Russia were strong, but they came six months later and that does not constitute a timely action that will deter someone.

Our toolset is pretty slim, although we can use diplomatic options like when we worked with China. We also have sanctions and economic options. We can use law enforcement actions, although they are really unlikely to deter a nation-state. We can use cyber actions, but people tend to think of cyber actions as a kind of red button to push that has some instantaneous effect, but in fact, cyber is not nearly as well developed as that. As one of my colleagues in the White House said, you can knock someone down with a cyber tool, but you cannot use it to put your knee on his chest and keep him down. So, this is not the kind of deterrent effect that you would like to have. It needs to cause pain and discomfort to the adversary, but we also need to be able to say that the pain is reversible, and that it will be taken away if he changes his behavior. Of course, there are kinetic options, but we are not going to launch a missile in response to a cyberattack, unless it causes death and destruction, and this is not going to happen. So, it is a limited toolset. Are there other things we can do? Can we block all internet traffic? Can we keep people off SWIFT, as the former president of Estonia suggested when I talked to him about this? This would require more thinking about our options, and their second-order consequences. I think this is a new area for private sector and civil society to collaborate on in order to think all of this through.

In response to a cyberattack, can we block all internet traffic or keep people off SWIFT?

Delivering Cyberspace Rules of the Road: From Theory To Practice

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

I will start off with the U.K.'s objectives concerning cyberspace. The U.K.'s objectives are framed around the notion of a free, open, peaceful and secure cyberspace. Today, we have talked about states looking at state-sponsored cyber-attacks and states wanting to exert more state control over the internet and using the digital hook to try to rewrite or undermine the existing International system. So, just like in the case of increasing cyber-attacks, the whole undermining of the international system feels very much like a growing threat. In order to combat this threat, governments, international partnerships between governments, and multi-stakeholder approaches involving industry and civil society, are clearly important.

In looking at the rules of the road, the previous panel reviewed some of the progress that has been made, drawing on the UN Group of Governmental Experts (GGE), the applicability of existing international law, the voluntary norms, the promotion of frameworks of stability and also events like the Global Conference on Cyber Space that took place in New Delhi in November or the Internet Governance Forum that is happening this week in Geneva—both of which are multi-stakeholder events involving industry and civil society.

Cybersecurity from Theory to Practice

We need to broaden our focus to include India—and the OSCE, ASEAN, and OAS.

What I would like to focus on today is how to move from discussions around the theory and what the rules of the road should be to the practice of what the situation is like on the ground. The way the U.K. is looking at this is centered around building cooperation and trust, transforming capacity-building, implementing confidence-building measures, and moving into implementing them as well as raising the cost of malicious cyber activity. Each of those draws on information exchange, cooperation and crisis management. So, building cooperation and trust is absolutely fundamental if we are to deliver a more positive environment for the constructive discussions that we want to have, whether in the UN or in other fora. We need to focus beyond our traditional allies—that was part of the reason why India was the host for the Global Conference on Cyberspace (GCCS) in November—and it seems like regional and multi-stakeholder fora are becoming ever more important. Others have mentioned the OSCE, but ASEAN and the OAS are also doing good work in that area, as well as the EU, NATO. There are discussions taking place in the G7 and G20.

Cybersecurity will be one of the strands at the Commonwealth Summit hosted by the U.K. in April.

Building Cooperation and Trust. As an example of trying to broaden the conversation on building cooperation and trust, the U.K. is looking at cybersecurity as being one of the strands for the Commonwealth Summit that the U.K. will host in April 2018. The Summit will bring in a different group of countries, many of whom want to build their capacity, knowledge and understanding in those areas. This very much feels like building a common understanding of the threat and being able to move on to solutions.

Transforming Capacity-Building. The second U.K. objective is around capacity-building and trying to turn it into a transformational space, a little bit like what happened with climate change. When you have a lot of small projects and a lot of bilateral engagements, how do you make them really transformational to deliver a step change? This is important because it builds confidence, it builds trust and it builds the capability that we can have in discussions at UN fora or elsewhere. It also reduces the attack surface area and helps the global response.

The Global Conference on Cyberspace in New Delhi showed a need to leverage more capacity-building funding.

A positive step forward happened when the Global Forum of Capacity Experts agreed to the global agenda for capacity-building during the Global Conference on Cyberspace in New Delhi. This set out agreed areas such as information exchange, cooperation on crisis management, training, and exercising. The next step is how to leverage more funding for this and we have been talking to development partners that look at big programs on digital access to bring cybersecurity trust and resiliency. We are doing our first project with our department for International Development, making sure that we are working closely together so that when they deliver on that digital access, we can make sure that capacity-building on the cybersecurity side is delivered as well.

Russia has blocked the OSCE's groundbreaking work on confidence-building measures.

Implementing Confidence-building measures. Confidence-building measures, the third U.K. objective, is a highly effective way of increasing cybersecurity. These measures are positive, pragmatic, and help build understanding, transparency, and trust on the ground. Again, we want to see more movement from paper into practice in this area and actual delivery on those measures. The OSCE has done groundbreaking work on this but, over the past few months, Russia has blocked it. So, as we try to move into a more practical space and deliver more of these measures, we are encountering obstacles. We need to try to overcome them and figure out as a community how to do it. I also agree with Merle Maigre that we need to do more testing and exercising. This is where you really see where the issues are, prompting questions like, "What would you do if? How would you deliver on that?" and doing it all the way up from the operational to the strategic level. It is absolutely vital to start delivering on these confidence-building measures. Trust and understanding also tease out some of those issues instead of just talking about them theoretically.

Raising the Cost of Malicious Cyber Activity. My final point is about raising the cost of malicious cyber activity. Cyber is like a low-cost area at the moment by appearing as a hybrid threat under the threshold. Some states are testing how far they can go and how much they can do before there is a reaction. As an international community, we need to be clear about what is not acceptable, what is not responsible state behavior, and what the consequences for such behavior will be. What are our diplomatic and economic tools? How do we make sanctions timely, which can be tricky when investigations are ongoing? How can we move into practice the EU toolbox, which has developed strongly over the past six months? There can be attribution of a broad trend, as U.K. prime minister Theresa May and the head of the National Cybersecurity Center, Ciaran Martin, did concerning Russia, or attribution can be specific around a specific threat. It can be done in public and it can be done in private and will always be in the national interest. But how do we deliver on that? How do we move to the law enforcement level (we are seeing progress on that) and how can we work with an ever-larger group of partners to deliver the deterrence messages and actions that together will have a greater impact? Finally, how do we ourselves model what responsible state behavior looks like? How can we be more

Some states are testing how far they can go before there is a reaction.

transparent about our capabilities and clearer about the applicability of international law, and how we can deliver on that? As all this becomes clearer and as we show what responsible state behavior looks like, we will be able to call out that behavior that does not look like responsible state behavior.

Cyber Security Lessons Learned

Ms. Merle Maigre
Director, NATO Cooperative Cyber Defence Centre of Excellence (CCD COE)

Introduction

Ten years ago, Estonia's digital infrastructure was hit by waves of denial of service cyber attacks during a period of heightened tensions with Russia. This incident, the first time that cyber was used in a coordinated manner against another state, set off a still-ongoing debate in NATO on the role of cyber operations. The attacks triggered a number of military organizations around the world to reconsider the importance of network security to modern military doctrine. They also promoted a first serious public discussion on the possible impact that cyber attacks could have on national security. What did we learn from this conflict at a national and international level? How can NATO develop better strategies to deter attackers, build up the cyber capabilities of Allies and contribute to stability in cyberspace?

Lessons Learned at the National Level

Openness and transparency during ongoing cyber attacks. One of the first and most crucial decisions back in 2007 made by the Estonian government was to be completely transparent with the outside world about what was happening and what the government knew. To go public with the attack was a conscientious choice reached as a result of debate and discussion with the opposition. Acknowledging publicly that cyber attacks were carried out all at once against the parliament, banks, ministries, newspapers and broadcasters was brutal and embarrassing, but it also helped contextualize the coordinated nature of the attack and open lines of communication with non-governmental institutions.

Information sharing in real time is a key way to defend collectively against a cyberattack.

The attack was a distributed denial of service attack from a botnet using computing devices around the world. Once Estonia put out the word about the attack, officials identified the IP addresses and host nations for every one of the devices used in the attack. Investigators eventually identified 175 jurisdictions around the world that hosted at least one of the devices used in the attack. Ultimately, they were able to communicate with and receive cooperation from all the countries that hosted those devices—except one. A decade later, governments at times still fail the transparency test around ongoing attacks, but the concept of information sharing in real time is now widely acknowledged as one of the best means to defend collectively against a cyber attack. Openness and transparency also help to build cooperation with the private sector.

Openness in communication during election hacking. Election technology has recently come into focus because of increasing attempts to influence elections and campaigns across the world. "Election hacking" covers phenomena ranging from email leaks and website defacement to compromising voter rolls or attempts to penetrate campaign finance voting systems. Often coupled with intense information operations, cyber attacks on systems linked to campaigns and elections mean that the adversary does not shy away from directly influencing the fundamental democratic processes of another nation.[20]

The legitimacy of I-voting elections depends on openly disclosing risks and vulnerabilities to the electorate.

Transparency measures significantly impact confidence and trust building among the electorate. Estonia has "established a trust relationship" with voters. It was the first country to introduce Internet voting (I-voting) in 2005 in a mode where the votes can be cast online during the early voting period. With the municipal elections of October 2017 being the ninth chance to vote online in a dozen years, the proportion of online voters has reached a steady level of one-third of the population. (31.3% at the 2014 European Parliament elections and 30.5% at the 2015 parliamentary elections). This is a steady increase from 1.9% in the first-ever I-vote in 2005.[21]

Risks and vulnerabilities must be openly addressed. One of the basic lessons learned from a dozen years of I-voting at national level is that the legitimacy of the elections does not only depend on the technical execution of voting procedures. Risks and vulnerabilities need to be openly addressed in public communication as the illusion of absolute security will undermine the election process once the first incident inevitably takes place.

The security of the electoral process requires clear standards. Naturally, given the fundamental importance of elections in a democracy, it is useful to set clear standards to ensure the security of the electoral process. This can be done by implementing baseline security standards including appropriate reporting and auditing for designated elections, but also for services that elections rely upon, such as population databases or digital identity.[22]

If a liberal democracy is to succeed, it also needs to take a holistic and comprehensive approach. This encompasses strategic communication, democratic education and securing the technology. As multiple campaigns demonstrated in 2016, this approach includes improving the cyber hygiene, awareness, capacity building and the operational security of political actors and candidates, allowing them to cover cyber security as well. Covering the basic cyber hygiene means changing default passwords and making passwords hard to crack, not using the same password for different systems, making sure that all systems are patched and up-to-date (including the use of antivirus software), ensuring that systems are only connected to the internet if necessary and making sure that essential data is backed up securely.

Lessons Learned at a Collective Level

Every military operation in any foreseeable military operation of NATO will have a cyber component.

Where does NATO stand today concerning its debate on the role of cyber operations and the changing nature of conflict? NATO has been taking cyber defence increasingly seriously in recent years, first making it clear that a cyber attack with severe impact could potentially trigger a collective defence clause and, more recently, defining

[20] Liisa Past, "All Elections are Hackable: Scalable Lessons from Secure I-Voting and Global Election Hacks" from the European Cybersecurity Journal, Vol 3, 2017.

[21] Nurse J., Agrafiotis, I., Erola, A., Bada, M., Roberts, T., Williams, M., Creese, S., An Independent Assessment of the Procedural Components of the Estonian Internet Voting System, Oxford 2016; Vassil K., Introduction, [in:] E-Voting in Estonia: Technological Diffusion and Other Developments Over Ten Years (2005-2015), Tartu 2016, pp. 1-13.

[22] Past, *op.cit.*

cyberspace as a an operational domain—that is, a likely battlefield. Last month, NATO made a dramatic change to its cyber policy. As the NATO Secretary General explained, different national cyber capabilities are as any other national capabilities owned by the nations. Nations own their planes, ships, cyber capabilities and they can share them with other allies and deploy them in NATO missions and operations. Every military operation, in any foreseeable military mission or operation of NATO, will have a cyber component. Therefore, cyber is also part of the review and adaptation of the NATO command structure. During their meeting in November, NATO defence ministers discussed how to strengthen the cyber element of the NATO command structure.

Challenges accompanying the NATO cyber policy shift. On the surface, NATO's cyber policy shifts might seem to be little more than incremental changes to its existing policy. However, the fact that the alliance is standing up a cyber operations center to integrate cyber capabilities from Alliance members sends a message that the Allies both possess and have the will to use their cyber capabilities and weaponry during military operations. But there are a number of challenges linked to this. For example, the Alliance needs a process by which national voluntary contributions for cyber effects are well defined and understood by commanders. The NATO Cooperative Cyber Defence Centre of Excellence is moving this issue forward with our work on the NATO cyber operations doctrine. We are also struggling with how to convince nations to move cyber effects out of the status of "national strategic assets." National strategic assets are difficult to deploy because of their classification and the high-level approval necessary to deploy them. How can we make a case that cyber assets should be operational assets whose effects can be understood and utilized by operational commanders, as is the case with the air, sea and land domains?

Important achievements and lessons learned. In addition to challenges of cyber security at a collective level, there are also important achievements and lessons learned. Among them are exercises. Exercises are the best way to prepare skills and build capacity. Their importance is to highlight a number of strategic concerns and topics that arise in connection with any hypothetical cyber crisis. These exercises provide the strategic guidance to address similar crises in real life. A major focus of our NATO CCD COE is to provide member states with practical training. This is perhaps best highlighted through our exercises. We organise Locked Shields, the world's largest and most complex international live-fire cyber defence exercise. Its aim is to teach to both military and civilians about the cross-dependencies from each other, to work together and to understand each other's systems. Our strategic gameplay is centered on how an individual nation should respond to a cyber attack, and how to make decisions from a legal and diplomatic perspective. The aim is to put constant pressure on the defending teams, to test them with the sort of full-scale cyber attack that hardened security professionals would hope to never experience in real life.

Exercises provide the strategic guidance to address similar crises in real life.

Organised since 2010, Locked Shields focuses on training for technical experts, policy staffers, legal and media advisors who are responsible for national cyber security. Teams deal with tasks such as:

- *How to report the technical developments in a humanly-readable form?* We do want our teams to be able to write humanly-readable reports about what is going on, something they could send to a manager or a government minister—condensing what they know into something that a non-tech expert can understand, because we have seen time and time again that this is a weak spot in the cybersecurity community. Cyber has been often considered by politicians as a technical matter. By now everybody likes to state that cyber security is important, but there is less comprehension by the strategic level on how and why. Therefore, we need to do a better job in translating the potential effects of technical processes into a language that is understandable at the political level.

- *How to respond to legal questions?* The legal picture around cyber operations is often unclear, so the teams have to do everything they can to ensure that they are behaving legally. For a cyber operation to qualify as an armed attack, it does not matter whether it is directed against public or private infrastructure or against military or civilian personnel. What matters are the scale and effects of the operation.
- *How to best engage with the media?* In the media element of the game, the teams have to be able to explain their actions and put across their point of view accurately, even when being questioned by journalists who are trying to trick the teams into saying too much.

In short, we need to take cyber security issues to the political level to show that cyber is not merely a technical matter. This is why Estonia recently organised the first ever strategic table-top cyber exercise, EU CYBRID 2017, at the Defence Ministers level. It was also attended by the NATO Secretary General. With that exercise scenario, the ministers were asked how they defined what was going on, how to communicate the incidents outside, as well as what would be the preferred course of action to deal with the cyber attacks. The focus of the exercise was on situational awareness, crisis response and strategic communications. These are all very much political and strategic issues.

Summing up the value of exercises, large scale cyber exercises like EU CYBRID, NATO Cyber Coalition or CCD COE Locked Shields provide a unique opportunity for national teams to be in rapidly evolving situations in which they rarely find themselves as a team in their daily jobs. What is the recipe for success? Seeing the bigger picture is the key: To see, understand, and communicate the big picture, without being lost in the small technical pieces. Adjusting your initial defence strategy on-the-fly is important. Cyber security needs more discussion at the strategic level to ensure leadership by the decision-makers. In cyber issues, international cooperation has a crucial importance—we all know that national borders do not exist in the virtual world. Cyber is a transnational and trans-institutional issue. In order to mitigate cyber threats, we need much better international cooperation than now.

Defending Critical Infrastructure from Cyber Attacks: France's High Tension Electrical Transmission Network (RTE)

Mr. Xavier Carton

Deputy Director of Information Systems, RTE (Réseau de Transport d'Electricité)

Our company, RTE (Réseau de Transport d'Electricité), is the French national electrical transmission system operator, a subsidiary of the EDF (Electricité de France). We are responsible for ensuring access to the French electrical grid for all power utilities, optimising the operation of the French power system, and ensuring the security of electrical supply. To give an idea of its scale, RTE has sales of nearly 5 billion euros and 8,500 employees.

Damaging the smart grid could have domino effects, possibly costing hundreds of billions of euros.

Cybersecurity Issues with the Electrical Grid

According to a 2017 report by the World Economic Forum, the risk of cyber-attacks on the electrical grid is greater than for natural catastrophes. It is also likely to grow faster, with the prosumers now playing an active role in the smart grid. Damaging the smart grid has many domino effects, with potential costs in the hundreds of billions of euros.

The cybersecurity risk in the smart grid is structurally increasing. Three major factors contribute to the structural increase:

- *The attack surface is growing:* Renewable generation, prosumers and smart appliances are not only connected to the grid, but they are changing the power and financial flows. This is exponentially increasing the number of attack points for the smart grid.
- *The coupling of the grid and its environment is increasing*: Power failures impact society, particularly due to the fast-growing digitization of a society highly dependent on IT servers. The linkages among the smart grid actors (utilities, prosumers, aggregators, the marketplace, etc.) and the growing electrification (electrical vehicles, heating) will amplify the domino effects, causing power failures to have cascading consequences.
- *The sensitivity of the installed base with insufficient cyber-protection is increasing:* This is first of all about existing utility products. Consider for instance the recent example of protection relays.[23] Digital products have been generalized for 20 years with limited cyber-defense, and, while new ones are much better, they are exposed to more communications (mobile devices, cloud, peer-to-peer) and thus bring new risks. A large majority of modern smart appliances are also recognized as sources of potential issues, with upgrade capabilities that are either limited or too expensive.

The cyber protection of the grid is insufficient, while adding new components bring new risks.

[23] https://nakedsecurity.sophos.com/2017/05/02/ge-patches-flaws-allowing-attackers-to-disconnect-power-grid-at-will/

Preventing and recovering from a smart grid attack is more complex than in other sectors. While a cyberattack in several sectors could be mitigated by a duplication of the IT infrastructure, the power system is more complex.

- First, because the domino effect will propagate the phenomena beyond the grid.
- Second, because some attacks may not only cause blackouts but will also physically destroy the electrical infrastructure, so that recovery times will be much longer.
- Third, because the software upgrades needed to prevent the activation of a known issue are delicate.

Some attacks may not only cause black-outs but will physically destroy the electrical infrastructure.

Just as the Stuxnet virus targeted Iranian nuclear centrifuges, the electrical grid is also vulnerable: access to circuit breakers could result in a short circuit damaging or destroying the substation; exploitation of multiple distributed energy resources could generate an electrical congestion of a line, putting it down; control of a wind turbine would make it possible to change the wind vane speed, damaging the equipment. The time and cost to repair are several orders of magnitude above the blackout without damage.

The smart grid is now in the radar of cyber terrorists, so damages are likely to grow. The number of attacks on the smart grid is increasing, while tools and strategies specific to smart grids have been discovered that are designed to target these installations. The Crash Override Malware[24] discovered in June 2017 explicitly targets the protocols used in the power industry, namely IEC 61850 and IEC 61870. Those protocols are used quasi-exclusively in the power industry, so this malware intentionally targets the grid.

The "Crash Override Malware" targets protocols used quasi-exclusively in the power industry.

In September 2017, Symantec published on its website a warning regarding the Dragonfly organization[25]. Here are some extracts:

> "The Dragonfly group appears to be interested in both learning how energy facilities operate and also gaining access to operational systems themselves, to the extent that the group now potentially has the ability to sabotage or gain control of these systems should it decide to do so."

The Dragonfly group is learning how energy facilities operate—and seeks access to operational systems.

My team, with thirty people working on cyber, is not large enough to deal with all these threats because there are millions of hackers.

Cooperation between RTE and the French Government on Cyber Security

In order to deal more effectively with these threats, RTE collaborates frequently with the French National Agency for Information Security (ANSSI)[26] within the Prime Minister's Organization. This cooperation includes, for example, a recent tender for renewing the SCADA project as well as a security data center

[24] https://www.us-cert.gov/ncas/alerts/TA17-163A

[25] https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group

[26] Agence nationale de la sécurité des systèmes d'information. ANSSI has more than 500 specialists devoted to the protection of information systems.

project. RTE also participated as a player in the 2016 Piranet exercise. At the same time, we also collaborate with other institutions like the EU, ENTSO-E, G7 and others in order to define standards and share experience.

Conclusion

Cyber risk is one of the main issues that RTE has to address. This risk is also very likely to grow faster, given that the prosumers are now playing an active role in the smart grid. Damage to the smart grid would have many domino effects, with costs that would amount to hundreds of billions of Euros. The imagination of cyber-terrorists seems to be without limits, and, as mentioned above, show that the economic consequences of some unfortunately realistic scenarios would be very severe.

The risks call for a major redesign of the grid—such as putting in place resilient micro-grids.

Protection cannot be achieved by relying only on traditional security counter-measures. Instead, the nature of the risks calls for a major redesign of the grid (such as putting in place resilient micro-grids). Technologies are available, but what is at stake now is the budget for deployment.

Finally, the main question is not to whether RTE will be victim of a major cyberattack, but what we will have to do the day after. While we are spending a lot of energy and money to protect our system and to make our employees aware of the risks, we must also be ready (to the extent it will be possible) to recover our systems in case of an attack.

The Use of Social Media to Spread Extreme Ideology

The Lord Harris of Haringey
House of Lords, United Kingdom

ISIS and increasingly other terrorist and violent extremist groups are using cyberspace and social media to radicalize, recruit, fundraise and train. This is the concept of "electronic Jihad" that was first promoted by Ayman Al-Zawahiri and Anwar Al-Awlaki, so the use of this idea has been quite long-standing.

The Jihadi rap video made by Sheikh Terra, "Dirty Kuffar," was released in 2004 and has been downloaded millions of times.

I don't know how many of you have watched execution videos or recruitment films that the Islamic State produces but their production values are becoming increasingly professional and effective. Again, this is nothing new. The Jihadi rap video made by Sheikh Terra, "Dirty Kuffar," was released in 2004 and has been downloaded millions of times. I tried to see it but discovered that it seems to have been blocked in the United Kingdom. This means that something is working, which is impressive, but the message has been disseminated very, very, widely. The film starts with what purports to be U.S. soldiers shooting an Iraqi and rejoicing. That is the same sort of process now used by ISIS to say that everyone not with them can be lumped into one Islamophobic monolith that they label as "The West" or "The Crusaders." Actually, this sort of process of labeling your opponents is used by extreme right neo-Nazi groups to demonize all Muslims as terrorists and beheaders.

A model student who stabbed the MP, Stephen Timms, was entirely self-radicalized over a period of 4-5 weeks.

The other phenomenon that has been developing over the last ten years is the process of self-radicalisation. In the United Kingdom, one of the most graphic examples was when a friend of mine, Stephen Timms, who is a member of Parliament in London, was attacked in his constituency surgery by Roshanara Chaudry. She had been a model student and was expected to do extremely well in all her examinations. Over a period of about 4 or 5 weeks, she changed from a model student to someone who had become entirely self-radicalized. There was no sign that this was directly orchestrated by any particular group—she had radicalized herself. She bought two kitchen knives and the one she decided she could conceal in her clothing was the shorter one. She stabbed Stephen in the abdomen but, luckily, the knife missed the vital organs. She was a model student who had self-radicalized and this is what we are increasingly seeing.

As ISIS approached Mosul, thousands of messages were posted saying an invincible ISIS army sent by God was arriving.

I already mentioned that the use of cyber tools by ISIS is becoming more and more sophisticated: in 2014, a UN report warned that ISIS's social media photos of jihadists holding kittens and also AK-47s were turning into a successful recruitment strategy.[27] In another example, an estimated 2,000 ISIS fighters took over Mosul in June 2014, overcoming the Iraqi army's 30,000 soldiers equipped and trained by the United States. A few months before, ISIS had developed the 'Dawn of Glad Tidings,' an Arabic language app

[27] Reported in *The Guardian* by Spencer Ackermann 30 October 2014.

which allowed users to hand over their social media accounts to ISIS operatives.[28] As ISIS approached Mosul, tens of thousands of messages were posted simultaneously, swamping social media feeds worldwide with the message that an invincible ISIS army supported by God and fulfilling a millennium-old prophecy was marching towards Mosul. Not surprisingly, many Iraqi soldiers stripped off their uniforms and fled because the message coming from all sides was that this was actually happening.

ISIS's technique is similar to fake news in which extremists provide answers to people's desire for simplicity.

Part of ISIS's recruitment technique is the message that you too can join the 'biggest baddest' gang in the world and star as the hero in your own action movie or video game on the net. This is very similar to the fake news phenomenon in which extremists like ISIS or the far right provide an answer to people's desire for simplicity within our immensely complex global environment. Eliminating all the confusing grey zones can be comforting, helping to build a global Muslim victimhood narrative. Anything that happens to a Muslim can be translated as being part of that global victimhood narrative.

Extremists of all types have been good at telling stories about corrupt political institutions, rigged democratic systems and "fake" media. As Austrian journalist, Julia Ebner, puts it: "Even if half of the world's population stopped believing in gravity, apples would not stop falling from trees; but democracy, the rule of law and press freedom are likely to collapse once people stop believing in them."[29] So, the message that these institutions are corrupt and do not really matter is extremely dangerous because, unlike gravity, they can disappear.

Democracy, the rule of law and press freedom are at risk of collapse once people stop believing in them.

Websites can host messages and propaganda videos which raise morale and further the expansion of recruitment and fundraising networks. There are online magazines translated into multiple languages like "INSPIRE" that tell you, for example, how to use common objects that you would find in your mother's kitchen which can then be used to kill the infidels. So, websites can be used as virtual training grounds, offering tutorials on building bombs, firing surface-to-air missiles, attacking soldiers and security personnel, and even entering and leaving countries illicitly.

Once people sign up to receive propaganda, they are selected, trained and incited to commit terrorism.

Now that Twitter and Facebook are shutting down pro-ISIS accounts more rapidly and effectively, users migrate to other providers like Telegram, which ISIS adopted rather than WhatsApp because Facebook had bought WhatsApp and it was assumed that it would probably not be secure much longer. Telegram provides both one-to-one and one-to-many encrypted communications on very secure platforms with hundreds of channels to disseminate propaganda but also individual guidance.[30] People sign up to receive the propaganda and, from there, they are selected, trained and incited to commit acts of terrorism. Seumus Hughes, Deputy Director of Washington University's Program on Extremism, describes a growth in what he calls ISIS "virtual

[28] J M Berger, 'How ISIS Games Twitter,' *The Atlantic,* 16 June 2016.

[29] Julia Ebner, 'The Rage,' I B Tauris and Co., 2017.

[30] *Journal of Strategic Security*, Vol. 10, Issue 3 (2017), by Ahmad Shehabat, Teodor Mitew and Yahia Alzoubi.

entrepreneurs[31]—intermediaries on social media connecting people in the West with extremist organizations.”

So, for the terrorists, using the web has a number of advantages:

- It makes it easy to hide behind anonymity (there are encryption tools and means of hiding data like steganography and “dead dropping” in draft files which can be accessed remotely)
- it provides the means to securely distribute information
- It gives access to a global pool of potential recruits and donors
- It also provides untraceable online payment services like Bitcoin

and of course, the tools for manipulation are already available for purchase on the Dark Web.

In fact, a cyberattack could more easily achieve mass casualties than a conventional attack.

I personally believe that it is only a matter of time before terrorists use cyber as a weapon itself, not just in terms of propaganda or recruitment, training etc. but also for attack and disruption. Such a method may not have the same visual impact as a bomb or vehicle attack, but it can cause huge problems—particularly if it is used in conjunction with a conventional attack. In fact, a cyberattack could more easily achieve mass casualties than a conventional attack. We have been talking about the impact of the grid being off for a period of days. In most countries, it would cause several thousand deaths in terms of failures of medical services. That is far more than is achieved in a typical conventional terrorist attack. So, my conclusion is that we underestimate terrorists’ and violent extremists’ use of social media and cyber techniques at our peril.

[31] “The Reach of ISIS’s Virtual Entrepreneurs into the United States” by Seaumus Hughes and Alexander Meleagrou-Hitchens, Lawfare, 28th March 2017.

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

Ambassador Fatih Ceylan
Permanent Representative of Turkey to NATO

The aim to defeat, degrade and ultimately destroy DAESH is still intact. We are on the verge of attaining this goal thanks to the tireless efforts of men and women representing national armies from all around the world. Let me pay tribute to those who are serving and those who have fallen for this noble cause of fighting terrorism. Thanks to our collective efforts, the physical presence of DAESH in Iraq and Syria has come to an end. Yet, the threat is far from over. Despite the success we have achieved so far, we should not lose sight of the clear need to address the root causes and the influence tactics that terror organizations use. For every youngster that is being radicalized to terrorism, there is a breeding ground in which distortion of facts, economic factors and ethno-sectarian and/or political grievances have a role to play.

The territorial integrity, sovereignty and political unity of Syria and Iraq must be preserved and strengthened.

That is why the international community should focus first on ensuring a genuine political transition in Syria and a political re-calibration as well as a reconciliation in Iraq in order to avoid the re-emergence of DAESH or similar terrorist organizations. The territorial integrity, sovereignty and political unity of those two countries must be preserved and strengthened. There should be no room for alternate terrorist organizations, loose actors and free-riders to exploit the still evolving situation there.

DAESH's ability to inspire and incite followers to commit acts of terror is not completely diminished. The cyber domain is still conducive to spreading its propaganda or claim responsibility for its attacks. Therefore, I will focus first on a strategic overview of Syria and Iraq with particular attention to what our next steps should be. Next, I will briefly elaborate on the cyber-terrorism aspect and last, I will touch upon what NATO's role could be. We cannot take up in isolation the future risks that DAESH poses to the transatlantic security—including through cyber terrorism. The ecosystem in which DAESH is nurtured needs to be carefully understood, analyzed and dealt with. This is key to being able to address its root causes effectively and avoid spillover effects elsewhere that would directly impact our security.

A Strategic Overview of Iraq

As Iraq's fight against DAESH is on the verge of a successful end, the inner structural political problems begin to resurface in Iraq. The insistence of the Kurdistan Regional Government (KRG) on holding an illegal referendum on independence in November in violation of the Constitution has shown the fragility of the post-DAESH dynamics in the country. Such precarious temptations should be avoided. Our position with regard to the territorial integrity and political unity of Iraq remains unchanged. While taking specific and measured steps to prevent the KRG from committing such a grave mistake, we never meant to harm the Iraqi Kurds. That is why we adopted a gradual approach when we were confronted with the situation. We will continue to support the Iraqi Government in its efforts to preserve the territorial integrity of the country and achieve the desired end-state.

The Kurdistan Regional Government's referendum on independence showed the fragility of post-DAESH dynamics.

Now the focus should be on restoring diversity, consolidating security and starting the process of reconstruction, not only in the disputed areas, but also in the areas liberated from DAESH. As we enter the post-DAESH phase, the Iraqi Government should give impetus to reforming the political and economic system and making it more inclusive and transparent, empowering local communities, devolving more authority to the governorates and starting a genuine campaign of national reconciliation, in tandem with efforts on reconstruction. The international community's support of Iraq's efforts to preserve its territorial integrity, achieve enduring stability and maintain the constitutional order, remains vital. We should all help Iraq become resilient against certain regional ambitions and domestic influences rivaling the authority of the Central Government.

The Iraqi government needs a campaign for national reconciliation and efforts on reconstruction.

What Should We Do in Syria?

When speaking about the ecosystem of DAESH, I would be remiss if I were not to touch upon Syria. The important question now is what do we have to do in Syria?

- First, we need to consolidate the cease-fire. The Astana talks are important since they are a confidence-building measure that is not intended to replace the Geneva process under the auspices of the UN.
- Second, we need to revitalize the Geneva talks which are the main basis for the political transition. The political solution is also essential for a more effective fight against DAESH and other terrorist organizations with different agendas.
- Third, speaking of other terrorist organizations, let me reiterate that we continue to disagree with the way operations like Raqqa, Deir Ezzor or Manbij were conducted. Oppression of local people, regardless of their origins or beliefs or gender, forced displacement of locals, demographic alterations, use of child soldiers, razing of villages, closing down opposition political parties, their offices and media outlets, assassination or detention of dissidents as well as customary public executions. Now, most of you would probably pair all these crimes with the terrorist organization, i.e. DAESH. Well, I must say you are wrong. This is a non-exhaustive list of what PYD/YPG, the direct offshoot of the PKK terrorist organization, has been doing in Syria, unfortunately with the help of some Allies. PKK has been designated a terrorist organization by the international community and PYD/YPG is its Syrian franchise. There is abundant evidence of a link between PKK and PYD/YPG. The collaboration with a terrorist organization to defeat another, even for tactical reasons, is a grave mistake. Short-term tactical actions have become a source of perpetual instability in our region. Never could anyone imagine that the Coalition would give weapons, ammunition and air support to Al Qaeda affiliates just because they were against DAESH. Now that HTS (Hayat Tahrir Al-Sham) is fighting with DAESH in Hama, shall we give armored vehicles and over three-thousand trucks loaded with weaponry? Such ill-designed cooperation schemes are flawed and doomed to failure.

  Collaboration with a terrorist organization to defeat another, even for tactical reasons, is a grave mistake.

- Fourth, the administration of the areas that have been cleared of DAESH should be assumed by indigenous elements that have legitimacy in the eyes of the local population. The presence of PYD/YPG in Arab-majority towns is sowing new seeds of ethnic strife. Therefore, priority should be given to ensuring the return of local populations to the liberated areas as soon as possible. In this respect, let me re-emphasize that Turkey cannot be part of any effort that might legitimize a terrorist entity with a separatist agenda.

- Fifth, once the ultimate goal of the political process has been achieved, Syria's reconstruction will naturally be the next step ahead. Before seeing any meaningful progress on the political track, however, funding reconstruction projects might be premature.

Iraq and Syria must have governments that are seen as legitimate by all segments of their population.

For both Iraq and Syria, there must be a governing authority that is seen as legitimate by all segments of its population. The state must have the monopoly to exercise its sovereignty within its internationally recognized borders and the state's ability to secure those borders must be intact. Any kind of instability prevailing in the Fertile Crescent would risk a resurgence of DAESH or different versions of it by exploiting the power vacuum. This may lead to a reversal of the accomplishments we have achieved. We cannot allow this instability to be exploited by any terrorist organizations without distinction.

There is also a broader issue: In post-DAESH Syria and Iraq, we should exert the utmost care not to give breathing space for sectarian or territorial ambitions. If left unchecked, this would become a recipe for new conflicts and instability. Any attempt to conduct Great Game version 2.0 in Syria and Iraq is as dangerous as the DAESH v. 2.0. It would just trigger further ethnic and sectarian tensions, foment all kinds of centrifugal tendencies in Syria and Iraq and lay the groundwork for the next wave of terrorism dominating the scene, and infecting the Euro-Atlantic area.

The Cyber Terrorism in the Region

Early indications show that terrorist organizations are developing offensive cyber capabilities.

Now some comments on the cyber side of the story: Internet propaganda is probably the most common use of technology by terrorist organizations, spreading the language of hate. But they also use the Internet for recruitment and mobilization, fundraising, data mining, information gathering, secure communications, buying false documents and disseminating training materiel to militants and what have you. There are also early indications that terrorist organizations are developing offensive cyber capabilities. The aim could well be to attack critical infrastructure or the computer systems of targeted countries.

Consequently, addressing the strategic communications and social media dimension collectively to prevent and counter terrorism also remains an urgent and unrelenting challenge. Together we need to kill the ideology of these terrorist organizations. As a guiding principle, we should remain sober about the very fact that they have nothing to do with Islam and do not represent Islam as a religion of peace.

Fighting terrorism is integral to NATO's approach to deterrence, defence and projecting security.

What Could the Role of NATO Be?

NATO has already been responding to this threat. NATO has a role to play and adds value. This is without any doubt. Let me recall again that NATO's Afghanistan operation was launched following a terrorist attack against an Ally. Our maxim has always been "solidarity and indivisibility of security." Fight against terrorism will not and cannot be an exception. This threat requires us to act faster and be more flexible and adaptable.

At their special meeting in May, our leaders defined the fight against terrorism as being integral to the Alliance's approach to deterrence, defence and projecting stability. It is related to all three core tasks. That said, bolstering our deterrence and defence capabilities should be *primus inter pares.* Employing more robust efforts of partnership and crisis management is also important. In this respect, NATO's defence and related capacity-building activities stretching from Maghreb to Mashreq rank atop.

As an ambassador representing a country that is the last stronghold of the transatlantic community against the scourge of terror, particularly for the rest of Europe, I must reiterate that eliminating DAESH is not an issue that Turkey can solve on its own. Neither can it truly be defeated without accommodating our considerations and concerns.

The ecosystem that nourished DAESH is still intact, so DAESH look-alikes such as PYD/YPG should not have our support.

I shall conclude as I started by saying that the ecosystem that incubated DAESH is still intact. The remedy is to address the needs and aspirations of the real owners of the Fertile Crescent, not less, to support the moderate peoples and forces in the region. The DAESH look-alikes such as PYD/YPG should not have the privilege of our support. That is what Turkey will continue to stand for. We all know only too well that terrorist groups like DAESH, Al Qaeda or YPG/PKK seek to undermine our unity and solidarity to advance their agendas. But in the face of their attempts to divide us, one of our greatest strengths is our ability to contemplate and work together. Year after year, workshop after workshop, as long as we keep fostering our collective thinking, winning not only the battle but also the peace will be easier to attain.

Dealing with Jihadism: A View from the Southern Region

Ambassador Luis de Almeida Sampaio
Permanent Representative of Portugal to NATO

In the fight against terrorism, NATO is doing a lot, but should NATO do more? Is it doing enough? Could NATO do it by itself? Those are the main questions that we ask ourselves at NATO when we discuss Jihadism and the fight against terrorism. Article 5 of the Washington Treaty was invoked and acted upon for the first time in its history after the 9/11 terrorist attacks against the United States, which led to a major NATO operation in Afghanistan. In the wake of these attacks, NATO had to deal with a flow of events that rapidly changed all our lives and our political environment and, consequently, the Alliance can truthfully claim to have a lot of experience in the fight against terrorism.

NATO is still divided on its participation in the coalition against ISIS.

Yet NATO is still very much divided on the question of its participation in the coalition against ISIS. As you may know, John Kerry, who was the U.S. Secretary of State at the time, presented initial formal proposals for NATO to join the coalition in December 2015. But it took more than a year and a half for NATO to finally decide that it should formally be part and parcel of the coalition. This is very important and very telling because it highlights how sensitive this divide is within the NATO organization and its 29 member-nations. Two main dimensions circumscribe the divide: First, the geography of the fight against terrorism and second, the instruments or tools in the international toolbox to fight against Jihadism and terrorism.

There is a Geography to the Fight against Terrorism

Let me talk briefly about the geography and why it matters so much. I will take as examples countries like my own, Portugal, or even Spain, Italy, or perhaps France and other countries on the Southern shore of NATO that are very close to the Mediterranean. When we talk about terror, Jihadism or terrorism, it would be very difficult to convince the public opinion of these NATO nations that we are only talking about Afghanistan or Iraq. For the majority of these countries, the terror threat comes from much closer, from the Sahel, which is in our geographic and geostrategic vicinity. In Portugal for example, if we say that NATO does whatever is needed to fight terrorism because it has been engaged in Afghanistan for the past 18 years and now it is formally part of the coalition against Daesh in Iraq, the public opinion would not feel comfortable or safe with these kinds of statements. As I mentioned earlier, the public opinion in the southern rim of NATO close to the Mediterranean basin considers that Jihadism is much closer geographically than Afghanistan and Iraq.

For most Mediterranean countries, the terror threat comes from the Sahel, which is a geographic and geostrategic vicinity.

NATO needs to address this issue if it wants to display an important show of unity in July during the next Summit in Brussels. It is not the question of East versus South that will be at stake. NATO will need a 360-degree approach by the end of the Summit. We achieved a remarkable consensus and balance in Warsaw in July 2016, but we need to reinforce that consensus and that unity. Otherwise, these different security perceptions will create an imbalance at the outcome of the Summit and NATO will suffer from that. The divisions inside NATO would obviously be highlighted by any decision claiming that NATO is much more focused on only one of the strategic directions instead of a 360-degree perspective.

Does NATO have the Necessary Tools to Fight against Jihadism and Terrorism?

NATO has not yet developed the needed tools to fight against terrorism.

If we think about the Maghreb, the Sahel and the Mediterranean further south in terms of the fight against Jihadism in the Mediterranean basin, a second important question is "with what tools?" Does NATO have in its toolbox the necessary tools, means and mechanisms that would allow the organization to claim a meaningful role in this fight? The answer is, not yet. When we shift our focus geographically from Afghanistan and Iraq to the vicinity of many NATO member nations, we must recognize that NATO has not yet developed the tools that would allow it to play a frontline role in the fight against terrorism. This is very important because there are international organizations that probably have much better tools and are better prepared and we can also even claim that the bulk of the fight against terrorism in this geographic area is the responsibility of states. It is an internal security problem that should also be dealt with on a bilateral basis and, as mentioned earlier, there is this ongoing geographic divide within NATO and within the European Union and other international organizations. But the fact that we recognize that NATO does not have yet the needed tools while other organizations and states already have those tools leads to another dimension of the question, which is the division of labor and partition of responsibilities. If this division of labor could be solved in the future by a political decision, it would entail a much greater degree of complementarity and coordination between different international organizations. We are relatively far away from achieving that. If you look at the 34 measures that were agreed to on 5 December to expand the cooperation, complementarity and coordination between NATO and the European Union institutions, you will easily reach the conclusion that there is very little in them that can be identified as being important tools to fight Jihadism. We all know that Jihadism will be with us for years, probably for decades, and we must think strategically in order to fight it. So, the geography of Jihadism matters a lot in what concerns NATO's unity and NATO's cooperation with other international organizations. Of course, the issue of the tools in the toolbox is probably key.

Many issues that relate to the fight against terrorism are also cultural and religious.

I will finish by pointing out that many issues that relate to the fight against terrorism are also cultural and religious—a long-term set of problems that are not for us to solve. It is arrogant on our part to pretend that we can impact or influence these problems. Their solution—the educational solution and the long-term cultural change of mind will be a task for the political, civilian and cultural elites of the countries that are in our immediate southern vicinity and in the Middle East. It is not for us to convince the Imams about the right way of reading the Coran, it is up to the respected political leadership of those countries, for the NGOs and civil society organizations of those countries to do so. When I say these things at international gatherings like this one, I immediately sense that there are doubts and questions, but again, it sounds very pretentious for us to pretend that we could ever have a serious impact on the cultural and deep religious divide in countries that are not our countries. That means that they should have the ownership of the process, the "appropriation" as the French would say. It is their responsibility, but we do not see yet a real significant display of that ownership and responsibility in the fight against terrorism.

Winning the Battle of Ideas in the Face of the Spreading Jihadist Threat

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

Three days ago, the French Constitutional Council, which is equivalent to the Constitutional Court, the Constitutional Tribunal, censored a French law that enabled the repression, the prosecution, and the condemnation of people who regularly accessed websites related to terrorism.

Of course, many were surprised in France, thinking: "At a time when we are engaged in a real war against terrorism, how can we legally disarm the public actors?" Actually, the Constitutional Court simply reminded us that we could not conceive of the digital space without relying on two essential poles – security and freedom – and in truth, between the two, a correct balance had to be found. I often say that it is a bit like an electric battery. You have a positive terminal and a negative terminal. The two do not touch, but it is thanks to these two terminals that light is produced.

It is because we have both *security* and *freedom* that we have an Internet that is open, for everyone's benefit.

Well, it is because we have security and freedom that we have an Internet that is open for everyone's benefit. So, the French Constitutional Council said: "You have gone too far in your security provision; Even with the fight against terrorism, and even with the fight against websites that make apologies for terrorism, you have gone too far. You have created an imbalance by instituting an unnecessary law that is unsuitable and not proportional."

It is interesting because the French constitutional judge simply said to the government and the security forces: "But you have all you need today to act against those illegal contents. You have a penal code that has many articles. You have penal proceedings that allow investigations which are sometimes very intrusive in private lives, with the interception of private mail, data capture, and audio tapings. All of that, you have. On top of that, you have intelligence services that have recently been endowed with a law to frame their actions. And you also have another vital element: the possibility of telling social networks: "You must remove the illegal content, if you are a social network; you must block it, if you are an Internet service provider; or you must dereference it, meaning you will delete the reference, if you are a search engine."

The government can tell social networks to delete "illegal content," ISP's to "block it" and search engines to "dereference it."

So, actually, we have today two solutions. For the first, faced with the massive amount of illegal content that has swept over France and other countries as well, we can say: "We will take a "sovereign" action, meaning it is the State that will intervene."

The second idea is to find another solution by communicating with social networks. In January 2015, as you know, France has been through an attack that really disrupted our public opinion: the Charlie Hebdo attack. In the following days, 19,000 official websites of museums, local councils, town halls, and towns were defaced—meaning that their data was modified with Daesh propaganda. Of course, people were concerned, because we often think that terrorism is far away. And then, we discovered that terrorism had arrived very close to our home, in our little towns. And that is an element that really changed things.

With the Charlie Hebdo attack, we discovered that terrorism is not far away—it had arrived close to our home.

The Interior Minister at the time, Bernard Cazeneuve, went to California to meet with the social network companies. I was not with him, but I know what he would have said: "In the end, there are only two solutions. Either we work together, or we will all die. We will die because we will become victims of terrorism. And you, the social networks, will also die, because at some point you will be rejected by public opinion, by those who use your networks and who are therefore indirect contributors to your advertising and to your business. They will all end up rejecting you. So, we have to be able to cooperate and to collaborate."

Minister Bernard Cazeneuve told the social media, "There are only two solutions. Either we work together, or we will all die.”

That is how in France, as well as in Europe, we started opening up a dialogue with social networks. It began with an Internet forum in December 2015. It regularly continues its work and includes not only the 28 member-states (for me there are 28 and not “27 plus one”), Europol, and of course, all the actors of the Internet, including the big Internet companies. Actually, the last meeting of this assembly was on December 6th in Brussels. We can clearly see that the European institutions and the private actors, which are the great organizers of content on the Internet, are slowly starting to work together.

This was not the only level at which we worked, however. After the Brussels attacks, there was a Justice and Interior Affairs council which decided to go further and to create a code of conduct for the European Union and the partners. Well, the partners came together at this Global Internet Forum to Counter Terrorism. The forum’s objectives are to share knowledge, share known websites, and also to implement algorithms allowing us to detect websites of a terrorist nature, and even detect those that could be put back online and create major issues.

And of course, Europe acted with a cyber package that, as you know, was suggested after Mr Juncker's address on September 13th, which showed that there was indeed a will to fight against content of a terrorist nature. So today we are really in a dialogue with social networks, which reminds me – and I apologize, because I will mention a French singer whom you may know, Serge Gainsbourg, who has a song called *Je t’aime, moi non plus. “*I love you, me neither.” *I love you*, refers to the social networks, since we will work together. But the *me neither* applies because you still have to be a bit serious. Recently, our German friends, who introduced the *Netzwerkdurchsetzungsgesetz* law on October 1st, have shown that they could be extremely directive with social networks, by saying: "Beware, if you don't do things correctly, you will soon be sanctioned for up to 50,000 euros."

Germany’s *Netzwerkdurchsetzungsgesetz* law warns the social media, "If you don't do things correctly you will be sanctioned up to €50,000."

To some extent, we can also see the tightening on the other side of the Atlantic. There is right now in Congress an investigative commission on the American elections, studying the hoaxes and fake news which could have influenced (or not) the outcome of this election.

So, there is also a certain will to employ “the carrot and the stick,” meaning: “we are willing to work to help you, but be careful, you must also work with us and in the way we are expecting you to."

Actually, this illegal content of a terrorist nature simply reminds us that Internet was built, some say, with three layers. The first layer is the hardware, the submarine cables, the data centres, the computers, the cables, the optical fibre, the routers – to talk like our industry friends who are with us today. All of that is the hardware and equipment layer which is important because you only need a power failure or an optical fibre cut for the system to shut down.

And then we have a logical layer, the layer of codes and of algorithms. This is the layer people talk about when they mention hackers, cyberattacks, and malware that is inserted in the systems.

But we have often forgotten the third layer, which is the semantic layer, the cognitive layer, or the data layer. And since it is the layer of data, it becomes the layer of meaning. Yet we have entered a battle which is not the battle of artificial intelligence, even if we also must be concerned about AI. It is the battle of meaning, because meaning is the real battle we are fighting. Meaning is the battle in which we will be winners or losers. It is the battle that relies first and foremost on speech and counter-speech. What use is it for Western countries to say: "it is not right to dictate what terrorist sites can say, if we don't even have a coherent discourse of our own? If we are not promoting values ourselves? If we don't uphold ideas that promote freedom, that promote equality between genders, that promote a certain number of practices that are our fundamental beliefs?

AI is not the battle that matters. It is the battle of meaning in which we will be winners or losers.

In the introductory speech of the conference, we said, "We must be brave." Yes, today, we must be brave. The problem is not technical. It's not legal. The problem is firstly about politics. And politics does not mean governments. Politics means us. It is you; it is me. We are the ones who must say: "Enough. We must stop." The time has come to uphold great values. Europe must uphold values, otherwise it has no purpose. If Europe is only there to formulate regulations or directives concerning the flow of water or the quality of certain products, it is useless. Europe must exist firstly to support and defend a message.

The time has come to uphold great values. Europe must uphold values, otherwise it has no purpose.

Actually, I do find that, even indirectly, with the general regulation on interpersonal data (GDPR), it is upholding a message for which we cannot yet measure the impact in the rest of the world, including in Africa, in the Middle East, and everywhere. Because everyone is wondering: "What is this European text? What are these values? What is this personal data? If we want to continue to do business with Europe, maybe we should start adapting ourselves to what Europe is doing."

So, I think that is a very important step. The battle of meaning has started. Today, we are in the midst of a discourse that is not a technical or an algorithmic discourse. It is a political discourse. And this is where, I believe, we must find the solution. Because we will not avoid a dead end without an impetus. This impetus is one that I would like to call “spiritual” – in the secular sense of the word, meaning an impetus of the spirit. One very important point is to collaborate with social networks. But we must not ask them to be the judges of meaning. That is for us to do, and for them to apply.

The battle of meaning has started. We are in a discourse that is not a technical one. It is a political discourse.

What I mean by that is that we could see how we could get, in fields other than terrorism, some errors of assessments. When the Little Mermaid of Copenhagen gets censored because she is too erotic, when a painting at the nearby Orsay museum, *l’Origine du monde* by Courbet, is censored because it is too pornographic, we can clearly see that there is a risk when we tell social networks: "The choice is yours. Filter it yourself, and we will look at it down the road."

I think that today, it is up to us to regain control. And it is true that it is important to see a number of algorithms pop up with technological ways to do this filtering. But I think that we must not forget that the filtering must first be human, and it is up to us to do it.

La Vraie Bataille dans laquelle Nous Sommes Engagés : La Bataille du Sens

Général (Gendarmerie) Marc Watin-Augouard
Fondateur du Forum international de la Cybersécurité (FIC)
Directeur du Centre de Recherche de l'École des Officiers de la Gendarmerie Nationale

Mesdames, messieurs, chers amis, pardonnez-moi de m'exprimer dans ma langue natale. Il y a trois jours, le Conseil constitutionnel français, qui est l'équivalent de la Cour constitutionnelle, du Tribunal constitutionnel, a censuré une loi française qui permettait de réprimer, de poursuivre devant les tribunaux, et de condamner les personnes qui allaient consulter d'une manière habituelle des sites à caractère terroriste.

Au moment où nous sommes dans une guerre contre le terrorisme, peut-on désarmer juridiquement les acteurs publics ?

Evidemment, cela a beaucoup surpris en France, où certains disaient: « Au moment où nous sommes dans une véritable guerre contre le terrorisme, comment peut-on désarmer juridiquement tous les acteurs publics ? » En fait, le Conseil constitutionnel nous a simplement rappelé qu'on ne pouvait pas imaginer l'espace numérique sans s'appuyer sur deux pôles essentiels—la sécurité et la liberté—et qu'en vérité, entre les deux, il fallait trouver le juste équilibre entre cette sécurité et cette liberté. Je le dis souvent, c'est un peu comme une pile électrique. Vous avez un pôle positif, un pôle négatif. Les deux ne se touchent pas. Mais c'est parce que vous avez ces deux pôles qu'il y a la lumière. Et bien, c'est parce qu'il y a la sécurité et la liberté qu'il y a effectivement un Internet ouvert pour le bien de tout le monde.

Donc le Conseil constitutionnel français a dit : « Vous avez été trop loin dans une disposition sécuritaire. Quand bien même la lutte contre le terrorisme, contre les sites qui en font l'apologie, qui provoquent aux actes de terrorisme sont à condamner, vous êtes allés trop loin. Et vous avez créé un déséquilibre en instituant une loi qui n'est pas nécessaire, qui n'est pas adaptée et qui n'est pas proportionnelle ».

Le juge a dit au gouvernement : « vous avez tout ce qu'il vous faut pour agir aujourd'hui contre ces contenus illégaux. »

C'est intéressant parce que le juge constitutionnel français a dit tout simplement au gouvernement, aux forces de sécurité : « Mais vous avez tout ce qu'il vous faut pour agir aujourd'hui contre ces contenus illégaux. Vous avez un code pénal qui comporte de très nombreux articles. Vous avez une procédure pénale qui permet de faire des enquêtes, et des enquêtes même très intrusives dans la vie privée, avec des interceptions de correspondance, des captations de données, des sonorisations. Tout cela, vous l'avez. Vous avez en plus des services de renseignement, qui sont dotés depuis peu d'une loi qui encadre leur action. Et puis vous avez aussi un autre élément essentiel : la possibilité de vous adresser aux réseaux sociaux en leur disant : « Vous allez retirer (lorsqu'on est hébergeur), le contenu illégal. Vous allez le bloquer lorsque vous êtes Internet Service Provider. Ou alors vous allez le déréférencer, c'est-à-dire que vous allez supprimer la référence, quand vous êtes un moteur de recherche' ».

Alors, en fait, on se trouve confronté aujourd'hui à deux solutions. La première, confrontés aux contenus illicites massifs qui ont notamment déferlé en France, mais pas seulement en France, on peut dire : « On va faire une action, comme on dit, régalienne. C'est l'Etat qui va intervenir ».

La deuxième idée, c'est peut-être de trouver une autre solution en dialoguant avec les réseaux sociaux. Nous avons connu, vous le savez, en France en janvier 2015, un attentat qui a beaucoup perturbé notre opinion publique : l'attentat sur Charlie Hebdo. Dans les jours qui ont suivi, 19 000 sites officiels de musées, de collectivités territoriales, de mairies, de communes, ont été défacés. C'est-à-dire qu'on en a modifié les données avec de la propagande pour Daesh. Cela a forcément troublé les esprits, parce qu'on disait souvent que le terrorisme, « C'est loin ». Et là, on a découvert que le terrorisme arrivait tout près de chez nous, dans notre petite commune. Et cela, c'est un élément qui a beaucoup changé les choses.

Ou bien nous travaillons ensemble avec les réseaux sociaux ou nous allons tous subir les conséquences.

Le ministre de l'Intérieur de l'époque, Bernard Cazeneuve, est allé en Californie. Il est allé rencontrer les réseaux sociaux. Je n'étais pas avec lui, mais je crois savoir qu'il aurait dit : « De toute façon, il y a deux solutions. Ou bien nous travaillons ensemble, ou nous allons tous mourir. Nous allons mourir parce que nous serons victimes du terrorisme. Et vous allez mourir, les réseaux sociaux, parce qu'à un moment donné vous serez considérés, y compris par l'opinion publique, par votre propre public, ceux qui utilisent vos réseaux et donc qui ont des apporteurs indirects de publicité donc du business, ils vont finir par vous rejeter. Donc il faut que nous puissions coopérer et collaborer ».

C'est comme cela qu'en France bien sûr, mais en Europe aussi, on a commencé à dialoguer avec les réseaux sociaux. On a commencé à dialoguer avec les réseaux sociaux parce que s'est créé un forum Internet en décembre 2015, qui continue régulièrement ses travaux et qui comprend non seulement les 28 Etats-membre – et je salue les 28, car pour moi il y en a 28 et non pas 27 plus un, il y en a 28 en tout – Europol et puis, bien sûr, tous les acteurs d'Internet, les grands majors de l'Internet. D'ailleurs, la dernière réunion de cette assemblée a eu lieu le 6 décembre dernier à Bruxelles. On voit bien qu'on commence progressivement à faire travailler ensemble à la fois les institutions européennes et des acteurs privés qui sont, en quelque sorte, les grands organisateurs des contenus sur Internet.

Un conseil « Justice et affaires intérieures » a décidé d'aller plus loin et de créer un code de conduite de l'Union européenne.

Ce n'est pas simplement à ce niveau qu'on a travaillé, puisque, après les attentats de Bruxelles, il y a eu un conseil « Justice et affaires intérieures » qui a décidé d'aller plus loin et de créer un code de conduite de l'Union européenne avec les partenaires. Et bien, les partenaires se sont rassemblés dans ce Global Internet Forum to Counter Terrorism. Ce forum a pour objectif de partager des connaissances, partager des sites connus et de mettre en œuvre aussi des algorithmes permettant de détecter les sites à caractère terroriste, et même de détecter ceux qui pourraient être remis à nouveau sur la toile et donc poser des problèmes majeurs.

Et puis, bien sûr, l'Europe a agi avec le paquet cyber que vous connaissez, qui a été proposé après l'allocution de monsieur Juncker le 13 septembre, dans lequel il y a effectivement cette volonté de lutter contre les contenus à caractère terroriste. Donc on est vraiment aujourd'hui dans un dialogue avec les réseaux sociaux, qui me fait penser à un chanteur français que vous connaissez peut-être, Serge Gainsbourg, qui avait une chanson dont le titre était *Je t'aime, moi non plus*. Je t'aime, moi non plus, c'est un peu ça. *Je t'aime*, réseaux sociaux, on va travailler ensemble. Mais *moi non plus*, parce qu'il faut quand même que tu sois un peu sérieux.

Récemment, avec une loi du 1er octobre Netzwerkdurchsetzungsgesetz, nos amis allemands ont montré qu'ils pouvaient être extrêmement directifs vis-à-vis des réseaux sociaux, en disant : « Attention, si vous ne faites pas les choses correctement, rapidement, vous serez sanctionnés jusqu'à 50 000 euros. » On voit bien aussi, dans une certaine mesure, le raidissement outre-Atlantique avec la commission qui a lieu actuellement au Congrès, une commission d'enquête sur les élections américaines, avec les hoaxes, les fake news, qui ont pu éventuellement influencer ou ne pas influencer l'issue de cette élection. Il y a donc quand même une certaine volonté de dire : « La carotte et le bâton. C'est-à-dire : je veux bien travailler mais attention, travailler aussi avec nous et dans le sens que nous attendons. »

Avec la loi *Netzwerkdurchsetzungsgesetz*, les allemands sont extrêmement directifs vis-à-vis des réseaux sociaux.

En fait, ces contenus illicites, ces contenus à caractère terroriste, nous rappellent tout simplement qu'Internet a été construit selon trois étages. Un premier étage, qui est un étage où il y a tout l'ensemble matériel, c'est-à-dire le hardware, les câbles sous-marins, les data centers, les ordinateurs, les câbles, la fibre optique, les "routeurs" – pour parler comme nos amis qui sont en face de moi. Tout cela, c'est une couche matérielle, mais qui est importante parce qu'il suffit que vous ayez une panne d'électricité ou une panne de fibre optique pour que le système s'arrête.

Et puis on a la couche logique, celle des codes, celle des algorithmes. Tout le monde en parle en disant : « Il y a les hackers, il y a les cyberattaques, il y a des malwares qu'on fait rentrer dans le dispositif. »

Mais on a beaucoup oublié le troisième étage, qui est l'étage sémantique, l'étage cognitif, l'étage des données. Et à partir du moment où c'est l'étage des données, c'est l'étage du sens. Or nous sommes rentrés dans une bataille qui n'est pas la bataille de l'intelligence artificielle, même si nous devons y réfléchir. C'est la bataille du sens. Parce que c'est la vraie bataille dans laquelle nous sommes engagés. C'est la bataille dans laquelle nous serons vainqueurs ou vaincus. C'est la bataille qui repose d'abord et avant tout sur un discours, un contre-discours. Que sert à nos pays occidentaux de dire : « Ce n'est pas bien de dire ce que font ou disent les sites terroristes », si nous-mêmes nous n'avons pas un discours cohérent ? Si nous-mêmes ne nous sommes pas porteurs de valeurs ? Si nous-mêmes nous ne sommes pas porteurs d'idées qui mettent en avant la liberté, qui mettent en avant l'égalité entre l'homme et la femme, qui mettent en avant un certain nombre de pratiques sur lesquelles nous reposons ?

Nous sommes rentrés dans une bataille qui n'est pas la bataille de l'intelligence artificielle – C'est la bataille du sens.

Le texte introductif de la conférence dit : « Il faudrait avoir le courage ». Oui, aujourd'hui, il faut avoir un courage. Le problème n'est pas technique. Il n'est pas juridique. Le problème est d'abord politique. Or la politique, ce ne sont pas les gouvernements. La politique, c'est nous. C'est vous, c'est moi. C'est nous qui allons dire : « Ça suffit. On arrête. » Il est grand temps maintenant de porter de grandes valeurs. L'Europe doit être porteuse de valeurs, sinon elle ne sert à rien. Si elle est là uniquement pour faire des règlements, uniquement pour faire des directives, pour réglementer le débit de l'eau ou la qualité d'un produit, ça ne sert à rien. L'Europe doit d'abord être là pour porter un message.

Il est grand temps maintenant pour l'Europe de porter de grandes valeurs—sinon elle ne sert à rien.

D'ailleurs, je constate que, même indirectement, avec le règlement général sur les données interpersonnelles, elle est en train de porter un message dont on ne mesure pas l'impact dans le reste du monde, y compris en

Afrique, au Moyen-Orient, partout. Parce que tout le monde se dit : « Qu'est-ce que c'est que ce texte européen ? Qu'est-ce que c'est que ces valeurs ? Qu'est-ce que c'est que ces données à caractère personnel ? Si nous voulons encore faire du business avec l'Europe, il va peut-être falloir que nous nous adaptions à ce que fait l'Europe. »

Donc, vous voyez, ça, je crois que c'est un élément très important. La bataille du sens est engagée. Nous sommes dans un discours aujourd'hui qui n'est plus un discours technique, un discours algorithmique. C'est un discours politique. Et c'est là où il faut, à mon avis, vraiment trouver la solution. Parce que nous ne sortirons pas de cette impasse sans faire cet élan. Cet élan qui est un élan, j'allais dire spirituel—au sens laïc du terme, c'est-à-dire l'esprit.

On ne doit pas demander aux réseaux sociaux d'être les juges du sens. C'est à nous de le juger. C'est à eux d'appliquer.

Il y a un point qui est très important, c'est que bien sûr il faut collaborer avec les réseaux sociaux. Mais on ne doit pas leur demander d'être les juges du sens. Ce n'est pas à eux de dire : « C'est bien » ou « Ce n'est pas bien. » C'est à nous de le dire. Et c'est à eux d'appliquer. Je veux dire par là qu'on voit bien comment on peut avoir, sur d'autres domaines que celui du terrorisme, des erreurs d'appréciation. Quand la Petite Sirène de Copenhague est censurée parce qu'elle est trop érotique, quand un tableau qui se trouve au musée d'Orsay juste à côté, *l'Origine du monde* de Courbet, est censuré parce qu'il est trop pornographique, on voit bien qu'on a un risque si on dit aux réseaux sociaux : « A vous de jouer. Faites le tri vous-même et nous, on verra la suite. »

Je crois qu'aujourd'hui, c'est à nous de reprendre la main. Et c'est vrai qu'il est important de voir apparaître un certain nombre d'algorithmes, de moyens technologiques pour faire ce tri. Mais je pense qu'il ne faut pas oublier que le tri sera d'abord humain, et c'est à nous de le faire. Je vous remercie.

Russia’s Cyber Influence Operations in the U.S. and Europe Are Causing Deep Divisions that Could Spark a War

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

The fact that we speak about the need for a new relationship with Russia is indicative of the constant deterioration of relations with that country after 2012. The illegal annexation of Crimea in 2014 and the subsequent military destabilization of Eastern Ukraine—both sanctioned by the West—have played a crucial role: Russia has lost the confidence of the West. The subsequent interference in the U.S. Presidential Elections, in the French Presidential Elections, in the attempted separation of Catalonia from Spain, and also in the BREXIT—because there is an investigation going on in Britain, all flatly denied by Russia, has only increased that mistrust.

The mistrust has been fed substantially by a brinkmanship policy on the air and seas re-launched by Russia vis-à-vis NATO countries some years ago. Now, some of us are questioning whether we would need new accords to prevent such air and sea incidents. But we had some agreements dating back to the Cold War that Russia simply stopped observing. And if we, say, conclude a set of new ones, what is the guarantee that these will be respected, when the old ones, which were perfectly fine, were not respected?

We also have to look at Russia through the lens of Russia being a major actor on the international scene. Whatever Russia does, it has an impact on the international system. Therefore, cooperation with Russia is preferable to confrontation if we are to solve some of the problems we all face. Sometimes, we do not have a choice. The Russians decide whether they will cooperate or not but, even when they do cooperate, their cooperation is rather punctual, therefore tactical. They have their own interests. Consider Syria, for example. Syria does represent a certain strategic dimension of Russia’s involvement there, but what are Russia’s true strategic objectives? Are they constructive or are they destructive? Is the current post-Cold War world order convenient to Russia or not?

What are the true strategic objectives of Russia? Are they constructive or are they destructive?

In other words, can we count on Russia to defend the current world order faced with an increasing number of big challenges or is Russia aligning itself with those who want to destroy it? The answer to this is fundamental in understanding correctly the title of our panel: *The need for a New Relationship with Russia—Despite its Cyber Influence Operations, Russia is Reaping Few Benefits, but it is Causing Deep Divisions that Could Spark a War.* In case Russia is constructive and a defender of the current world order, this title is warranted. We could say to Russia: “If you want to get some results, you should cooperate and change your attitude.” But what if Russia is pursuing a destructive agenda bent on destroying the current world order, most probably considering that it is unfair to its status and aspirations? Then this would be exactly what Russia would like to achieve: Pitting one against the other to cause deep divisions, even risking war. Actually, this is what Russia is doing. So, we must pay attention to this major question, “What are the strategic objectives of Russia? “

There are claims that Russia should be given a “droit de regard” in certain areas, which are the normal spheres of influence of the great powers. Russia’s new concept of politics is actually the old concept of politics from the 19th century and beginning of the 20th century. My question here is, How relevant are spheres of influence in a globalized world when we see that not even the national sovereignty of the great powers can be protected from outside interference? If a great power is granted a sphere of influence, can it protect it and jealously guard it as being the only power that can make decisions in that sphere of influence? I do not believe that it works! With globalization, Russia has been denying the value of spheres of influence by interfering in every country that becomes a Russian target. So, how would you expect anyone to respect a deal on spheres of influence?

> **How relevant are spheres of influence when the national sovereignty of the great powers cannot be protected from outside interference?**

I think that this is a matter for reflection. Our problem in Romania is that we are too close to Russia and we have seen in our experience a lot of things that were not always good. As a result, in view of the historical record, we are more distrustful of Russia compared to other countries that are further away. Therefore, we have to balance other countries’ views of Russia, which are more benign, and our view, which is not. In the end, Russia is what it is. We will have to find a way to keep this important actor of the international scene in a more cooperative mode and not in a competitive mode. If we manage to do that—and I am a bit skeptical, the effort will be worth taking.

Propaganda, Fake News and Influence Operations: How to Respond?

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

I have been asked to talk more specifically about fake news and not just about the Russian hacking operations. We have mentioned the possible influence of fake news on Brexit, on the 2016 U.S. elections, on the recent French elections, and on the Catalonia referendum. The concern in each of these cases is really about the propagation of news that is fabricated to influence opinion, destabilize societies, and weaken national cohesion—or worse. So, I will stick to the big picture but will be happy to discuss our research in terms of operations.

My first point is that this is really a new debate over an old problem. Whenever disruptive technologies arrive, they can be political game changers and empower new actors—this was observed after the invention of printing when the church worried about its potential loss of control and loss of political power. The whole issue of propaganda, false news and influence is not new. We have seen it with the Protocols of the Elders of Zion[32], and we have seen it during the Cold War or when elections are manipulated in many countries.

Since influence operations have always existed, how are they different today? Perhaps we need to distinguish between two different kinds: One kind of news is completely false, and its motivation is profit. In fact, it has never been so easy to profit from fake news by just making a few clicks on a computer. That is a scam, a cybercrime, and it really needs to be dealt with in a special way. Some platforms are developing strategies to prevent profiting from fake news by using a combination of human or artificial intelligence, or possibly by requiring the certification of sites that are allowed to receive ads. The more worrisome kind is news that is distorted or presented in a biased way with the intention of influencing opinion in order to pursue strategic goals. This raises the question of what is objective truth, who has the legitimacy to decide what the truth is, and what can be done?

What is objective truth and who has the legitimacy to decide what the truth is?

The debate over truth in the traditional media was resolved with editorial responsibility and potential liability.

For a while, that debate was resolved in democracies with editorial responsibility and the liability of the traditional media. There were editorial boards that acted as filters but now, we have a double crisis: Traditional media are losing ground, losing power, and losing credibility. This is mostly because their business models are being challenged by platforms, but also because their filters are no longer as good and respected as they were in the past. Some media—Fox News and possibly MSNBC—are not as “fair and balanced” as advertised and they are taking a lot of blows for it.

[32] The Protocols of the Elders of Zion is a fraudulent document that served as a pretext and rationale for anti-Semitism in the early 20th century.

The second factor is that, not only are social networks totally unfiltered, but this is actually their own business model. In addition, a number of leaders are undermining the credibility of traditional media by calling them biased and referring to them as fake news. I will not mention any names! At the same time, these same leaders are propagating their own so-called “alternative facts.” So, these factors tend to reinforce each other by blurring the very notion of truth, which becomes a sort of relative notion. It is leading to a whole new notion of objective truth that people have called the “post truth” world. This is raising some questions about how we can determine what is true and what is not and, unfortunately, the Russians might be willing to take advantage of that. Ambassador Martinon mentioned this morning the notion of relative truth, which undermines the notion of objective truth.

The mere fact of news being amplified through the internet can influence opinion.

A third factor to take into account is the amplification of the news through the internet. News may or may not be fake and may or may not be distorted. Yet, the mere fact of its amplification can influence opinion. So, we are dealing with something new where quantity is more important than quality. With this virality, with the use of botnets and algorithms that automatically reinforce the message, we now have what can be called “weapons of mass destruction” or even “weapons of mass distraction.” Not only is there big data available for micro targeting, paid suppliers for fake news, and paid advertising on social media to reinforce the message, but all of this broadcasting is free to the user. Since it is free, another filter has been removed. We can see that cyberbullying is on the rise, and intimidation is on the rise whenever you counter an argument and whatever its source. There are haters of all kinds. As a result, a former Facebook executive recently criticized the social media for how it affects the functioning of society. He cited an incident in India where a false report spread over WhatsApp and led to the lynching of 7 people.

So, we have a double problem. Because the notion of truth is undermined, we have an internal threat within our democracies: a loss of common ground, a rise of populism, and a crisis of trust in the traditional media. At the same time, we have an external threat, which is the manipulation by foreign actors of our weaknesses and of our internal problems. These two issues are very much linked. Since we cannot solve them without treating them together, it is even more important to treat them because the respect of our core democratic values—whether it is free speech, freedom of opinion, or freedom of dissent—is at stake. In international diplomacy, our credibility about our commitment to our values is at stake. In fact, I heard a Chinese scholar cite Google’s de-ranking of *Russia Today* and *Sputnik* to justify blocking the *New York Times* and *Facebook* in his own country. Consequently, we need to be careful about the vocabulary that we use and what we are trying to achieve. We need to consider whether we want to regulate any speech that is likely to destabilize our democracy. Would this include haters of all kinds and conspiracy theorist? How do we want to counter influence operations that try to destabilize our democracies?

How can we counter influence operations that try to destabilize our democracies?

We have different types of instruments available:

- The first one is the liability and responsibility of publishers’ platforms, something that is being done for child pornography. They should be able to filter content. Is that what we want? And what is the basis for it? Is it on the basis that the news is true or false? For traditional media to make that distinction, the incentive was to maintain their credibility or even to protect against liability in case of defamation. Platforms are only facilitators, however, so they are not producing content. They are just hosting it, and it would mean changing their model if they were to filter for content. One possible basis could be what is legal or not. This would raise the question of harmonization of legislation across countries, however, because these platforms all operate at the global level. And, of course, it is a problem that most fake news are not illegal in any way. Could it be done by distinguishing what is distorted news versus real information? But how do you define distorted news? How do you implement that technically? Is it by algorithms? If so, what kind of data do you feed to the algorithms? Can machine learning help to decide who has legitimacy?

Fake news is not illegal, but can distorted news be distinguished from real information?

- Our second tool is international law and the norms of responsible behavior, which we have talked about today. It is also a matter of establishing responsibilities and countermeasures and this involves dealing with attribution, which we have also discussed. I think the most important part is being creative and agile. It is all about educating people. It is about empowering credible media. We have also seen that initiatives are going forward. Google and Facebook created a coalition called “First Draft News” to provide guidance on how to find, verify, and publish content sourced from the social web. Traditional media have started to provide fact-checking services, and this is empowering people as well. We have seen initiatives for collaborative fact-checking. There is also research on understanding patterns in order to elaborate effective strategies and to find ways to disrupt capabilities, to counter messages, and therefore to discredit fake news.

The question is why are people receptive to all that crap—which they surely know is untrue?

In the end, it is a question of strengthening our democracies, because the real question here is, “Why are people receptive to all that crap?” That should be the central question and, unfortunately, I do not think it is.

Russia’s Policy: Continuation of War by Other Means

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

I will start by recalling an episode from recent history which, I think, is important to mention right at the beginning. The last meeting between Mr. Putin and the NATO Secretary-General—it was Anders Fogh Rasmussen at the time—took place in 2009 in Moscow. Secretary General Rasmussen was quite fresh in his function, and when he actually came to NATO, one of his three fundamental priorities was to improve the relationship with Russia. I was then at NATO as Assistant Secretary General for Defense Policy Planning and also part of the team that was preparing the checklist of the Secretary General’s main points and messages for the meeting. Mr. Putin, who was Russia’s Prime Minister then, was listening to Mr. Rasmussen´s list of ambitious proposals. When he finished, Mr. Putin said, “Do you know what my ambition is, Mr. Secretary-General? It is that your organization will cease to exist.” This was during the bilateral—the tête-à-tête. Much later, Secretary General Rasmussen shared this with us, the NATO ambassadors, in fact shortly before the end of his term in office. So, it is good to keep this in mind as Mr. Putin’s ultimate goal.

Russia sees policy as “the continuation of war by other means.”

A second preliminary comment is actually the title of my short exposé: It is the concept of Russian foreign policy, which actually goes back to the early years of the Soviet Union and to Lenin's reinterpretation of Clausewitz. Lenin was an avid reader of Clausewitz, and he reinterpreted the best-known dictum of Clausewitz as “Policy is the continuation of war by other means.” This is deeply instilled in the Soviet strategic mindset. If you look at the current top leadership in Russia, all of them were educated, socialized, and formed during the Soviet times. So, they see policy “as the continuation of war by other means.” Recently, I came across a quotation in a paper written by Mark Galeotti,[33] who is one of the best experts in this area. He cited a Russian diplomat who said, “We engage in foreign policy in the way we engage in war, with every means, with every weapon, with every drop of blood.” So, this not only confirms the assumption of the continuity of Leninism and its notion of a permanent struggle in the current Russian policy, but it also grasps well the substance of what we call hybrid warfare.

Their strategic goal is to transform the post-cold war order in Europe so that it serves Russian interests.

What is actually Russia's strategic goal since, naturally, Russia cannot beat NATO, cannot beat the West and cannot destroy us? The strategic goal seems to be, at least, to partially transform the post-cold war order in Europe so that it serves Russian interests, and to change, at least partially, the rules of the game. Russia wants to restore its great power status internationally, and Putin and his very small circle of power want to reinforce their grip on power internally. We therefore need to keep in mind that their foreign policy is to a large extent an extension of their internal policy. Their ultimate goal is to maintain their grip on power, and the “siege mentality” is instrumental to that end. As mentioned at

[33] Mark Galeotti is professor at the Institute of International Relations Prague and coordinator of its Centre for European Security.

various times, their tactics or partial goals are to impose a sort of limited sovereignty around Russia's border and, at worst, in parts of the post-soviet space. This is in order to create buffer zones between the West and Russia and to weaken the West, NATO, and the European Union. In other words, their policy is to divide and weaken us.

Russia uses cyber-espionage, manipulation, propaganda, subversion and sabotage—and a coup d'état attempt in Montenegro.

Since they cannot ever rule us, beat us and overwhelm us directly, indirect tactics, hybrid war, or ambiguous warfare come to the fore. It is an indirect approach, driven by the opportunism of a weak but completely ruthless actor. This includes cyber-espionage, manipulations, propaganda, in addition to ruthless, outright subversion and sabotage, and not only in the Ukraine where it would be obvious. There was an attempt at a coup d'état in Montenegro fomented by Russia, shortly before Montenegro joined NATO—which was to prevent Montenegro from joining. This is serious!

Today, cyber is the most feared dimension of that indirect approach, in the operational space that we have now established in NATO as a fifth domain. Cyber is instrumental in a wider context that is important to keep in mind—our social context, our political context. I believe that a key notion is resilience and building resilience against hybrid warfare, and a critical part of that is the cyber security of government critical infrastructure.

Our resilience depends on the cohesion of our democratic institutions, their legitimacy, the quality of democracy, and our fundamental values.

In the end, while technical or material aspects of resilience are important, its moral dimension will be decisive. I have in mind the cohesion of our societies and our democratic institutions—the legitimacy, the quality of democracy, coherence of the society, solidarity among citizens and their loyalty to the state and its fundamental values. Daesh, Moscow, or some other actor cannot beat us, the West, in a direct way, militarily. Thus, they will keep seeking to exploit our own vulnerabilities, weaknesses and frictions in order to deepen them, to drive wedges dividing us, to compromise our institutions and undermine our alliances, be it NATO or the EU. This means that we need to start with a frank and honest assessment of our own vulnerabilities and of our own weaknesses in order to know ourselves, be resilient and able to stay calm, and carry on despite whatever pressures there may be.

Cybersecurity, Trust and Resilience

Mr. Anthony Grieco
Chief Trust Strategy Officer, Cisco

Today, I will talk about cybersecurity, trust and resilience. I have been at Cisco for about twenty years now and seventeen of those years have been spent dealing with cybersecurity in some shape or form. A lot of my time has been spent with public sector customers and agencies around the globe, trying to get a deep feeling for how public sectors are approaching cyber security. At Cisco, we have been working with them to build strategies for resilience in this environment. These working relationships that focus on cybersecurity and resilience are critical if we are to achieve a unified view of what is going on.

Having engaged with many of the countries represented here today, we believe that some foundational commonalities are worth pointing out. We definitely see similar challenges across those countries and these challenges have become rallying points for the problems we are trying to solve. In particular, there is a real struggle to keep up with policy and defense in the new digital area. Every country is striving to keep building innovation and technology leadership. Conrad Prince mentioned the drive to create innovative technology startups inside the U.K. and every country that we engaged with is seeking that same set of capabilities. Every country is also struggling to provide protection for their critical infrastructure. In addition, all are grappling with how interconnected the world is today and what that means from a cyber security perspective.

The common thread across countries is on how they deliver mission capabilities in ways that leverage technology while providing the assurance necessary for the mission.

The common thread that we see across all these countries is how they deliver mission capabilities, particularly in the departments of defense and ministries of defense, to defend their countries in ways that leverage commercial technology but do so in a way that provides the assurance necessary for the missions. My point is that we are all facing collective challenges and if we want to build cyber resilience into what we are doing, none of us can do it by ourselves. Fundamentally, when we think about the notion of resilience, whether we are talking about resilience from a national disaster in preparing a community for it, or about cyber resilience, no one silo will be able to do it by itself. Resilience really thrives on the idea of a connected community and is critical to help flesh out how the private and public sectors can come together to think about cyber security and cyber resilience together.

Let me share with you how we engage with our customers around the globe and how we think about cyber security holistically in order to address the idea of resilience. I will give some examples of places where we have instituted strategies to think about cyber security in the right way or, at least, start down that path. A fundamental premise is that the world is going digital. This is an easy statement to make, but it is also an opportunity to understand what it means at a deeper level. Our customers are businesses and service providers around the world. For the past ten to fifteen years, all have been focused on using technology primarily for back office operations—they are doing HR with IT, filling orders with IT, doing personal management and all of those things that run the back office of the business with IT. This notion of a digital era is really critical because every one of those businesses are now looking at how to leverage technology in a way that it is built into the products and services that they are delivering to the market, that is, they are moving technology and its use out of the back office to help run their business instead of technology only being part of their business and part of what they offer to the market.

That fundamental transition creates a number of different opportunities. It creates opportunities for economic growth, for efficiencies, for jobs, and for global competitiveness, but it also creates opportunities for cyber risk, whether it be malicious attacks by criminals or malicious attacks by nation-states. We recently surveyed the leaders of a thousand global businesses across a variety of sectors. Eighty percent of these leaders were actively transforming their business by taking IT out of the back office and moving it to the delivery of their products and services. Unfortunately, forty percent of them had to stop this major digitization because of cyber security concerns. They had not factored in cyber security when planning to deliver these capabilities. It meant that, as a result, they were unable to deliver the economic benefits to their company. This has to change. For us to stay competitive globally, Cisco and all the companies that we serve have to think about cyber security proactively so that we are not bound and stopped in our efforts to digitize our businesses. Ultimately, strong economies are a part of the hallmarks of democracies. Providing cyber resilience is not just to ensure better defense. Cyber resilience is the idea of building security in early. From a democratic perspective, this is fundamental to economic growth and economic growth in turn generates additional stability.

Cyber resilience is the idea of building security in early.

It is important to note that no one is immune. Every industry like banking, health care, all of them, are suffering from the same sets of challenges. Our solution to that is simple. We must find the right ways to provide these businesses with incentives to build security in at the beginning of what they are doing. We must think about how to build security, trust, data protection of privacy, into the design, the development, the manufacture, the sale and the delivery of the service throughout the life cycle. We must also strive for ways to provide evidence that these things have occurred because, by providing that evidence, we can get to the notion of explicit trust. Explicit trust is an essential component of the conversation because it gives us evidence as to why we can trust what we are doing. Building this notion into the very beginning of the design and development of the products and services we are offering is critical for delivering on that explicit trust vision. If we fail do this, we will be faced with repeated scenarios where our customers, our governments, our public sectors will be unable to continue to innovate and deliver on the services that digital capabilities make possible. Ultimately, they will have to stop their mission, restart it, and rethink what they are doing because they have not built in security from the very beginning.

A secure development life cycle is essential to providing built-in security.

We do not have that luxury anymore. Today, we are at a point where a fundamental change must take place. As we start down this path as an industry, let me give you an example of where we are. One of the ways Cisco thinks about building security into our company products is through a secure development life cycle. This means looking holistically at how to think about security in the supply chain, how to think about it during development, how to think about it during the manufacturing, design and delivery, and throughout the entire life cycle of the products and services we are offering. That secure development life cycle is essential to providing built-in security. It includes everything from modeling what the threats might be to managing risks in the supply chain to doing proactive penetration testing as part of the product delivery. The success of this holistic method is measured in real tangible metrics. Ten years ago, before we instituted that secure development life cycle, three quarters of the vulnerabilities were found in Cisco products because external researchers came to us and reported them to us. Today, we find three quarters of the vulnerabilities inside our own development process and through our quality checks before the product ships. Building that capability into the design and development process has totally inverted that ratio.

Is it where it needs to be? Absolutely not. Is it a step in the right direction? Absolutely. That still leaves twenty-five percent of those vulnerabilities undiscovered, which is a chance for us to start thinking about public private partnerships and how public and private entities can get together to think about this. Chris Painter mentioned yesterday the Vulnerability Equities Process (VEP) that has been recently revised in the United States. This is a chance for us to have a robust conversation between private industry and public entities. Cisco was encouraged by the developments concerning additional transparency and accountability described in the existing VEP in which the government will evaluate whether to disclose vulnerabilities it has obtained or discovered and notify the vendors so that the vendors can fix them. I think there is an opportunity to take the lead on this and to continue building this capability throughout the countries that are involved in this forum today. While vulnerabilities are a very complex topic, Cisco believes that it is critical for all of us to know about them as soon as anyone, government, private or other entities, discover them so that they can be fixed. That need is being driven because there is such an interconnected dependency today between technology systems. You need to look no further than the Mirai botnet that took down a DNS server and infected so many of the services we all use, from social media to many others. When you look at the total internet ecosystem today, it is impossible to map those interdependencies that are triggered by vulnerabilities. So, when we think about the vulnerability equity process and the transparency to vendors, it is really important that we get on the same page and continue to push forward.

Cisco believes it is critical to know about vulnerabilities as soon as anyone discovers them so that they can be fixed.

We need "pervasive security" where trust, data protection and privacy are built into the fabric of the business and organizations.

We have seen the critical role that technology plays and how we should build security in from the beginning, but another critical challenge that we see across our customer base is not technology based at all, it is actually cultural. When it comes to cyber security today, one of the biggest challenges is changing this culture of cyber security. Many of you have been involved in the cyber security space for a long time. I have been involved in it for quite some time myself and you know that cyber security historically has been an "expert" conversation, i.e., the only people who talk about cyber security are cyber security experts. Historically, the idea is that there is a security organization with a group of security experts who are responsible for security. No one else needs to worry about cyber security because this group is responsible for it. Yet as we look at the state of things today, there is no way that this strategy of execution from a cultural perspective will get us where we need to be from a security perspective. What we need is what we call pervasive security. It is thinking that trust, data protection and privacy cannot be built by a group of security experts, but they have to be built instead into the fabric of the business and organizations that we all run. In this cyber security perspective, it is only when we will get to that way of thinking that we will be able to look at cyber security holistically and help everyone understand their role in it.

At Cisco, we embarked on this journey a number of years ago and we developed a high-level framework that is useful when considering how to make the shift from a cultural to a pervasive security approach. It has four main elements:

- *People in the organization.* We must think about the people who are part of our organizations and, regardless of their functions, assess their awareness of cyber security. Yesterday, Xavier Carton spoke about how he tested his employees on whether or not they would click on unknown links. These sorts of activities are essential when we seek to help security people and everyone else in the organization understand that they have a critical role to play from a cyber security perspective.
- *Integrating security into the corporate development process.* All our organizations operate with process. I have a procurement process, a deployment process, an engineering process for building products. All those provide opportunities for us to integrate security into the processes. So, when we think about cyber security, integrating security into existing processes becomes another critical component.
- *Technology.* Technology is a third element that we do think a lot about—how to stay up-to-date, how to continue to innovate, how to keep investing in cyber security to make sure that we are prepared, to make sure that the products that we are delivering are ready for the threats of today and those of tomorrow.
- *Policy.* How does policy, which has been the subject of a number of conversations yesterday, supports the notion of pervasive cyber security in the organizations or corporations that we run?

In the pervasive approach, there are four useful domains to consider: People in the organization, the Integration of security into the corporate process, technology and policy.

For us, these four elements have been critical to transforming our own company and they can be useful for broader organizations as well. What is critical is not to think about anyone of these elements in a silo. If we write a policy that says that we must treat customers' data well and be ready for the EU General Data Protection Regulation (GDPR), it will be insufficient unless we have trained employees on what customer data is. There is definitely a training component and we must make sure that we have provided the technology capabilities that will allow the employees to actually implement that policy. In the pervasive security approach, we need to think about all four domains and understand that almost every problem will require multiple other problems to be thought about and solved in the context of the original problem.

Another crucial element to consider when we look at opportunities to build a pervasive security system is how agile all four components are. Their agility, their ability to change, to keep up with where the business and the threats are going is essential. An example of where we collectively need to do better as an industry and as public-sector partners is in the certification and employment of product inside the public sector environments. In particular, we see a lack of agility driving a set of behaviors that, I believe, need to be thought about carefully. We see a private sector's set of bespoke processes for certifying and accrediting products and services that are delivered throughout many of the markets that you all are responsible for. That set of bespoke processes creates a challenge because many of them are driven by a common goal—wanting assurance—but they are driven uniquely on how they are executing against them. Most are driven by people, not automated processes, and most are driven by investment in time and dollars. From a real security return, it would be an investment that you would really struggle to make. Ultimately, we have an opportunity to reflect on how we think about certification in particular and the assurance that comes from them together in a way that is more digitized, more automated, and more real from a security capability perspective.

Forward leaning organizations are taking advantage of this to deliver additional capabilities to the market. One of the best examples is what has happened in the United States in terms of protection of classified data. The U.S. developed a program called Commercial Solutions for Classified Program (CSfC). It was struggling with how to keep protecting classified data as they were transmitted and received so that the protection would be sufficient for the risks they were seeing. As they built larger modern data centers, they saw bandwidth increase more and more with the mission needed and the capabilities from a speed and agility perspective, but the legacy way of accrediting and certifying crypto products in particular became a burden around their neck. They were unable to deliver mission capabilities because of this legacy way of thinking about certifications. Ultimately, they rethought it and created a set of programs that allows them to leverage commercial capabilities in certain risk environments to provide mission capabilities. They rethought how to approach cyber security risks with a holistic perspective and how to build an architecturally pervasive security into their mission. These types of reinvention of how we think about certifying and accrediting will become necessary as technology continues to evolve rapidly and the mission needs that we all have will continue to expand.

The U.S. developed the Commercial Solutions for Classified Program (CSfC) because the legacy way of accrediting and certifying crypto products was a burden.

Cisco products and services block 19.6 billion threats on the internet every day.

Finally, I will give you examples of where we come together with entities to build collective resilience. As a private sector entity, we engage with public sector organizations around the globe. Every conversation we have with their governments is very narrow and focused. It starts with intelligence sharing: "Share intelligence with us, we need cyber security intelligence." Cisco products and services block 19.6 billion threats on the internet every day and the first and only conversation that many governments have with us is about sharing intelligence. This is a great first step but, from our perspective, it is entirely insufficient. We have to think more holistically, more pervasively about how public and private entities come together. What about training? What about best practice-sharing? What about opportunities to share employees across organizational boundaries?

We have partnered with a European state that is under active cyberattack. Their critical infrastructure, private sector business and public-sector entities are constantly being attacked, resulting in power outages, transportation issues and all sorts of financial issues. When we started to engage with them, our first conversation was about shared intelligence. It was a necessary component for evaluating how we could provide them with broad-based protection and help them in time of need. Ultimately, we stepped back and asked them what was really going on. What were the real challenges? What was inhibiting progress from a cyber security perspective? We ended up instituting a pervasive security holistic approach that thinks about how to build resilience into what they are doing. We have training exercises that teach both the SOC engineers that are running and defending active systems and the IT professionals across a broad range of industries, as well as a broad-based general citizen education activity. We talk about best practice-sharing and how we can help accelerate their ability to be resilient in the infrastructure they are building. We also talk about building capabilities where Cisco products and services are being built to help provide better, more resilient cyber security.

We believe that this type of holistic thinking will be very fruitful and, from a public and private perspective, we must challenge one another to identify where and when we can partner. The threats that we are facing have so many common characteristics that we need to look for opportunities to work together. There is no way private industry or anyone of the countries can solve this problem by themselves and I believe that even NATO itself cannot solve it alone. When we will look back in the distant future, we will look at this as an inflection point of how to build security into everything we do early on. We can no longer continue to patch and deliver our systems without thinking about cyber security at the very beginning. We must begin this journey around pervasive security and build security into every organizational component that we have. It is also incumbent upon us to be emissaries and the voice of the conversation with other organizations.

Neither private industry nor any of the countries can solve the cyber problem by themselves. Even NATO cannot solve it alone.

How can private sector industry, and particularly Cisco, partner better from a public-sector perspective?

How can we, private sector industry and particularly Cisco, partner better from a public-sector perspective? Ultimately, I do not know what the private sector's role should be. There was not a lot of conversation on the private sector yesterday, perhaps intentionally or not, but I would like to discuss with you whether the private sector is playing the right role in the direction and policy conversation that we are at. From a tactical perspective, I would like to ask all of you to consider how you could be part of this change, to think about how to do vulnerability disclosure and how to drive that change because it is fundamental to where we are going as a country and as a company. In particular, we need to think about how to do certifications so that we can deliver technological capabilities into the hands of our missions as rapidly as possible.

The Impact of Hybrid Warfare on NATO's Strategic Communications: Implications for the Credibility and Effectiveness of NATO's Future Defense Posture

Dr. Jamie Shea[34]
NATO Deputy Assistant Secretary General for Emerging Security Challenges

The new version of the U.S. National Security Strategy is just on the streets today, and one of the intellectual Inspirations behind that, General H.R. McMaster, is looking at fake news and social media. He has spoken of "new generation warfare." I don't know if it is really new generation though, since warfare has always consisted of identifying and exploiting the weakness of the adversary. Those vulnerabilities have moved from borders and military forces to the functionality of domestic economies and civil societies. Homefront is now the new center of gravity for strategic competition and the things that we are going to be examining today, like fake news, botnets, trolling and aggressive propaganda, work precisely because we live in more fragmented and more polarized societies. The mood is anti-establishment, anti-elite, fed by anger, passion and an acceptance of misinformation voluntarily if it feeds one's emotions and prejudices. We have, if you like, a conjunction of these divisions with the more connected cheap, easier to use universal social media. Our adversaries of course have become more and more skillful at exploiting this political domain.

Homefront is the new center of gravity for strategic competition… because we live in more fragmented and more polarized societies.

In the U.S. elections to which we all are referring, we had numerous examples of this: YouTube videos of police beatings on American streets, internet hoaxes about veterans being mugged on freezing winter nights, stories about the federal government expropriating poor citizens from their land for just a few cents on the dollar, and Muslims being beaten up on the streets of New York. Most of this material, by the way, was not posted by the Russians, but posted by Americans. The skill of Russia or other potential adversaries is not so much in creating these stories in the first place but in finding ways of amplifying their effect by placing advertisements, by stealing content without attribution and leaking to other sites. This is a process that you might call amalgamation—by introducing into the script other fictional characters that can give the stories more scope. It is basically feeding a narrative of anger to certain extremist groups to start or test the terrain, to see if these messages are going to be amplified and find a willing audience. The basis of this is the polarization that we are imposing on ourselves. Jonathan Albright of Columbia has called this "cultural hacking." The battlefield has moved away from some of the more normal strategic competition toward this notion of interfering in our own sense of self and our own sense of culture.

[34] The last time I participated in the workshop, we were all shivering in sub-zero temperatures and I remember that the most priceless object in Paris that day was a spare overcoat. But I am really pleased that the portrait behind us, King Louis XIV, the Roi Soleil, is actually living up to his reputation today and radiating some sun to warm us up. Today he is not saying *l'état, c'est moi*, he is saying *le chauffage, c'est l'état.* I thank the dear monarch for that. I will also notice that since the last time the armor on the walls has been keenly polished, so I will endeavor to give an equally polished presentation today.

What are the Characteristics of This Media Environment?

The criminalization of the practice of journalism. I think Clay Shirky, whom a lot of you will know, is one of the big American experts on social media. He has written a book with a very attractive title, "Here Comes Everybody." It is all about the empowerment of individuals to be part of this global conversation. It is less tolerance for different points of view. It is the disdain for experts and expert opinion characterized by British government Minister Michael Gove who, during the U.K. Brexit referendum campaign, said we have had enough of experts. This is what leadership is saying of journalism—with a willingness to attack any criticism immediately as fake news and as politically motivated, and to actually describe journalists as enemies of the people. This is not something that we just see on the other side of the Atlantic. In an Eastern European NATO member-state last week, we had the government imposing a massive fine on an American owned major TV channel. I could go on and give other examples to the extent that we ourselves in our own society even criminalize the practice of journalism. We do not make it easier on ourselves when we point the finger at Russia or China or the Philippines or others.

There is a willingness by leadership to actually describe journalists as enemies of the people.

There is a more rapid dissemination of information with less ability to check the facts. A media that is operating because of competition and ratings—with less depth and less reliable sourcing and less brand identity. And media culture, it has to be said, is more involved in talking about the news and commenting about the news rather than generating or showing the news. Commentary has become more important than reporting.

Heavily-funded adversary state TV channels are based on the notion that the real news is not the real news.

There is a big investment by state adversaries on TV channels. For example, RT yesterday set up in France, having already established itself in Germany, and in addition to the existing English and Arabic language channels. There will be 150 people and an initial budget of $24 million. These are heavily-funded state TV channels, based on the notion that the real news is not the real news. In fact, the real news is supposedly suppressed by the more conventional media as part of a conspiracy to keep the average citizen in ignorance. "Question more" is the slogan of RT and, of course, these channels are very good at satirizing themselves to give themselves extra credibility. If you were going to the London Underground at this moment, you would see lots of RT posters in a row, saying "we get blamed for everything;" "the weather is bad today, we get blamed for it." "Blame it on us." It is sort of an extreme extrapolation of the sense that RT is the victim being blamed for everything and how can that be fair?

In our culture, we are getting more and more of our news from social media, Not from conventional journalism or even TV. For example, the Pew Research Institute in the United States has done a study. A year ago, in 2016, 50% of Americans were getting their information from TV and 45% from social media. Today, it is now 30% getting their information from TV. Within a year, the change has been very quick with 67% getting their news from social media.

How Can We Respond to this Change in the Media Environment?

Exercises are the first way to respond to changes in the media environment. Exercises are being talked about at this workshop. And one thing that we do need to do in NATO exercises is to actually see how we can deter this kind of propaganda and hybrid operations, without getting into a military battle. What would be effective responses? What would be deterrence? And what is the toolbox we could possibly use to counter this? Since we have been so focused on military security and military defense, we tend to skip over the hybrid side as a sort of foreplay—before we get to the main course—or simply as a preparation before kinetic activities. If you only have a hammer, all problems have to be defined as nails. And I think we need to step back from this and really play hybrid warfare as a conflict in itself. Even if no tanks cross any borders, how do we respond?

Situation awareness is key. We need to be more aware of what is being done to us and act much faster. In spotting fake news and orchestrated attacks, we must be using better intelligence, better sensors, and algorithms that can spot fake news much faster. We need to establish the credibility of facts much faster. I think we got off to a better start at NATO with the way we handled the ZAPAD 17 exercise. Much more intensive intelligence-gathering allowed us to counter much faster the Russian narrative and to counter the fake figures about numbers of participants that were put out by Moscow.

Attribution of facts. We need to be faster and I know that Jānis Sārts will talk about this concerning trolling and sourcing where the stories are coming from. We need to develop a more credible narrative on our side that appeals to the social media generation, which is interested in stories and narratives of human interest rather than in abstract arguments and facts. In the cyber area, just a moment ago, Anthony Grieco was talking about this kind of echo system. It is also the same when dealing with the area of fake news and propaganda.

Social media companies need to do more research, hire more fact-checkers, and ban abusers.

Social media needs to be more engaged. Obviously, the role of the social media companies is coming to light. They need to do more research. They need to hire more fact-checkers, and they are doing it. They need to ban abusers, like Twitter has done with many Russian advertisements after the elections and not accept any advertisements from anonymous or unverified sources. They need to identify fake news faster and to work with law enforcement. It seems that they need to see that the problem is not simply incendiary or violent language as in traditional jihadist videos: the problem is anything that is not accurate even if it is not violent or incendiary.

Our own engagement with the social media companies, private citizens and NGOs. The trouble at the moment is that Russia can do propaganda on social platforms perfectly legitimately within the rules that the social media companies have established. We need more engagement with them. We need to invest with our own government and when we give RT or Sputnik a license to operate in NATO countries, we need to demand equal access for Voice of America, Radio Free Europe, BBC World Service, or CNN International in their markets. Finally, we need to create effective networks with private citizens and NGOs because identifying and countering the fake news comes more and more from citizen engagement.

When we give RT or Sputnik a license to operate in NATO countries, we need to demand equal access for Voice of America, the BBC, and our other media.

There are some excellent initiatives—in the United States, the Atlantic Council has a digital forensic lab and you are familiar with effective NGOs like “StopFake” and the “Baltic Elves, which has mobilized citizens in Latvia, that can also contribute to this effort. Someone said earlier “Even NATO cannot solve this problem alone,” a bit of an insult (!), but actually it is true. We need to establish a more credible network, not just with international organizations like the EU, but also involve people by demanding that the internet should be something in which the citizens play a greater role for checking and policing.

Can Digital Technologies Kill Democracy?

Mr. Jānis Sārts

Director, NATO Strategic Communications (StratCom) Center of Excellence

Let me begin with my view of cyberspace. In cyber security workshops like this one, people typically concentrate on the networks, their hardware, and their software. This leaves out a significant piece, which is the place of humans in cyberspace. Their minds increasingly interpret the world with the information that is processed through the digital internet and the online environment. Most of the activity there is geared towards influencing the cognitive space of those humans, which is the ultimate target. Russians, who have been cited frequently at this workshop, typically see the cognitive space of humans as the main way for them to achieve influence. As Jamie Shea reminded me, we increasingly get our news digitally. In the U.K., more than 80% of the people get their information digitally and more than 60% get their information on social media. What does that mean? It means that the information flow which existed as recently as ten years ago has basically collapsed.

Most of the cyberspace activity is geared towards influencing the cognitive space of humans.

The dissemination of information depends on how big the network is. In a number of countries, some of the large click-bait businesses have bigger networks than those of the traditional media. Nobody minds if they share jokes, talk about cars, women, or cat pictures. But when the click-bait starts to introduce political content, it has a profound and significant effect because, in a network sense, it feels like everybody is sharing the same opinion and story. In one case, because a click-bait business was bought by a political proxy, the popularity and ratings of the government dropped by five percent points in a two-week period. This is the kind of effect you can achieve because the assumption is that the news comes from humans. Since many of you are probably on some social media, I would ask you this question: “How many bot friends or follow requests do you get per month?” If you respond, "None," be careful because research indicates that, for both Facebook and Twitter, the number of bot accounts in these two networks is between 10% and 19%.

Research indicates that, for Facebook and Twitter, the number of bot accounts is between 10% and 19%.

I will share some of our recent research on Twitter in which the terms NATO Estonia, NATO Latvia, NATO Lithuania, NATO Poland, appeared in the Russian and English languages. In the Russian language, the robotic presence with two of these mentions was 70% and the content they generated was 85% of the total. That was at the time when social media companies were under intense pressure from the U.S. Senate. Why does this matter? Because of lack of trust. Who do people trust? Do they trust governments? No. Do they trust the media? Not necessarily. But they trust their next-door neighbour. If you can make a robot in a social media context appear to be your next-door neighbour sharing information, the trust level will be higher than for any governmental player.

These methods are pretty commonly used and there is an effect of certification by abundance. Since everybody seems to share the same point of view, you are kind of pulled towards the centre. A few months ago, one of the botnets that we monitor in our systems suddenly changed and started talking about Catalonia. One can wonder what that was for? Clearly, bots have an effect.

Data sets can help understand behavioral patterns to make predictions and operate behavioral changes.

Concerning other big data, there have been references to Cambridge Analytica. I do not think that they had the effect it is claimed they had nor the skills and methodology for that. But if you think about all the companies that are collecting big data on consumers—Oracle for example, has data for two billion users—and look at what kind of data they have on individuals, I would say that, 30 years ago, intelligence services were collecting these same kinds of data sets for their governments. Today, these data sets are abundantly available. What can they be used for? They can help understand behavioral patterns to the point of being able to make predictions. They can also be used to understand what buttons can be pushed to operate specific behavioural changes.

Videos able to alter reality already exist and are becoming cheaper to make.

Typically, this kind of knowledge exists within a family. My wife, for example, knows all my data, but she has spent 20 years with me. However, an increasing number of people outside my family now has access to these same data. When this is extended to the political context and bots can be used to disseminate, to amplify or to mute voices, this can have a fundamental effect on societies. In addition, the large amount of information that can be gained through social media and online makes it possible to alter the reality. Videos able to alter reality already exist and are becoming cheaper to make as augmented reality technologies are increasingly coming in. This information flow contributes to the information bubble. It turns our echo chambers into belief systems, which further amplifies their effects. Ultimately, many of these things will be even more amplified by the growing ability of effective machine learning or artificial intelligence.

The bots started with Twitter. Right now, when I see a typical bot, I know that beautiful, young females will not befriend or follow me because I am nice. I know that there is an underlying reason for wanting to follow me and, typically, it is because it is so good looking. Otherwise, I would have no means to actually tell a bot from a real human. And there are more things like that in the future.

Let me propose some solutions:

- The first one concerns education. Our citizens have to be educated so that they can be depended upon for democratic decisions such as who to elect, on what grounds to elect someone etc.
- Second, we need digital transparency. Facebook finally gave up its data on what happened during the U.S. elections. For a number of governments that are now facing elections, this is a difficult discussion. Is it okay if somebody buys Facebook services and you do not even know it? I am not sure about that when there is no possibility of legally saying, "That is not okay."
- Third, regulation is a growing topic. Right now, we are in an online environment which is like the Wild West, especially in an election period. In my view, there should be a balance with taking some regulatory steps because, at present, you can do whatever you want. You will not be caught unless it happens two or three years down the road, and then it does not really matter anymore. You have obtained your effect already.

- *There is a need to balance with a buy-in from the tech companies.* It is not yet there but I hope it will come and there should be more push on this. Governments must have capability development and, more or less, most of them have a good set of capabilities to do cybersecurity but cognitive cyber security is a scarce asset.
- Lastly, we do not build bridges based on fake physics and would not want to walk on a bridge that is built on imaginary physics. Similarly, would we want to build our democratic processes on an information space where facts do not matter? If we did, the bridge might collapse, and we would not trust such a bridge to walk on it.

Prepared for Battle, But Not Prepared for War

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

On December 7, 1941, the Imperial Japanese Navy was brilliantly prepared for the battle that it was about to fight at Pearl Harbor, but not prepared for the war that engulfed it. As was pointed out during this workshop, the velocity, volume, and scope of information—including social media—now allows our adversaries to target the home front directly.

Are future conflicts moving from tanks, troops, and artillery to the minds and mobile devices of citizens?

If the center of gravity of future conflicts is actually moving from the tanks, troops, artillery and command posts to the minds and mobile devices of the citizens of the engaged nations, what kind of a conflict is that? And how do things like F-35s, Eurofighters, tanks and artillery contribute to our readiness to fight that battle?

I had originally intended to talk about several things drawn from one of my recent articles called "Cognitive Emotional Conflict." The point here about cognitive conflict is really important, since a lot of people spent time convincing me that "cognitive" really refers to rational thought. In point of fact, a lot of what we are talking about here is very, very emotional and that may depend on a different set of buttons that your opponents can push on! So, I think we should think in terms of "cognitive emotional."

As was mentioned, however, the U.S. National Security Strategy was released yesterday, in fact at 8:00 PM last night our time. After taking a look at it, I thought I would point out some of the things in that strategy that may apply to what we are talking about today.

The strategy highlights threats from countries that it refers to as "revisionist powers," which means China and Russia. The way they phrase the threat from revisionist powers is, "To use technology propaganda and coercion to shape a world antithetical to our interests and values." The second group of threats is regional dictators, who spread terror, threaten their neighbors, and pursue weapons of mass destruction. The third threat is Jihadist terrorists who foment hatred and promote violence, and so on and so forth. The strategy also addresses the trans-national criminal organizations. Those are the main threats: the revisionist powers, the regional dictators, the terrorists and criminal gangs.

The U.S. National Security Strategy sees the main threats as: "revisionist powers," regional dictators, terrorists and criminal gangs.

It says that America will use all terms of statecraft—diplomatic, information, military and economic (DIME)—to protect our interests. Also, we will strengthen our capabilities across numerous domains, including space and cyber. Information in this is given high priority: "Data, like energy, will shape U.S. economic prosperity and future strategic positions…The ability to harness the power of data is fundamental to the continuing growth of the economy, prevailing against hostile ideologies, building and deploying the most effective military."

There is also a very interesting section on "Promoting American resilience." The term "resilience" is used quite often in the document. The basic point is that democracy is only as resilient as its people. The strategy calls attention to actors, presumably Russia or China, who are undermining the legitimacy of democracies. It says the American public and private sectors must recognize this and work together to defend our way of life.

With Russia undermining the legitimacy of democracies, public and private sectors must work together to defend our way of life.

While both Russia and China are cited, the concern with China is mainly economic. Significantly, the new strategy document does not talk about a new way of warfare, even though General McMaster has been publicly cited as being concerned about it. But the document does talk about modernized forms of subversive tactics and information operations as part of offensive cyber efforts, attributed to Russia, in order to influence public opinion across the globe.

As to new tools, the strategy document discusses the possible attempt of strategic attacks against the country without resorting to nuclear weapons in ways that can cripple our economy and the deployment of our military forces. Deterrence is considered as the appropriate response against all of those.

It talks about the country needing to prepare for this kind of competition. There is also an interesting discussion about not viewing the world in binary terms of war and peace but in terms of a continuous competition.

Risks to U.S. national security will grow as competitors integrate information derived from personal and computer sources.

There is a very interesting section in here on information statecraft, which is actually not a term I had heard the U.S. use before. As my colleague Chris Painter pointed out, it sounds more Russian than American. But it says that risks to U.S. national security will grow as competitors integrate information derived from personal and computer sources, which is the same point Janis Sarts made in his presentation. The use of artificial intelligence and machine learning will also expand.

The strategy warns that "Breeches of U.S. commercial and government organizations provide adversaries with data and insights." The point here is that the American private sector has a direct interest in supporting and amplifying voices. So, it is not just Russia that has the ability to do this.

As to responses, the strategy advocates prioritizing the competition, driving effective communications, activating local networks in addition to Voice of America and Radio Liberty and finding more ways to work with local forces to have them tell their stories and their narrative.

It will be important to combine the technology of cyberspace with the messaging of information and psychological operations.

How does this fit together? There are three kinds of information campaigns that one has to be ready to fight. One is in the military sense. It is potentially interesting that just last summer the U.S. designated information as the seventh joint warfare function. We are still working through what that means, but it involves things like combining together the intelligence and the communications CIO (chief information officer) roles. Looking at cyber, it will be important to combine the technology of cyber space with the messaging of information and psychological operations. And this will need to be done more effectively.

The U.S. government needs to be reshaped for cognitive emotional conflict. Basically, it is not just the State and Defense Departments, but the Commerce and Treasury Departments need to be included, too. National resilience must be strengthened, but I think that the government alone is unlikely to resolve this. There is too much distrust of government and too many countervailing views. An example is the rich debate in our democratic society over such things as Apple's refusal to release encryption information to law enforcement.

Two or three billion users of the internet will be from societies that have no sense of the Magna Carta or of the Bill of Rights.

At the Black Hat cyber security conference two years ago, there was a very interesting discussion about the evolution of information on the internet. In the early days, information was considered to be free and hacking was seen as a good and possibly noble. Then there were the debates over encryption and browsers in the ’90s which were eventually resolved in favor of allowing strong encryption to be exported. After 9/11, there was an enormous amount of sharing, with a “responsibility to share.” Right now, there is a regulatory and legislative focus on increasing cyber security. A consideration for the future is that two or three billion users of the internet will be from societies that have no sense of the Magna Carta or of the Bill of Rights.

Journey to the Cloud: Staying Calm Amidst the Turbulence

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

I have some predictions about the future of cybersecurity and technology and would like to share some thoughts on where I think they are going. For almost 40 years now, my career has been in cybersecurity. I started as a U.S. Air Force officer, and, during the Cold War, I was stationed at the National Security Agency where I got some experience. In my view, the cyber security threat continues to grow, and it is certainly greater than it has ever been. This is primarily caused by the cloud and I will explain what I mean.

Used today by every organization, the cloud has become a natural part of our infrastructure.

Cloud services are what every organization— public or private—uses today. Whether it is for webmail, file sharing, or storage, the cloud has become a natural part of our infrastructure. It is a global, highly distributed, massively shared, commercial and government infrastructure, which everyone uses to build practically all applications today. What does this trend, which is well underway, mean? Clearly, the cloud causes problems with respect to cybersecurity, but it also solves some problems, so it is a bit of a balance. I will address first the problems caused by the cloud and second how we can look forward to some solutions.

What are the Challenges Posed by the Cloud in Terms of Cybersecurity?

Let me set this in the context of a recent cyber-attack. The NotPetya attack, which occurred on June 27th of 2017, was a massive attack that primarily targeted the Ukraine. Within a day, it took down huge numbers of systems across the globe. In the Ukraine, practically all organizations—government ministries, banks, utility companies, all massive targets within the Ukraine—were victims.

Targeted at the Ukraine, the NotPetya attack caused enormous global collateral damage.

Interestingly, the attack also caused an enormous amount of collateral damage. For example, Cisco and some of its customers, including a Danish shipping giant, the radiation monitoring at the Chernobyl nuclear plant as well as the Merck multinational pharmaceutical company, were affected. At Merck, not only the IT systems, but also the manufacturing, research, and sales systems were all impacted. According to public data, Merck's reported financial losses based on lost sales during the breach were in excess of $300 million. So, there was a massive direct impact.

Another interesting point here is that the attack on Merck jumped from the IT systems, which were the primary target, to the manufacturing systems. Because they had to shut down the production of a particular vaccine, Merck had to borrow $240 million worth of vaccine from the U.S. Center for Disease Control in order to get the necessary stockpiles of this vaccine. These consequences were quite unpredictable since It all started in the Ukraine and ended up shutting down the manufacturing of critical medical supplies of a multinational company. No industry was immune from the attack, which propagated very rapidly.

NotPetya is a self-propagating worm. The notion of a worm has been around for many years, but in this particular case, it is the idea of something that can move very rapidly from system to system. Another particularity of this attack is that it was called ransomware in the press, but you could not pay a ransom and get your data back. It was clearly intended to be highly destructive.

Three Lessons that We Learned from this Attack concerning the Cloud

No borders. There were no borders to the attack. It was at machine speed and clearly an attack on the supply chain. Every environment—public, private, military, commercial—was exposed. As a side comment, I have heard of many environments—manufacturing environments, governments with classified systems etc., that are claimed to be isolated because they are "air gapped." I do not believe that. In every single example where systems are supposedly truly isolated, even in highly classified environments, there are examples of such attacks. Today, there are no borders in case of an attack.

The attack had no borders, was extremely fast, and based on a compromised application vendor.

The machine speed. The machine speed of the worm's transmission is very troubling. We saw tens of thousands of machines shut down within minutes, a propagation of the attack that was so fast that no human could ever detect or physically stop it.

Supply chain. The attack was based on a compromised application vendor, in this case a Ukrainian tax accounting software package. It was not a classic attack where somebody clicks on a link or downloads a piece of malware. It was an attack on the supply chain where the software vendor was compromised and then, any customer of that accounting package who upgraded to what they thought would maintain security upgraded in fact to a malicious system. This means that, even if you had perfectly updated your windows environment and had very good security hygiene, you were still exposed to these attacks. So, this notion of supply chain, I think, is critical. If the same sort of attack had been made against Microsoft, Apple or Facebook, it would have been quite catastrophic.

How Can the Cloud Help? The Way forward

We just saw the problems posed by the cloud and how these distributed systems can cause so much damage. Let's look now at how the cloud can help.

The cloud is a very effective way to collect and disseminate threat data.

Sharing threat data. First, concerning the issue of borders, international standards for threat sharing have come up several times during this Workshop. The cloud is a very effective way to collect and disseminate threat data and we see massive use of it across the world today. Anthony Grieco mentioned earlier that, at Cisco, we have a big threat repository and we work very closely with industries and governments all over the world. As we think about sharing threat data on a global scale, quite a lot of R&D will be needed in areas like better standards to be able to present and share data. One classic challenge is how to trade off the sharing of threat information with privacy. Of course, we need to maintain privacy with respect to individual citizens' data, but we still need to be able to detect the threat.

Direct automated responses. The second issue concerns machine speed. We need to remove more and more humans from the loop and have direct automated responses for these attacks. In order to do that, a lot of analytics will be required to be able to detect these attacks and respond. The challenge here is that the R&D

must be accurate. If this highly automated system makes a mistake, that is a disaster. A false positive can potentially be worse than the attack itself. So, having very accurate analytics is key here.

How can you determine which software vendor or which particular package you can trust?

Trust. The third issue, which concerns the supply chain, is trying to understand whom you trust. What software vendor do you trust? Has what he is providing been tampered with? How can you tell that the particular package you have is the one you expect? The cloud can help here. There are new technologies like blockchain and there may be ways to have open transparent means to prove the source of software. Again, it will be important to foster R&D and international cooperation on the supply chain in order to be able to determine whom you can trust. As a side note, let me say that fake news is a similar issue. Thinking about news content or software content is about trying to deeply understand its source and whether it has been tampered with. Perhaps there is some technology that can address, not only how we can trust applications, but how we can deal with some of our other sources of information. I have not seen much research in this area but technology might be relevant.

In conclusion, there is no question that a move to the cloud is well underway. It does not matter what organization—government or industry—it is clearly the trend, and with this trend, there is an enormous amount of cyber risk. I also believe that there is an enormous potential to leverage the cloud to solve the cyber problems as well.

The Insufficient Collective Consciousness of Cyber Threats to our Societies and Democracy

Mr. Emmanuel Germain

Deputy Director General, ANSSI (French National Cyber Security Agency)

Thank you for welcoming ANSSI at this high-level conference. I would like to quickly introduce ANSSI, which is the French Cyber Security Agency. Then, I will speak about what happened in 2017, which will complement what Bret Hartman said earlier. Finally, I will offer future perspectives.

Introducing ANSSI

As you know, the French model for cybersecurity and cyberdefense clearly separates the offensive parts from the defensive ones. The offensive part is the business of the security services, while ANSSI is in charge of defending the networks of French institutions and our critical infrastructure, our critical operators. We have three missions: prevent, defend, inform.

Defense and Prevention. To defend, which is our core mission, we have an operational center in charge of detecting, assisting, and reacting to a major cyberattack on behalf of our "clients," which are our institutions and the public and private critical operators. Of course, we also work with our European partners and allies since there is no border in cyberspace. Our networks are all interconnected, which obviously means that we must work with our partners on prevention. I would say that increasing prevention represents 80% of the business of our everyday life, because it is about urbanizing, securing, and organizing cyberspace to make this cyberspace safer and more operational for businesses and for all human activities. This is also a long-term investment and we have laboratories, experts, certification processes, and qualification processes. We certify products at the highest level possible to guarantee that they are as safe as they can be, given the knowledge that we have of the modes of action of today's attackers. We also qualify trust service providers.

Today, we consider that the collective consciousness of cyber threats is insufficient.

Information. The third mission is about information and training. Today, we consider that the collective consciousness of cyber threats is insufficient. Since people, authorities, and employers are not sufficiently aware of the threats and vulnerabilities of our networks, the cyber threat is clearly under-evaluated.

- *WannaCry.* The year 2017 was a turning point with the WannaCry attack, which was a ransomware that propagated very rapidly. It emerged in the U.K. and spread quickly to Spain, Europe, and all over the world. Fortunately, we were able, in the end, to collectively stop WannaCry.
- *NotPetya.* The second attack was NotPetya, and, as Bret pointed out, we were hit by collateral damage. We were not targeted since NotPetya only targeted Ukrainian institutions, and this phenomenon was very new. First, it was new because the damage was collateral and because it was a very intense sabotage process. It was an indiscriminate attack and it represented a barometer of dangerousness that was new for us and is probably going to happen again in the future.

- *The French Elections.* The French electoral campaign was also under attack, but without as many consequences as in the US. One of the candidates, who is now our President, was attacked. This means that our democratic processes, the very foundations of our democracy, were under attack. This is also a new source of concern.

With the attack on the French elections, the foundations of our democracy were attacked.

Some Perspectives for the Future

Looking to the future, this kind of attack will occur again. We are preparing for a big attack, and we consider that probably in the coming months or years we could have a region or cities that are totally paralyzed. Our economic sectors could also be out of service with the consequences that you can imagine for people, for all human activities, and probably with casualties. I do not want to be too pessimistic, but we must announce this because this year we have heard some CEOs and authorities within the field say that, after all these attacks, we may have had to pay millions of euros but, at the end of the day, everything is still operational. They feel that they can carry on with the situation. However, cyber is not a handicap—it is a risk, a systemic risk that has to be taken into account at the highest level by boards of directors and other authorities. We think that the collective consciousness of this fact is far from sufficient.

We are preparing for a big attack in which a region or cities could be totally paralyzed.

The second perspective is about urbanizing. It is not about operational business, but legal issues underlie the negotiations with our allies and partners in Europe. As food for thought, I will offer one example: In the U.S., freedom of speech—the 1st Amendment—comes before the 4th Amendment, which is privacy and the right to be secure. In our European legal culture, our priorities are in the opposite order. This has consequences on the way we organize the sharing of personal, private data and this has consequences for our business models. We are not going to change that, because it is too deep in our cultures. This means that we have to build a system smart enough to work with these two cultures. Economic competition in Europe has to take that into account and we are in negotiations with the European Union on this.

In our European culture, data privacy has an even higher priority than freedom of speech.

This situation also has consequences for the development of the cloud. We would like to have a European sovereign cloud, because sovereignty is very important. If we want to have an autonomous strategic capability, we cannot rely on artificial intelligence located in the U.S. or Finland or anywhere else in order to be sure that our data will have a guarantee of protection consistent with our legal culture. This is a fundamental situation that we have to face together.

In conclusion, I will say that our country alone cannot successfully solve all these problems. Success will require a collective action and we consider that the relevant area for cybersecurity is the European continent or, for us, the European Union in relationship with the U.S., the U.K., and all our allies in the world.

Understanding the Threats and Vulnerabilities: Data, Data, Data

Dr. Steve Purser

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

What is ENISA and How Does It Work?

For those who have not heard of ENISA, it is the EU Cyber Security Agency. Created in 2004, it is a regulatory agency, which means that we have a high degree of autonomy. And we do not need to toe the party line, although we work very closely with all the other EU institutions and with the member-states. For instance, ANSSI is a very important partner which is also at the head of our management board. ENISA is all about collaboration, about solving problems together on a European basis. Before getting into the subject of my talk, it is important to explain how ENISA works. My team is only 50 people strong, which is not very large when you consider that the mandate of the agency is a global one. For example, we can touch upon just about any aspect of cyber security as long as we do not stray into the military domain or the home affairs domain. So, we work by leveraging the experience of the member-states and making sure that we use your experience. Every ENISA deliverable is "our" deliverable in the collective sense of the word.

Let me start on my subject by saying that traditional security techniques consist of three things—people, process and technology. All three are very important, and the success of any solution depends on how you put these three components together. This is what we call a control framework. In a traditional world, control frameworks work very well but they have started not to work well at all and this trend will continue. We are at a tipping point in terms of the way things are evolving, and security techniques in tomorrow's world will be drastically different from those that are being used today. It is a problem, but it is not an unsolvable one.

> **Security techniques in tomorrow's world will be drastically different from those**

New Trends Make It Hard to Survive with the Techniques that Kept Us Safe for the Past Decades

Let's start with the cloud, which is an example of a highly distributed architecture. It is an old technology now, even though it is very important. ENISA has more or less moved out of the cloud because the industry is surviving very well on its own and does not need our help, but some issues are still associated with it. On the one hand, the cloud provides a lot of opportunities, but it is also a source of risks. Those risks are not all technological. Most have to do with contracts, SLAs (Service Level Agreements), understanding what people are doing, making sure everyone knows where the control is and exerts the control appropriately.

> **The cloud provides a lot of opportunities, but it is also a source of risks.**

To some extent, the need to have a strong cryptography on the cloud is a bit of a dilemma.

I will give you one example of a technological issue which is unlikely to be solved in the near future and has to do with the scalability on demand of the cloud. The idea is that, if you need an extra machine tomorrow, you can dial up your supplier and you have the processing power. Cryptography does not work like that. You need to distribute keys, which is a hard problem, and normally use out-of-band methods. The process is very clunky—it is slow and not agile, and it takes a lot of time. Of course, this is what real security is all about. It is taking due care to make sure that the system is really secure. So, to some extent, the need to have a strong cryptography on the cloud is a bit of a dilemma. You can pre-configure a system with keys but then you will not really have scalability on demand, because you will probably be paying for that reservation of keys. This is an example of a technical constraint.

Another example is the Internet of Things (IoT), which is a real dilemma. It is not a technology of tomorrow, it is today's technology and it is going into businesses and homes as we speak. It has three characteristics: massive scalability, short time to market and, at least as far as consumer electronics is concerned, low cost. Those three things give us a number of problems.

Traditional processes will not scale to IoT. There are too many devices. One expert predicts 20 billion devices by 2020, which is huge. As I mentioned earlier, the time constraints are extremely demanding and how much do you want to pay to secure a light bulb? Probably not a lot. Even if you have a device which is more intelligent, like a thermometer, and if it costs you €50 and it is manufactured for €20, how well can you protect the cryptographic keys? Not very well. We pay hundreds of thousands of euros for this in the bank. Then, who is going to run the Public Key Infrastructure (PKI) for 20 billion devices? These are definitely big problems and issues. Again, I am not saying that we cannot solve them, but we need to change our way of thinking. Personally, I think that architectural security would be very important for the future in IoT but, even once all this is resolved, who is going to administer the light bulb that connects to the fridge and curtains at home? We certainly have better things to do with our time. These are the sorts of things that we need to take care of.

We will have to rebalance what I would call the opportunity/risk equation.

I will also mention that, according to studies we have done, today's cars have about a hundred million lines of code. Given the time constraints and the fact that cars are assembled by a number of people, there is a complex supply chain. Where is this code coming from? Almost certainly, it has been downloaded from shareable sites with very little controls on them. This leads me to what people call Industry 4.0.[35] Industry 4.0 is an old term, but it is being used today to describe the fact that we need to re-engineer core processes to take care of a world that will be vastly different tomorrow from what it was yesterday. I think an essential part of this Industry 4.0 is that we will have to rebalance what I would call the opportunity/risk equation. We cannot possibly go on accepting or expecting the same kind of security/risk trade-off that we get for a mainframe, a mid-range or a PC on one of these objects. It doesn't make any sense. We need to think differently. New ideas, like lightweight certification, labelling, etc., are coming out, but the trouble is that security people do not like un-ticking the boxes. So, what I have seen so far is still not as light as it needs to be.

[35] Industry 4.0 is commonly referred to as the fourth industrial revolution.

Data, very quickly, is key to everything but there are problems there too. Most attackers are looking for data and data breaches are often identified a long time after the data has been stolen and is out there. How do we handle this need for accountability? Companies should only be collecting and using the data they really need, and users should be careful of how they use data.

Some key concepts are going to change: Safety and security are not necessarily the same thing.

And then I will make a very last comment. Some key concepts are going to change. For instance, safety and security are not necessarily the same thing. Let me illustrate that graphically. If you remember the Germanwings Flight 9525 air crash, the pilot used a security feature to crash the plane. He used the armoured door of the cockpit to keep the other pilot out and was therefore able to crash the plane. So, with cyber physical systems, safety and security should normally be aligned but not necessarily so. We will have to give a lot more attention to making sure they are compatible.

To summarize, we need to rebalance the opportunity/risk equation. We need to use people, process and technology separately and probably differently in the future. People and process are likely to become more important. It is okay to sub-contract security, as in the cloud, as long as you do it in a sensible way, we know what we are subcontracting, and we have the right level of control. We need to minimise data exposure by not collecting and storing data that are not needed. In any case, we will be forced to do this in Europe as a consequence of the GDPR and privacy regulations. And we should be aware of the fact that old concepts are evolving, and we should not rely on the same idea of security we have had in the past to guide us in the future. We must challenge everything.

Measuring and Reducing the Cyber Risks in Application Software

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

CISQ was formed in 2010 when both the Software Engineering Institute (SEI) at Carnegie Mellon University and the Object Management Group (OMG)[36] were approached by system integrators and asked to develop standards for measuring software attributes such as reliability and security. These attributes frequently appeared in development and outsourcing contracts, yet every customer had a different definition of how they were to be measured. This led SEI and OMG to co-found CISQ with twenty-four companies to create the first round of measurement standards. CISQ has since developed according to OMG's traditional model of a special interest group with several companies sponsoring CISQ's activities[37], but with fee membership for individuals.

CISQ defines software structural quality with 4 key measures—Reliability, Performance Efficiency, Security, and Maintainability.

During a series of international executive workshops, IT executives selected four measures to define the structural quality of software—Reliability, Performance Efficiency, Security, and Maintainability. Experts from the 24 original member companies submitted specifications to OMG's standards approval process. The four quality characteristic measures are now approved as OMG standards. CISQ's four structural quality characteristic measures are based on quantifying violations of good architectural and coding practice within a software system that can be detected through static analysis. Violations are included in each measure only if they are considered severe. Vendor contracts and service level agreements can therefore be implemented to automate the identification and quantification of critical vulnerabilities.

The Reliability and Security measures can help significantly reduce cyber risk.

CISQ holds workshops for the IT community and has begun entering these measurement standards to OMG's expedited submission process. These measurement standards will become ISO international standards that will supplement the ISO/IEC 25000 series of standards by specifying measures of internal quality at the source code level. If we look more closely at the four measures of structural quality, two of them—Performance Efficiency and Maintainability—are dealing with costs while the other two—Reliability and Security—are dealing with risk. This is why CISQ standards matter in the discussions we are holding at this workshop. Cyber security has to be managed at different levels—human, infrastructure, and the last (or first) rampart to protect data and ensure continuity of service is the application software resilience.

[36] The *Object Management Group* (*OMG*) is an international, open membership, not-for-profit technology standards consortium.

[37] Current sponsors are Accenture, Cognizant, Booz Allen, Huawei, Synopsys, and CAST.

The Security measure effort was led by Bob Martin who oversees the Common Weakness Enumeration Repository (CWE)[38] maintained by the MITRE Corporation. This repository contains over 800 weaknesses that hackers exploit to gain unauthorized entry. Periodically, the assurance community determines the Top 25 weaknesses, and they become the basis for the CWE/Sans Institute Top 25 Most Dangerous Security Errors[39] and the OWASP Top 10 Vulnerabilities[40]. Of these top 25 weaknesses, 22 can be detected through static analysis of the source code. These 22, listed in numerical order by their CWE identifiers, became the basis for the CISQ measure. Among the most exploited weaknesses are the perennial favorites: SQL injection, cross-site scripting, and buffer overflows. We have known about SQL injection since the late 1990s. How can this weakness continue to be a common entry for hackers? Too many IT organizations have failed to cleanse their systems of obvious weaknesses.

MITRE's repository identifies 800 weaknesses that hackers exploit to gain unauthorized entry.

Measuring the structural quality of a modern application is tricky and needs to be analyzed at three levels. At the Code Unit level, components are analyzed to ensure good code hygiene. At the Technology Level, components written in the same language are integrated, requiring analysis of a thicket of components across an application layer. At the System Level, different technology layers are integrated into the application system. The complexity of these multi-layer, multi-language systems exceeds the capability of any single individual or team. Consequently, developers make assumptions, some incorrect, about how components at different levels will interact. Operational fiascos frequently result from unintended interactions.

The continuing stream of multi-million-dollar failures is increasing the demand for certifying software.

The continuing stream of multi-million-dollar failures is causing an increased demand for certifying software. Although CISQ will not provide a certification service, it provides an assessment process to endorse that a technology can detect the weaknesses that comprise the CISQ Quality Characteristic measures. Vendors using CISQ-endorsed technologies can certify the level of quality in a software application. These certifications do not guarantee incident-free performance; rather, they attest the level of quality in the software, reported in sigma levels, with an option to report defect densities. The vendors must use people who have been trained in the technology and the CISQ weaknesses to perform analyses and deliver certification results. CISQ has announced a program for evaluating the compliance of vendor technologies. It hosts outreach events, influences policy, and briefs analysts and the media on software quality. It has submitted position papers and requests for information regarding federal policy from several U.S. government agencies such as NIST, DoD, Federal Reserve Board and the SEC. Finally, it also hosts the Cyber Resilience Summit in Washington, DC to influence the cybersecurity and resilience of mission-critical applications.

[38] CWE™ is a community-developed list of *common* software security *weaknesses*. It serves as a *common* language, a measuring stick for software security tools, and as a baseline for *weakness* identification, mitigation, and prevention efforts.

[39] The *Top 25* Most Dangerous Programming Errors are found in government and industry software, and if programmers can be trained not to write them in, cyber security could improve.

[40] OWASP (Open Web Application Security Project) is an organization that provides unbiased and practical, cost-effective information about computer and Internet applications.

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

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

Thank you for the kind invitation to join you for this impressive event, in this equally impressive environment, and for allowing me the opportunity to speak about an issue that is a priority for me and for the Nuclear Threat Initiative **www.nti.org**. Since I have been allocated a limited time, I want to be clear that I have been brutally selective in my choice of words and much that is relevant cannot be covered by these remarks.

What Fundamental Changes Are Necessary?

At the 2008 Rome workshop, I spoke about the need to reform our international institutions. A decade later, this needs for fundamental change persists.

In correspondence preparing for today, Dr. Roger Weissinger-Baylon reminded me that, in 2008, as Secretary of State for Defence, I spoke in Rome at the 25th International Workshop on Global Security. The *Workshop Overview* records that I spoke about the "…need to reform our international institutions in the light of the global challenges we face…" and called for [member states] to "…focus on the transformation of NATO." Apparently, while recognizing NATO's remarkable successes, I stated that I believed that fundamental changes were necessary, that reform should take us towards three clear objectives: well-planned and well-managed operations; an ability to help identify and deliver the capabilities needed to support both current and future operations; and a framework of partnerships that would allow us to work with others who share our interests and can contribute to them, included as part of a more comprehensive approach. Disappointingly, that speech would still be fully relevant today, nearly a decade later. The need for fundamental change persists.

Even setting aside the Financial Crisis and the election of Barrack Obama, 2008 was not a quiet year. But, referring back to the Rome Workshop Overview once again, we see that over two and a half days of workshop discussion, including high level keynote contributions about the contemporary priorities of global security, cyber merited only seven references in the Overview: two, in consecutive sentences, about cyber-attacks by Russia against Georgia's internet infrastructure; four about cyber-crime and one about the economic and social effects of cyber-attacks. In 2017, we gather in Paris over two days to focus solely on cyber. The world has changed, the nature of warfare is changing and with it, global security priorities. It is time governments caught up. This is a timely workshop.

The world has changed, the nature of warfare is changing and with it, global security priorities.

My own journey over the last decade mirrors that change. In 2008, the U.K. National Security Strategy recognised cyber threats, but only in the context of *Global Trends*. The document states:

> “In response to the technological challenges, we are committed to working with international, public, and private sector partners to ensure that our government systems and critical national infrastructure are adequately protected against cyber-attacks. We are also investing…to update our intelligence and law-enforcement capability to meet the challenges of rapidly advancing communications technology. We are committed to maximising the opportunities and benefits of the internet, by protecting the freedom to develop and host new services, while also reducing the scope for terrorists and criminals to exploit those opportunities and freedoms and ensuring that the internet itself is resilient enough to withstand attacks and accidents. Finally, we support international efforts to monitor and protect the safety and security of new technology including the internet and communications networks, and the space assets that are increasingly important for communications. We will continue to explore how new confidence-building and arms control measures might contribute to international security in this area.”

Am I prejudiced, or, a decade later, does this appear somewhat insufficient?

The 2013 Defense Science Board Study on the Resilience of the DoD’s Systems

In 2013, by which time I was living and working in Washington D.C. for the Nuclear Threat Initiative (NTI), the Defense Science Board of the Department of Defense published a study on the resilience of the United States’ systems, which opened my eyes wide. Entitled *Resilient Military Systems and the Advanced Cyber Threat*, the report essentially concluded that the United States could not adequately defend its systems against the offensive capabilities of the highest-level threat actors, and therefore, must rely on deterrence, to prevent major cyber-attacks and intrusions. I recommend that you read the report in full, but today, the abstract of it on the DoD’s Defense Technical Information Center website reads as follows:

The U.S. cannot defend its systems against the capabilities of the highest-level threat actors, and therefore, must rely on deterrence, to prevent major cyber-attacks and intrusions.

> “The United States cannot be confident that our critical Information Technology systems will work under attack from a sophisticated and well-resourced opponent utilizing cyber capabilities in combination with all of their military and intelligence capabilities…While this is also true for others - allies, rivals, and public/private networks, this Task Force strongly believes the DoD needs to take the lead and build an effective response to measurably increase confidence in the IT systems we depend on…and at the same time decrease a would-be attacker's confidence in the effectiveness of their capabilities to compromise DoD systems. We have recommended an approach to do so, and we need to start now! While DoD takes great care to secure the use and operation of the hardware of its weapon systems, these security practices have not kept up with the cyber adversary tactics and capabilities. Further, the same level of resource and attention is not spent on the complex network of information technology (IT) systems that are used to support and operate those weapons or critical cyber capabilities embedded within them… “

I remind you that resilient military systems include nuclear weapon systems! Nuclear weapon systems, like all digital systems, are not immune to cyber–attacks today and the cyber threat is growing. While nuclear weapons systems typically are isolated from the internet, data must be transferred through command and control architectures and weapons and delivery systems are upgraded, creating vulnerabilities when malware could be introduced. In addition, there are a range of external dependencies, such as connections to the electric grid that are outside the control of defence officials. Finally, there is always the possibility that an insider could enable a cybersecurity lapse by either deliberately or inadvertently introducing malware. At the other end of the spectrum, cyber capabilities in their broadest sense may adversely impact survivability. Improvements in remote sensing and autonomy as well as the development of malicious software can create new vulnerabilities in survivable systems such as submarines or mobile missile launchers.

The 2017 Defense Science Board Complementary Report on Cyber Deterrence

Building upon the 2013 study, the Defense Science Board (DSB) published its complementary report on Cyber Deterrence this year and presented it to the Senate Armed Services Committee in a hearing on Cyber Strategy and Policy. The new report reiterates the conclusion that the U.S. cannot adequately defend its systems against the offensive capabilities of the highest-level threat actors, and therefore, must rely on deterrence to prevent major cyber-attacks and intrusions. As the report ranges more widely than just nuclear systems, I am being very selective in my references to this important work.

Russia and China have a significant and growing ability to hold U.S. critical infrastructure at risk via cyber-attack.

However, among the cyber deterrence challenges that the authors of this new study identify are the fact that:

- Major powers—specifically Russia and China—have a significant and growing ability to hold U.S. critical infrastructure at risk via cyber-attack and an increasing potential to also use cyber to thwart U.S. military responses to any such attacks;
- Regional powers—such as Iran and North Korea—have a growing potential to use indigenous or purchased cyber tools to conduct catastrophic attacks on U.S. critical infrastructure.

Thankfully, there have been no catastrophic cyber-attacks on nuclear weapons systems to date, but historical accidents provide some indication of what could happen. In 1980, warning systems showed missiles headed for the United States. Fortunately, in the minutes remaining before the president would have had to order a retaliatory strike, this was determined to be a false alarm caused by a faulty computer chip. In a more recent incident in 2010, 50 nuclear-armed missiles based in Wyoming were offline for nearly an hour due to a computer hardware failure.

In the four years between the Defense Science Board reports, the United States has experienced a number of cyber-attacks but not the "high end" threats that could be conducted by adversaries today. In coming years, all nations will face much more daunting threats of cyber-attacks and costly cyber intrusions as capabilities continue to grow rapidly, placing U.S. national security at unacceptable and growing risk.

To address these challenges, the authors go so far as to recommend that the DoD create a second-strike cyber resilient "Thin Line" element of U.S. military forces to underwrite deterrence of major attacks by major powers. The DoD, they say, must devote urgent and sustained attention to boosting the cyber resilience of select U.S. cyber, nuclear and non-nuclear strike systems and supporting critical infrastructure in order to ensure that the United States can credibly threaten to impose unacceptable costs in response to even the most sophisticated large-scale cyber-attacks.

In order to achieve their fundamental purpose—deterrence—nuclear weapons must be viewed as a credible retaliatory threat capable of inflicting unacceptable damage on a potential adversary. Nuclear weapons must be reliable and work when needed, and they must be safe and secure, so that they can never be used in an accidental, mistaken, or unauthorised manner. To ensure a second-strike capability, they must also be survivable—as must be the nuclear command, control, and communication systems, upon which they rely.

In order to achieve deterrence, nuclear weapons must be capable of inflicting unacceptable damage on a potential adversary.

To assess cyber vulnerabilities of nuclear weapons systems and to develop recommendations to reduce those vulnerabilities and their consequences, NTI convened a high-level Cyber-Nuclear Weapons Study Group. The Study Group focused on vulnerabilities to U.S. nuclear weapons systems, with the expectations that other countries would be examined in a later phase of the project.

Credible threats include spoofing attacks on early warning systems, attacks on communications systems, malicious code insertion, and unauthorized control of a nuclear weapon.

In 2016, the Study Group validated the cyber threat as an issue of concern and began to identify the types of systems and attacks that could threaten nuclear weapons systems with serious consequences. In 2017, the Study Group analysed four plausible scenarios that characterized the highest consequence of cyber threats against nuclear weapons systems. The scenarios described demonstrate the possible consequences of four types of attacks:

- an attack on early warning systems that spoofs an incoming nuclear attack;
- an attack on communication systems, preventing vital information and communication between decision makers and others, with the systems themselves, or with international counterparts;
- the insertion of malicious code, malware, or some flaw into nuclear weapons or delivery vehicles; and
- an unauthorized control of a nuclear weapon through a combined cyber and physical attack.

When considering the scenarios, the Study Group examined how these vulnerabilities and risks might impact strategic stability and nuclear deterrence, considering whether and to what degree certain policy options could mitigate the consequences of a cyber-attack, thereby increasing confidence in nuclear deterrence. In crisis situations—situations where the use of strategic weapons is most likely to be contemplated—deliberations within the Study Group revealed that cyber threats potentially could compromise confidence in the ability to validate information needed to make crucial nuclear decisions, leading to unpredictability and uncertainty and the ability to communicate with and use nuclear weapons when desired, leading to instability.

Deliberations within the Study Group also revealed that cyber threats could potentially compromise the ability to adequately protect nuclear weapons from unauthorized use, leading to increased risk of use.

Using the four scenarios to provide a framework for discussion and debate, NTI, with input from the Study Group, is developing recommendations to reduce the risk that a cyber-attack on nuclear weapons systems could lead to catastrophic consequences. I regret that I am not in a position today to share the precise recommendations with you, but I can tell you that:

- As long as nuclear weapons still form the foundation of deterrence and the cyber threat continues to evolve, significant changes in nuclear weapons policy, posture and structure will be necessary;
- As the DSB 2013 report asserts, technical cybersecurity measures, though critically important, will never provide 100% confidence in the security of nuclear weapon systems; and
- As the cyber threat affects all nuclear-armed states, bilateral or multilateral actions are necessary; other nuclear weapons states must thus address the cyber threats to their nuclear systems as well.

Technical cybersecurity measures will never provide 100% confidence in the security of nuclear weapon systems.

National and military leaders must understand the risk cyber threats can pose to nuclear systems and should exercise strict lines of control over offensive cyber tools that could compromise an adversary's nuclear weapons. Leaders should institute policies that would require the highest-level authorization for any use of offensive cyber weapons on an adversary's nuclear weapons systems (including for intelligence gathering purposes that would necessitate cyber intrusions into critical systems that, in turn, could be discovered and misinterpreted as an attack) to avoid unintended consequences or inadvertently cause or exacerbate a crisis. This latter point is most important.

Conclusion

Any vulnerability in a nuclear weapon system could be potentially catastrophic.

In summary, cyber-based threats target all sectors of society. At the same time, because of the development of a complex techno-military environment, where cyber threats and a growing reliance on computers are transforming the business of national security, governments must worry about cyber-attacks with dire consequences. Unlike attacks on corporate or financial systems, a successful cyber-attack on a nuclear weapon system could have the gravest consequences. Any vulnerability in a nuclear weapon system could be potentially catastrophic. Thankfully, to date, there have been no catastrophic cyber-attacks on nuclear weapons systems, but historical accidents indicate what could happen. As openly advised in both the 2013 and the 2017 reports of the U.S. DoD and Defense Science Board, we should assume that our nuclear weapons systems could be, or already are, compromised and that, no matter how much we invest, technical cybersecurity measures will never again provide 100% confidence in their security.

The threat that military, critical infrastructure and nuclear systems might be targeted or are already laced with malware will worsen mistrust, instability and fear.

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

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

Cyberwarfare as the Fifth Battlespace

Ambassador Michael Zilmer-Johns
Permanent Representative of Denmark to NATO

Introduction

For quite a long time now, cyberspace has been an environment that our societies have depended on, allowing us as individuals to interact, trade, share ideas etc. As our dependency on cyberspace has increased, our vulnerability has also become greater. Whereas both Allies and adversaries alike had more or less covertly exploited cyberspace in the past, in recent years we have witnessed an exponential increase in audacious cyber attacks against both NATO and individual Allies, with grievous consequences for our economies and citizens. The threat is constantly evolving, and we are continuously targeted by persistent campaigns that either aim to destroy, disrupt, or undermine our democracies and economies through subversive influence campaigns.

Nations and international organizations are taking this threat very seriously. Nations are making unprecedented investments in cyber defense and security; western democracies are more explicitly showing that cyberattacks are unacceptable by publicly attributing the attacks, as is the case in my own nation. In Europe, both the EU and NATO have taken up the glove. It could be argued that the EU and NATO have been too slow at realizing the severity of the threats and challenges that the digital age has brought, but the threat has now been recognized and the response has been more agile than we could have hoped for. And we must also constantly bear in mind that nations are and always will be the first responders when it comes to attacks on national structures or entities. That responsibility cannot be delegated or in any way handed over to an international organization.

At NATO and the EU, the cyber threat has now been recognized and the response has been more agile than we could have hoped for.

Before addressing NATO's recognition of cyberspace as a domain, there are three points that are worth recalling, especially since my title refers to the terms "cyberwarfare" and to cyber as a "battlespace."

A cyberattack against an ally can evoke an article 5 response, which may not be a cyberattack.

- NATO has a defensive mandate. As with the other three domains, NATO's responsibility is to protect and defend the Alliance.
- NATO recognizes the application of international law in cyberspace, including human rights law and international humanitarian law. Cyberspace is not an environment in which we are exempt from our obligations to the international society.
- A cyberattack against an ally or allies can evoke an article 5 decision. Like any other possible invocation of article 5, this is ultimately a political decision. However, a cyber attack does not require that a response be made through cyber means. Allies are free to choose any appropriate response to a cyberattack—and this may often not be a cyber attack.

NATO's Recognition of Cyberspace as a Domain

The decision to recognize cyberspace as a domain was made at the Warsaw Summit in 2016 after protracted negotiations. We needed to take a cautious approach since the cyber capabilities of the Alliance, its options for and willingness to share information as well as conducting exercises and training were and remain a sensitive issue. The recognition of cyberspace as a domain was prompted by the evolving threat landscape, and also by the rapid digitalization of our armed forces and command and control systems. In 2014, at the Summit in Wales, the Alliance affirmed that a cyber attack could reach the threshold of an armed attack. That was a monumental recognition of the possible consequences of a cyberattack but it left out the necessary integration into NATO's organization. Since 2014, Allied capabilities in the cyber domain have increased significantly. Set against this background, the decision to recognize cyberspace as a domain was a leap towards ensuring that the Alliance can defend itself in cyberspace as well as it does in the other domains.

Recognizing cyberspace as a domain was a leap towards ensuring that the Alliance can defend itself in cyberspace.

Recognizing cyber as a domain does not imply a militarization of that domain. Like on land, sea and in the air, the domains overwhelmingly host peaceful activities, such as communication and trade. But like the other domains, in response to an increased threat, NATO needs to be able to utilize cyberspace in defense of the Alliance. The decision was followed by an implementation roadmap agreed to at the NATO defense ministers meeting in February of this year. The roadmap has ten lines of effort that each seek to mainstream and integrate cyber in plans, exercises, doctrine, intelligence etc. It is a huge task, but it is absolutely necessary.

NATO's recognition of cyberspace as a domain shifted its mindset from information assurance to mission assurance.

The recognition of cyberspace as a domain has also marked a shift in the mindset of the Alliance from traditional information assurance to mission assurance. The Alliance's missions and operations on the ground depend on cyberspace and will increasingly do so as we digitalize our armed forces while also preparing our ability to operate in a degraded environment. The Alliance itself has an overall mission, and we need to ensure the working of our decision making processes and crisis management. The recognition of cyberspace as a domain is also a recognition of this, and we are working towards assuring the Alliance's missions and operations, as well as ensuring our decision-making processes and crisis management procedures.

Denmark's Cyber Capacities—The Cyber Defence Pledge and Allies' Obligations

It is not only article 5 in the Washington treaty that applies in cyberspace. So does article 3, and it is important to keep in mind that the recognition of cyberspace was one half of the decision to enhance the cyber defense of the Alliance. At Warsaw, Allies also made the Cyber Defense Pledge and thereby formally recognized their obligation to enhance their national cyber defenses, address cyber at the highest level of government and provide appropriate resourcing among others. When it comes to cyber, we are only as strong as our weakest link, and we depend on the capacity of the individual Allies for the defense and security of the Alliance.

My nation, Denmark, is one of the most digitalized nations in the world according to the Digital Economy and Society Index (DESI). We fully recognize that the security of the Alliance depends on individual nations, and we have made significant investments in our national cyber defense and security in recent years. In 2015, the Danish Parliament agreed to develop a Cyber Network Operations Capability. It is now in the final negotiations of a new defense bill that will, among other things, double the budget of the Danish Centre for Cyber Security. A new national Cyber Defense Strategy will also be launched at the beginning of next year. During the negotiations, it has been interesting to observe that cyber defense was an area that automatically received additional funding. Cyber has indeed the attention of the highest levels of government and is an area that has priority for all political parties.

With NATO's enhanced Forward Presence, Denmark has included the possibility of deploying cyber capabilities along the same lines as the deployment of special operation forces. Some Allies have already declared their readiness to contribute cyber effects to the Alliance Operations and Missions, and it is my hope and expectation that Denmark will be in a position to do the same in the near future. As with other domains, it is the Allies that have the capabilities, and the security of the Alliance depends on us to contribute them.

Implications, Challenges and Ways Ahead

That being said, it is not all smooth sailing from here. Implementation is ongoing, and we will see the first comprehensive stock-take at the NATO defense ministers meeting in February. We are conducting a thorough mainstreaming of cyber throughout the Alliance—inclusion of cyber in plans, situational awareness, training and exercises etc.—and there is still a long way to go. In addition, the evolving threat landscape requires that we continuously revisit our plans for implementation and identify new requirements if they present themselves. There is absolutely no resting on our laurels here; if we do, we will lose.

Defensively, cyberspace as a domain is "easy." A proper defense of NATO systems against cyber attacks is our first line of defense and our most efficient way of responding to any threat. And if our systems are compromised we must learn to fight with reduced or non-existent systems the "old way." It is in the interest of any ally to make sure that national systems are as secure as possible, as any national system that is compromised can quickly affect NATO. So, sharing information and exchanging experience with allies and industry are crucial.

Cyberspace weapons can be just as effective as conventional ones but require a very different approach.

Offensively, we are conceptually and practically more challenged. The weapons we use in cyberspace, nationally, can be just as effective as conventional hardware weapons, but cyber weapons, by their very nature, are different and our approach for handling them is therefore very different. The standard NATO approach when it comes to cooperation, procedures and interoperability, does not apply in most cases. All nations are inherently— and rightfully so—quite restrictive in their approach to sharing as wider knowledge of capabilities can compromise years of tireless hacking – to be very honest. Therefore, as I said at the beginning, cyber starts and ends with nations. International organizations can be facilitators but nations are responsible every step of the way.

Unfortunately, sharing brings a wider knowledge of capabilities that can compromise years of tireless hacking.

That is not to downplay NATO's role in cyberspace. NATO has a very important role to play, not least for a small nation like Denmark. Awareness and keeping nations abreast of the requirements and developments are crucial elements of NATO's role. NATO is not stronger than the weakest link in defensive cyber. As cyber defense is being mainstreamed and the destructive cyber capabilities seem to spread beyond state actors, it increases the pressure on NATO members to work even more closely together to make sure that no one is left behind. In the new generation of capability targets we see a useful tool in ensuring that everyone is on the same page.

Can you deter in cyberspace? I would argue yes, but only against state actors. And the first step in deterrence is attribution. Attribution is a powerful political deterrence tool, but it is rarely used and definitely not used by NATO. Shouldn´t it be our first response to any attack to publicly expose an adversary—of course given that reasonable confidence in the perpetrator´s identity can be achieved? Currently, perpetrators of cyber attacks act with seeming public impunity. We must be in a position to act swiftly and take joint action against nations that conduct attacks under the threshold of an armed attack. If we do nothing, we will invite further attacks against ourselves and NATO but, so far, we seem unable to agree on a common response.

Currently, perpetrators of cyberattacks act with seeming impunity, inviting further attacks.

Something that we need to also address is how to benefit from innovation and stay ahead of the technological curve. Nationally, Denmark has recently appointed a Tech Ambassador who will be instrumental in facilitating our conversation with the tech giants and our exploitation of their products, but how do we best approach this in the NATO framework? We could perhaps look into establishing the new Tech Ambassador as NATO's first contact embassy to the tech industry.

NATO’s Digital Endeavor to Transform the Alliance

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

NCIA: The Tech Arm of NATO

It is great to participate in this forum again since the last workshop I attended was in Berlin a long time ago. I am the general manager of the NATO Communications and Information Agency (NCIA). We are NATO's largest single entity with about 3,000 employees, military and civilian, spread out over 30 locations around Europe on three main campuses: one in The Hague, one in Mons, Belgium, and the main one at NATO headquarters. We have staff supporting the military units throughout Europe and in Norfolk and about 250 contractors and staff in Afghanistan who are keeping the networks up and running there. NCIA is an independent agency—we are not part of the international staff and we are not part of the military, the Allied Command Transformation, or the Allied Command Operations. We sit between them, and this puts us in a unique spot and with unique challenges given the current cyber security issues. We operate the networks for both the political and the military side and, in terms of the Washington Treaty, we operate the networks in a balanced way so that article 4 (consultation) and article 5 (collective defense) can be managed by the appropriate authorities. Imagine a scenario in the cybersecurity world where, if a network comes under attack and you want to protect operations in Afghanistan for example, we may need to make a tough decision about which other part of the network needs to be shut down in order to protect the other operations. If it comes to a situation where we have to shut down to allow operations to continue in other parts of the network—our nightmare scenario—how do I make this decision to tell the Secretary General that he cannot have his communications but, on the operation side, the communications do continue? This is the position that I worry about as the general manager.

NCIA is NATO’s largest single entity with 3,000 employees on three main campuses.

We secure NATO’s networks and monitor the cyberattacks, with approximately 500 significant attacks a month.

NCIA is NATO's Tech Geeks and we work on a variety of things from missile defense, to air command and control, to joint Intelligence, Surveillance and Reconnaissance (JISR). It is a wide spectrum of activities, not just networks. But for the networks and for cyber security, we are the design authority: We procure the networks and we have a team of acquisition experts. We operate the consultation and business networks. We secure the networks and we monitor the attacks. We receive approximately 500 significant attacks against NATO on a monthly basis. The NATO Incident Response Center is our tool to monitor those attacks and to defend against them. We provide technical advice to the Nations and we fly away teams when Nations come under a cyberattack and they need support.

Transforming the Alliance into a Digital Enterprise for the Future

We are improving cybersecurity in NATO with two large projects. One is the new NATO headquarters which is a beautiful building surrounded by glass and steel, but it is also a sophisticated and highly complex network. It is taking some time to get up and running as the ambassadors will know, because I have had to brief the North Atlantic Council a few times on the status of that program. On the heels of the new NATO headquarters and its modernization, the second project is a 200 million-euro uplift technology for the commands which will be coming in over the next two years. So, these two, the NATO Headquarters and its modernization, and moving the commands to the cloud, where we will just have three major data centers, is what I call NATO's digital endeavor. It is transforming the business of the Alliance, providing the infrastructure and the tools to really become a digital enterprise for the future.

The new NATO headquarters is a beautiful building, but also a sophisticated, highly complex network.

It was mentioned that the adaptation of the NATO Command Structure (NCS) is before the ambassadors and this is an important development for the agency concerning cyber and particularly a 5th operational domain. When the military started to think about the operational domain, there was a natural gravitation to the thought that “As commander, I have to own everything that is cyber; if I am going to be responsible for an operational domain, I need to own it.” So, in my first 6 months as general manager—I started last July—I have spent a lot of my time working with the commands to convince them that they do not need to take the agency away from me in order to have the situational awareness that they need to do their work. Actually, it is an issue that I worked on with SACEUR, General Scaparrotti, in order to have an understanding of where the lines are between the agency’s responsibilities and those of the commands. According to an agreement my predecessor arranged with SACEUR, the agency will be brought under SACEUR’s command and control in times of crisis. Our U.S. participants might recognize this as a combat support agency type of scenario—in times of war, the agency falls under the commanders. That is what NCIA is in a way in this scenario, but at the left of that crisis situation, a lot of work needs to go on. Passing the command-and-control to SACEUR only kicks-in if there is a decision by the North Atlantic Council that NATO is in a crisis situation. And there is a lot of activity and bad behavior that can go on in the cyber world to the left of a NAC decision.

In times of crisis or war, the agency can be brought under SACEUR’s command and control.

Unlike the Rules of Engagement for armed combat, rules for response to cyber threats do not exist today and they are needed.

For example, think of it in terms of a fighter pilot who has been scrambled to escort a Russian Bear bomber out of NATO airspace or to monitor it as it approaches our airspace. That pilot has clear instructions on how he or she should engage that bomber if it takes a turn one way or another. Those Rules of Engagement do not exist today in the cyber sphere, and that is what I am working on with the military commands and in particular with the Allied Command Operations (ACO) in the coming weeks. This is part of the adaptation of the NATO Command Structure (NCS) which will go before the NAC in February to be sorted out and to make sure that we have a good understanding of it. We had good discussions with SACEUR to secure the agreement that he does not need to own and break up the agency and take everything that is cyber-related. We have an agreement on working through those operations and activities to the left of a NAC-declared crisis.

Finally, I would like to briefly talk about three challenges that we are facing:

1. *Improving our security while helping with the operational domain at the tactical level.* First is the procurement system. We have a procurement system dictated to the agency from the Nations that was designed largely to procure runways and hangars and buy cement. It is not proving useful for software intensive, highly complex, and sophisticated IT systems. A clear example of this is the new NATO headquarters. We followed the rules and we have off-the-shelf technologies, but when you integrate those off-the-shelf technologies is when the trouble comes in. The NAC did not approve having a systems integrator on this project and that really turned out to be a shortcoming. So, we need to change our procurement rules in order to deal with these sophisticated systems.

We need to update our procurement rules in order to deal with today's very sophisticated systems.

2. *We need to enlarge the ecosystem that we are working with.* We mainly work with the largest defense contractors in cyber and IT. We need to expand that to the not-for-profits, the Fraunhofer Institutes, the MITRE Corporations, and others. We even need to expand that ecosystem to academia in order to get more talent and more collaboration with industry and with the expertise that is out there.
3. *We are losing the war on talent.* We cannot compete, even with our tax-free salaries, with our privileges, immunities, and benefits. We are not able to attract to NATO the talent that we need to work with on these technically complex systems. One thing we are doing is looking at our bench strength and we are leaving half of our talent on the bench. We are taking initiatives at the agency to bring more professional women into the agency and the technical activities of NATO. At the NATO's NIAS annual cyber symposium in Mons, we recently held a very successful "women in cybersecurity seminar" which was led by NATO Deputy Secretary General, Rose Gottemoeller. For the approximately 100 professional women who were there, and with Rose's encouragement, we are starting the "association of women of math disruption" as a way to bring professional women together and also to talk about how to engage more women, women engineers and technologists, to solving some of these problems.

We need to attract more talent to deal with our complex systems—especially by bringing more professional women into the agency.

In conclusion, we have some challenges in this fifth operational domain. We are working through the mechanical arrangements to the left of a North Atlantic Council-declared crisis and we are trying to get more talent, expertise and ideas from industry into the battle.

Speeding up International Cooperation in Warfare's Cyber Domain

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

Most of the world, and certainly this audience at the *34th International Workshop on Global Security*, are aware that cyber attacks can potentially cause catastrophic effects on nations and large population centers. Although such attacks have rarely been launched, the capability to unleash broader effects exists, whether conducted in isolation or as part of broader asymmetric warfare strategies. This leads us to consider three areas of cyber warfare that remain unresolved, and consequently have not been brought within accepted international norms and the legal frameworks of war.

After the cold war, the probability of a large-scale conventional (or regular) war declined, and a change to non-regular warfare…followed.

We have seen significant changes over the years in how nations conduct war. Before and during the cold war, conflict was categorized into three types of warfare—domestic insurgency and violent government change, conventional warfare and nuclear warfare. Nuclear warfare has always been seen as almost unimaginable although this assurance of security has been tested recently. After the cold war, the probability of a large-scale conventional (or regular) war declined, and a change to non-regular warfare, commonly called non-conventional warfare, asymmetric warfare, irregular warfare, or hybrid warfare, followed. This change has been particularly obvious when observing the largest economic and military powers. Aside from waging regular warfare against terrorist organizations, these nations are unlikely to engage in regular warfare against each other.

With this focus on developing irregular warfare capabilities, i.e., information operations that include influence operations, cyber warfare and electronic warfare, a new dynamic is taking place between nations that conduct these types of operations. Similar to the dynamic and responsibilities of the traditional nuclear powers, the "cyber powers" present a new challenge that requires further assessment and a need for cyber weapons to operate within an international framework. Rather than grouping all nations into the same category, I suggest that a future international cyber warfare framework should consider arranging nations into three separate groups.

The emergence of "cyber powers" is a new challenge requiring cyber weapons to operate under an international framework.

- ***Nation Actor Group #1***: This group includes a comprehensive superpower (which could be a global power like the United States, Russia or China) and the secondary group of nations that is known or believed to maintain significant offensive cyber capabilities. In this group, the nations are actors in a regular warfare framework and sometimes operate a hybrid war that can extend beyond traditional military targets.
- ***Nation Actor Group #2***: This group consists of countries like Iran or North Korea that are trying to create new capabilities with an asymmetric type of warfare.
- ***Non-state Actor Group #3***: This third group has political, religious, or criminal objectives such as individually motivated hackers, hacker groups, and terrorist or nationalist organizations.

Technical progress has brought changes to the traditional three warfare domains—land, sea and air—which have become five warfare domains by adding the space and cyber domains. These changes have led to the development of the multi-domain battle concept, including exploiting the electromagnetic spectrum. Space, cyberspace, and the electromagnetic spectrum have opened new opportunities for mankind, and new domains for warfare. To be dominant in one domain, however, is not enough to protect a nation, especially since traditional warfare is becoming less likely today.

Space, cyberspace, and the electromagnetic spectrum have opened new domains for warfare.

1. ***Grey Areas.*** There are grey areas in cyber warfare that extend to intent, type of damage, and the threat actors themselves. Cyber weapons are not only used for warfare but they are also used for espionage, criminality, and data access or disruption. They can be launched by nation states, private individuals, ad-hoc groups, companies, and terrorists. Automated programs and bots, controlled by unknown sources, can also launch such attacks. The grey area when a cyber attack is similar to other lethal attacks has led to quite a bit of analysis but little international agreement and movement.

   Of particular note are the Tallinn manuals. The first one, released in 2013, addresses questions on the legal framework and laws of warfare resulting from damaging cyber attacks and mostly concludes that current international standards are sufficient. In Tallinn 2, released earlier this year, attacks that are less damaging are analyzed in terms of legal and self-defense frameworks. Importantly, neither carries the weight of an international agreement as no single nation or international organization has signed up to their conclusions. I suggest that we should acknowledge their existence and use their analysis and conclusions to begin a real international discourse on cyber warfare for nation-states. This would be a start. Non-state actors, who also possess cyber weapons that can be launched against nations, should be reviewed in terms of whether existing legal and criminal frameworks cover their activities sufficiently. The first focus, however, needs to be on nation-state actions.

2. ***Public-Private Responsibilities.*** Just as non-state actors play a role in cyber attacks, non-governmental organizations control most of the critical infrastructure from which such attacks are launched. There are many instances where private industry has discovered and actively shut down malicious attacks passing through their networks. What is their responsibility when one nation is conducting a cyber attack against another nation and where private industry has the capability to stop the attack? Again, there are many scholarly articles that address many aspects of cyber warfare, including the role of private industry. However, at the international level, there is no agreement on what role, if any, such critical infrastructure owners should have in a cyber war. If such norms of behavior were agreed to at the international level, some legal justifications and guidance could exist for private infrastructure owners and operators. Once again, the international community is reluctant to address cyber attacks and cyber warfare comprehensively.

   At the international level, there is no agreement on the role of critical infrastructure owners in a cyber war.

3. ***International Cooperation in Cyber Warfare.*** For traditional warfare, bilateral and multilateral agreements exist between nations. Ad-hoc coalitions are created against threats. These frameworks could extend to cyber warfare, but do they? Without a clear understanding of what raises a cyber

attack to the level of an armed attack, uncertainly exists. Again, we see that agreement on the rules of cyber warfare will help clear up these uncertainties.

Proposal for an International Cyber Watch and Warning Center and an International Cyber Capacity-Building Center

International cooperation does not need to be limited to state-to-state agreements. I propose that two internationally sponsored and recognized capabilities be created for the cyber realm: An International Cyber Watch and Warning Center and an International Cyber Capacity Building Center.

- ***The Watch and Warning Center.*** The purpose of the Watch and Warning Center would be to monitor violations of internationally agreed norms of behavior and work with member states to shut down such violations. Like a Public-Private Partnership, it would have a broad range of monitoring and technical response personnel associated with the Center. It could be a single entity, or more likely, a dispersed entity with multiple hubs.
- ***The Cyber Capability Center.*** It would be focused on protecting critical infrastructure and providing knowledge, expertise, technical assistance, and possibly funding to protect national critical infrastructure.

Both centers could leverage existing attempts by numerous public and privates sector companies that offer such services today. However, the proposed Watch and Warning Centre would perhaps be UN chartered and funded by member states to uphold new international frameworks covering cyber warfare. Capacity building would be focused on nations that do not have the resources or expertise to protect their critical infrastructures.

The international community must begin addressing clearly and legally the rules of warfare for the cyber domain…

What I have proposed here is not new. My main message is a call to action by the international community to begin addressing clearly and legally the rules of warfare for the cyber domain, to reach international agreement on those rules, and to have mechanisms in place to address violations. I will conclude with an observation.

On 27 May, 2016, President Obama visited Hiroshima, Japan, after the G7 summit. This was the first time a sitting U.S. President had visited. In his remarks at this solemn site he said: "Science allows us to communicate across the seas and fly above the clouds, to cure disease and understand the cosmos, but those same discoveries can be turned into ever more efficient killing machines." He added that "The scientific revolution… requires a moral revolution as well" and concluded by saying that we have a shared responsibility for our human history to curb such suffering again. In the cyber domain, we can say the same thing. We have a shared responsibility to avoid the tragedy and destruction that uncontrolled cyber attacks could cause to our civilian populations and way of life.

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

Ms. Flora Garcia, Esq., CISSP, CIPP/US, CIPP/IT, FIP
Senior Privacy and Security Attorney, McAfee

The General Data Protection Regulation will enter into force on May 25, 2018. This 88-page law is causing a great deal of work and consternation across many industries and companies. Let me share my favorite sentence in the document, in Recital 4, which states "The processing of personal data should be designed to serve mankind." It is helpful to keep this quote in mind when thinking about the GDPR, as it catches the tone of the Regulation.

I will give a quick overview of the Regulation and what it means, offer three inherent conflicts in the Regulation and, finally, close with three predictions for the GDPR.

The Overview

The GDPR requires the integration of "Privacy and Security by Design" into the entire data life cycle.

The General Data Protection Regulation is a regulation, a type of European Union law that goes into effect instantly in the Member States of the EU and becomes a pan-European law. This is unlike a directive, which needs to be voted on by each of the countries and incorporated into their national law in a form. There are some areas in which the GDPR allows member countries to make some modifications but, as the goal of the Regulation is to normalize the different EU member state laws that were passed under its predecessor, the Data Protection Directive, those areas are rather narrow. The GDPR has taken many concepts that we have seen in other European laws throughout the years, especially since the earlier Directive was put into place in the 90s but it also expands data protection concepts. For example, the GDPR:

- Requires that products, applications, companies and processes integrate Privacy and Security by Default and by Design into their processing;
- Makes the entire food chain responsible for the security and privacy of the data, throughout the data's life cycle. While the Directive places responsibility on the Data Controller (the entity that directs what happens to the data), with the GDPR, we see compliance responsibilities and protection obligations flowing to the Data Processor (the vendor or storage company, for example, or other third party performing operations on the data at the request of the Controller) as well. These are important concepts to consider in the realm of cloud products and solutions.
- Adds a new pan-European breach notification requirement of notice to the appropriate regulatory authority within 72 hours of becoming aware of the security breach. Breach notification is a new tradition to parts of the EU, something we have in the U.S. in most of our states but has not been universally in place;
- Sets up a regulatory data protection scheme for the Member States and the means for them to work together to resolve conflicts regarding the interpretation of the Regulation;

At last, GDPR imposes a pan-European obligation for breach notifications.

- Normalizes the fine structure for data protection law offenses, formerly left to the Member States and handled widely differently in different jurisdictions. Under the GDPR, these fines can be massive depending on the transgression, potentially reaching 4% of the worldwide revenues of the whole company, not just the arm or subsidiary of the company with whom fault is found or the European subsidiary;
- Finally, the GDPR also offers a great deal of opportunity for confusion and for abuse. There is much fake news about the GDPR and there is even an unofficial website that looks a little too much like the official one of the European Union.

The Conflicts

A first conflict—the cultural differences between Member States. Highlighting these conflicts, I would posit:

Approach to Data Protection. The first conflict to consider within the GDPR is that, despite the many successes of the European Union, cultural differences remain between the Member States in regards to their approach to data protection. Some countries have seen personal data as an important part of growing an Information Technology industry and workforce and are more comfortable with its commercial use. Other countries have already passed internal laws that may be viewed as challenges to the GDPR. The Regulation is tasked with finding common ground where it may be intrinsically difficult to do so. It may be difficult to resolve the core principles of privacy and the protection of data about an individual as a basic human right that is held by that individual with the pressures of an internationalized business oriented and data-friendly IT culture.

Despite GDPR, cultural differences remain among the Member States on their approach to data protection.

The Right to be Forgotten. Another cultural difference may be highlighted in the much-promoted "Right to be Forgotten." This is the case we refer to as Google Spain, where a man who had had property seized in 1998 demanded that Google neither index nor link to and show the Spanish newspaper report of that seizure. In 2014, the European Court of Justice agreed with the man, and said this "delisting" could occur when information appeared "inadequate, irrelevant or no longer relevant, or excessive." Google reports requests for this delisting by nearly 400,000 individuals on 2.4 million URLs between May 30, 2014, and Dec. 31, 2017; it granted 43% of the requests. Two new cases reported from the United Kingdom in April with businessmen convicted of crimes show the complications that can arise. The Guardian reported that the high court judge who heard the cases said one of the businessmen continued to mislead the public, whereas the other had shown remorse. The judge, according to *The Guardian,* also weighed that the case where he found there should be delisting involved conviction related to the invasion of privacy of third parties, rather than wrongdoing related to "consumers, customers or investors." But at what point does this become potential censorship? Will different cultural traditions interpret this concept differently?

Europe First? Next, many of us would posit that there may be an element of "Europe First" in the GDPR, encouraging the growth of European data centers and the movement of data within Europe. Consider, also, that many of the major privacy fines have been levied under the banner of antitrust actions.

Lack of Transparency. If you consider the issue of transparency, the GDPR offers transparency in certain regimes but does not offer it in other regimes, for instance in data breach. In the data breach situation, the breaching party is expected to notify the regulator and the data subject but not the public at large. That is a very different regime from what we have seen in the United States, for example. At the same time, we have often seen consumer fatigue happen in the United States regarding data breaches, and perhaps this less public breach notification will be more successful.

The breaching party must notify the regulator and the data subject but *not* the public at large.

A second conflict—the balance between liberty and security.

There is a conflict between liberty and security for many reasons, but under the GDPR it continues because we still do not have a resolution for what data and information ownership is or truly means. Do I own my data, the data about me? I have a human right to privacy, but do I own my data or is that something that I am able even to trace? I would question the notion that a human right is something of a tangible commodity. In the United States, we still struggle with the concept of privacy and the protection of personal data as any sort of right; we are comfortable with and acknowledge that we regularly allow for the monitoring of activities for discounts in the commercial space. When I want to explain this at McAfee, especially to my colleagues out of Texas, I say that the equivalent holding of the value of my privacy is the ability of my friends in Texas to carry guns and so, the privacy right in the EU is like the right to own guns for many Texans.

Liberty versus security: Privacy in the EU has the same importance as guns to Texans.

In Europe, we see a surveillance society that we have not understood in the U.S. for many years, and which is yet again emphasized by the recent adoption of the CLOUD Act. Yet, we see concerns about the marketing which we are so comfortable with in the United States—this notion that an ad will exactly know what you just bought and will show you something just like it, and that intelligence is a good thing. That conflict remains in the GDPR: One person's behavioral targeting is another person's information security.

People have very different views about data: One person's *behavioral targeting* is another person's *device tracking*.

A third conflict—Bureaucracy versus pragmatic solutions.

Much of the pain and consternation in GDPR readiness may involve updating Data Protection Agreements to include new and specific requirements. If an organization has to go back into every single contract concerning personal data to get specific provisions that are required under the GDPR, is that increasing the security of the data subjects? I posit not. While much of the work companies are undergoing to get ready for the GDPR is substantive, risk-based, and smart, I would challenge regulators everywhere to focus on data protection activities that have direct benefits to the data subject or another direct public policy goal.

Predictions

And now, for three predictions. First, it will probably take 15 years before we really know what data protection under GDPR means and before member states have normalized their laws and come up with ways to define them. Second, the GDPR will be misused and we will see bad actors taking advantage of it, abusing companies that hold data and trying to trick them into doing the wrong thing. Third, the GDPR requires a new approach across many disciplines, across marketing, across data science, across information security, across information technology and across the legal space but we are not as technical, as legal, as aware and as educated as we need to be to take on this challenge, and it will require new ways of thinking about data and security. We need to work together as a team. But the GDPR gives us a framework to talk across our disciplines about personal data and its safeguarding and protection, to talk about how companies handle data, and to talk about how we respect the data subjects who are our ultimate customers.

The Significant Impact of the GDPR on the Private Sector

Ms. Patricia Murphy
Vice President, Southern Europe, McAfee

Responsibility and Liability of the Private Sector under GDPR

In addition to the geopolitical and social aspects of the General Data Protection Regulation (GDPR), the protection of personal data and identity has a significant impact on the private sector concerning two important aspects: One is responsibility and the other is liability.

Today, GDPR requires specific new language in all contracts. For many of us, this requires reopening all contracts that address personal data and it is a significant undertaking in all new transactions. We see new language that is non-standard, and we must negotiate new terms around a law that, in some regards, is lacking in clarity. Let us take the case of audit provisions as an example. How do you audit a cloud provider today? GPDR obliges us to require audits of the processor. For the first time, the processor of data has liability and that liability is both to the data subjects and to the regulators. This is still a shiftable liability between the controller and the processor but how the courts in the member-states will decide to interpret it, when it is not clear in the contract, is up for debate. This will start a new culture of blame like we have seen in the US. It makes risk a part of the pricing strategy. Do you sell cheaper if you take no liability? We are seeing this and do not believe it is in the best interest of security for the companies or the individuals.

For the first time, the processor of data has liability to both the data subjects and the regulators.

GDPR also allows groups of harmed or impacted data subjects to come together to seek restitution for their harm. It looks like the class action law system in the U.S. If there is a breach, does that mean that the system failed, and the breaching party should pay? One of the major goals of GDPR was to normalize and standardize across member states but we still see radically different cultural and legal traditions, and these will take years to move through the courts. In the meantime, we must clearly identify where responsibility lies concerning transparency and insure that we promote privacy and security by design and privacy and security by default.

The 2016 Russian Influence Campaign in the U.S. Presidential Election

Mr. Philip Stupak
Director of Cyber Security and Information Systems, Clark Street Associates

Overview

The fact, if not the scale, of the 2016 Russian influence campaign in the U.S. presidential election was known to the intelligence community who watched it unfold in a slow-motion disaster. Intrinsic weaknesses in western democracies were revealed, especially the susceptibility of large groups to continuous social media propaganda campaigns—but perhaps the most glaring weakness was the inability of national security professionals to react to a slow burning soft attack by a foreign adversary.

Election security against a Russian attack is a national security threat, but it needs a homeland security solution.

Free domestic elections are the foundation of liberal democracies, and if they are to be preserved, then election security must be treated as a national security threat without a national security solution. Instead, what is needed is a homeland security approach to election security.

What Happened?

At its core, the Russian attack on the U.S. blended a series of cyberattacks with a more traditional propaganda campaign run on platforms enabling Russian agents to access an unprecedented number of Americans without a correspondingly significant physical presence within the United States.

The cyberattack portion took two forms. First, there was (and continues to be) extensive probing of election systems. This is not unique to elections as nearly all critical infrastructure is under constant surveillance by foreign adversaries seeking to map and understand network vulnerabilities. Within the election ecosystem, Secretaries of State and local clerks' networks were repeatedly probed—at least two were penetrated—in an attempt to determine access points for a future attack. The U.S. Government has never confirmed whether a such an attack was carried out; however, substantial research has now demonstrated that such an attack is possible. The second cyberattack was a spear phishing campaign run by Fancy Bear (a cyber espionage group also known as Advanced Persistent Threat 28) against the Democratic National Committee (DNC) and the private email of John Podesta, Clinton 2016 campaign chairman.

Russian hacker Fancy Bear's propaganda was seen by over 126 million voters.

The broader propaganda campaign portion used a sophisticated understanding of public division points and amplified those that were detrimental to Clinton. A collection of the targeted ads purchased by Russian influence peddlers was released by the U.S. Senate Select Committee on Intelligence. Additionally, Fancy Bear posted edited and contextless documents to Wikileaks, which suggested nefarious activities. A susceptible segment of the politically unsophisticated public accepted the worst about Clinton and reposted the same to social media, thereby becoming unwitting agents of Fancy

Bear. It is now known that Fancy Bear was a Russian hacker whose propaganda was seen by over 126 million voters.

Just the Beginning

The 2016 Russian attack used simple hacking techniques to supplement an otherwise traditional propaganda campaign. But this is not the end to what is possible by a sophisticated cyber adversary like the Russian Federation.

The 2000 Presidential election between George W. Bush and Al Gore resulted in Florida's electoral votes, and the presidency, being awarded to Bush by a margin of 537 votes out of more than 6 million votes cast. The true outcome of the Florida election remains unknown due to antiquated paper ballots producing an unclear result. To remedy this, Congress passed the Help America Vote Act of 2002 that effectively digitized the U.S. electoral systems.

No one gave much thought to a cyberattack against America's newly digitized election system.

No one gave much thought to a cyberattack against America's newly digitized election system, and those who did were largely relying on a defense in complexity. A typical presidential election has 130 million voters casting ballots in 175,000 precincts, using machines certified by state bodies and procured by local clerks. Yet this is artificial complexity given that U.S. presidential elections are ultimately decided by a handful of swing states. Florida, a perennial swing state, has 6,000 precincts and was decided in 2012 by 13 votes per precinct and 19 votes per precinct in 2016. A state-sponsored hacker gaining access to election networks could easily swing such a modest number of votes without anyone being aware.

It may not take a state-sponsored actor to alter an election. In July 2017, DEFCON, the annual hacker conference in Las Vegas, opened its first Election Village with voting machines from various U.S. jurisdictions. The first machine, an AVS WinVote, fell in 20 minutes to a group of 16-year-old hackers who had never seen an election machine, much less voted! They breached the system by combining a 14-year-old vulnerability with a Google search for the machine's unchangeable default admin password—"abcde"—that allowed remote access to change votes. By the end of DEFCON, every machine had fallen, thus proving that a dedicated adversary could gain the necessary access to swing an election.

The 2017 DEFCON conference proved that a dedicated adversary could swing an election.

An unintended consequence of securing an imperfect paper election against domestic ineptitude has rendered the U.S. election susceptible to direct foreign manipulation.

Improving Defenses: Homeland Security, Not National Security

The combination of the Russian attack and the DEFCON report[41] demonstrated modern democracies' vulnerability to dedicated foreign actors.

[41] Blaze, Matt; Braun, Jake; Hursti, Harri; Hall, Joseph Lorenzo; MacAlpine, Margaret; and Moss, Jeff, "DEFCON 25 Voting Machine Hacking Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure"; DEFCON 25 Security Conference. Las Vegas, Nv. https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf

On December 7, 2017, Cook County Clerk's Office released a report[42] recommending four actions: more money from Congress, more exercises testing vulnerabilities, more information sharing, and more public scrutiny of elections systems. Congress provided $380M to improve state election security. The U.S. Department of Homeland Security has held exercises for local jurisdictions. But increased information sharing and public scrutiny have been withheld as the U.S. continues to take a national security view of election security.

Five years ago, Jane Holl Lute gave the keynote address[43] to the 2012 International Workshop on Global Security in Rome where she cautioned against a national security approach to cybersecurity, "National security is strategic, centralized, and top-driven. Homeland Security is operational, distributed, and bottom-driven. It is not unity of command. It is unity of effort. It is not 'need to know,' it is 'duty to share.'" The same must be true for election security. The failure of the national security's top-down need-to-know approach to election security was just demonstrated. Had Lute's homeland security approach been adopted, then the U.S. would have been in a superior defensive position to counter the 2016 Russian attack.

We must open the election machine code to public scrutiny and share information about attacks with Homeland Security.

The bedrock of Western Civilization is our collective dedication to free and fair elections. An election system protected by a few national security operatives is unable to timely react to a continuous, dispersed attack. Congressional funds for improving security and DHS exercises are the first step in protecting our elections. We must open the election machine code to public scrutiny and share information about attacks with the broader homeland security enterprise. Failure to do so will not only invite more attacks, it will also ensure the success of those attacks. The United States must do better in the upcoming 2018 elections.

[42] Praetz, Noah, "2020 Vision: Election Security in the Age of Committed Foreign Threats" on Cook County Clerk's website. https://www.cookcountyclerk.com/sites/default/files/pdfs/Election%20Security%20White%20Paper_Praetz_12062017.pdf

[43] Lute, Jane Holl, "Cyber Security Keynote Address" in *Critical Challenges to Peace and Security: The Economic Crisis, the Arab Spring, Afghanistan & the Rapid Growth of Cyber Threats. Proceedings of the 29th International Workshop on Global Security*; Center for Strategic Decision Research. Menlo Park, Ca and Paris, France. Baylon, Anne D., Editor, pp. 63-67.

https://www.csdr.org/2012%20Book%20-%20Rome/2012%20Rome%20Workshop%20Proceeddings.pdf

The Importance of Strategic Decision Making for Cybersecurity

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

I will start with a discussion about mitigation of the breaches, threats and vulnerabilities in our infrastructure that are growing in prominence. While we are learning how to keep adversaries out of our networks, cyberspace offers countless opportunities for projecting political power and achieving the advantages of military intelligence. One of these opportunities is strategic deception. We must understand that the infrastructure is not the only target. In the past, the Soviet Union struggled to match the West's technological advancement and development, so it started to seek alternatives to hard power. Eventually the Soviet Union began exploring physical and regulatory systems as a means to attack the very instrument behind the utilisation of assets which is the core of "decision making."

The Soviet Union struggled to match the West's technological advancement, so it sought alternatives to hard power.

The ability to depend on critical assets is of utmost importance to national security. Disruption of decision making is a very effective way to flatten the imbalance between rivals. By crippling the utilisation of advanced technologies and assets, you can take away the West's dominance. Cyberspace serves as a great enabler and amplification tool in that sense and provides means to achieve information superiority, which is essential for tampering with an adversary's decisionmaking mechanisms.

Cyberspace serves as a means to achieve information superiority, in order to tamper with an adversary's decision making.

We have been speaking about code and content operations. We have heard several examples over the past two days and I would like to say that we are analyzing what is going on, especially in the Ukraine theatre. Code and content operations are favoured by Russia right now. Russia has adopted the techniques of so-called 'active measures' and adapted them for cyberspace. By so doing, Russia can actually draw from the vast experience and long tradition of deception campaigns that were conducted by the Soviet Union in the past. This is the connection between the analogue past and the digital present. The active measures that were invented and used in the '50s, '60s, '70s of the past century and are used today in cyberspace and let us say that we are not really pleased about that!

Russia can draw from the long tradition of deception campaigns that were conducted by the Soviet Union in the past.

The key problem that we have identified is that all of us think of the protection of cyberspace mainly in terms of securing the ICT (Information and Communication Technology) infrastructure. However, the Russians perceive cyberspace as three different intertwined layers.

These are the *information sphere,* which involves interaction and perception, *information itself*, which involves formulating the perception of the outside world, and then *the information infrastructure* that we are seeking to protect.

As to the threat that we are facing, I would like to call attention to three aims of our opponent, which is to *shatter communications, demoralize the enemy* and then *take out the command structure.* There are a variety of ways to achieve these aims. You can buy or invest in the media, you can conduct detailed attacks, you can paralyze journalism with the threat of libel, you can confuse the West with mixed messaging, you can seduce experts through high-level fora, you can conduct information campaigns, you can divide the West through divide and conquer ruses, or you can buy up political influence. We are witnessing all these elements as we speak, especially in my country, the Czech Republic.

You can invest in media, paralyze journalism with libel threats, seduce experts, employ divide and conquer ruses.

One way to do this is to give a partner or an opponent specially tailored information so that he will voluntarily make a predetermined decision. This is called 'reflexive control.' It was invented by Vladimir LeFebvre, a Soviet military researcher in the '60s or '70s who is actually residing in the United States. Military decision making is based on information about such things as the area of conflict, troops, or their ability to fight. In peacetime, however, the target is political decision making, and the objective is to influence the information channels and send messages that shift the flow and content in a way that is favourable to you. This means that peacetime conflict is not between military or political assets or soft power, it is between decision making mechanisms and processes.

In peacetime, the target is political decision making—to shift the information flow in a way that is favourable to you.

The aim is to manipulate the sensory awareness of the outside world, how we perceive it and then how we act. This is achieved by a combination of tempering the so-called 'filters' or 'data processors,' which is essentially the ability to conduct analysis and decision making. From Russia's perception and that of its military thinkers and policy makers, information itself has developed into a national strategic resource. I would like to present you with a few of the elements of information warfare that are currently being used in cyberspace and, of course, in our ordinary world as well. Those are distraction, overload, paralysis, exhaustion, deception, division, suggestion and a few more.

There are countless ways to utilize cyber in these ways. To achieve distraction, for example, you can use code and content operations by shifting the focus of media and public attention and by nurturing fear. I think all of you remember the hack of *TV5 Monde* in France, which occurred in April 2015. It was initially attributed to the Islamic State or Daesh, but, actually, the hackers seem to have been Russian, not Daesh. It was a perfect way for Russia to distract the general population and decision makers who were tuned to Russian aggression in Ukraine. Suddenly, Ukraine and Russian aggression were no longer on the front burner. As to exhaustion, it can lead an adversary to waste resources on operations that are not strategically important or to relocate forces to areas that are not that significant.

The *TV5 Monde* hacking was a perfect way for Russia to distract decision makers from its aggression in Ukraine.

How can future generations deal with these information operations? The best approach is to combine cyber exercises with in-house strategic analysis. As to the analysis of strategic intent, intelligence agencies usually have these skills, but they are not necessarily found in cybersecurity. The exercises themselves present decision makers with real life-like situations and test how they respond to a threat or to a cybersecurity incident. We are conducting these exercises on a regular basis and at the beginning, participants are usually surprised and even argue that the situations could never happen. Therefore, the exercises are basically an exposure tool for decision makers.

When it comes to a real cyber attack, the decision maker needs to understand the severity of a given situation in order to respond adequately as it develops. Decisions typically have political costs which incentivize risk-averse decision making, even in a situation that might call for a bolder response. From the decision maker's perspective, of course, this is not necessarily unreasonable because many of the responses he might make will have potential legal and political considerations that will not always be apparent on the operational side.

In such situations, the in-house strategic team or strategic analysis team has an important role. As an example, consider that you have before you a minister or deputy minister. If you tell him in technical terms that you are being attacked from a certain range of IP addresses, or that you are finding certain indicators of compromise, you will not be understood and you will be out the door in two minutes. That is why you need someone to contextualize what is going on and who can explain the real world implications of technical events when they occur.

Not many understand the strategic intent of our adversaries, be it China, Russia, non-state actors, or others.

I would conclude with the fact that today's national security officers are not really accustomed to those old-school deception methods that are emerging again in cyberspace. We have very good technical experts, forensic and malware experts, and capabilities for reverse engineering. Yet, not many people actually understand the strategic intent of the opponents, be it China, Russia, non-state actors, or others.

The prominence of social media and the almost complete reliance on cyberspace when it comes to command and control is a vulnerability that allows Russia (or others) to manipulate the perceptions of decision makers. Well, cyberspace has become the new arena for decision making. It is the place where the battles for hearts and minds are fought today. And without the hearts and minds, the decision-making process is crippled.

How Is the Digital Age Transforming our Lives?

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

Over the last two days, we have heard about how much the cyber threat has grown. Since I am attending the workshop for the first time this year, I imagine that, ten years ago, the conversations were probably focused on issues like malware. Today, we hear about fake news, influence operations, how cyber is woven into the fabric of our lives and what threat factors exist at the government, corporate and individual levels. We see how the cyber threat is changing the way governments operate and legislate, how they raise individual concerns although those who are concerned may not necessarily be well-informed. There is certainly a lot to worry about as we consider how the digital age is changing our lives, but it is a double-edged sword since the digital age is also changing our lives for the better. It creates so many opportunities to advance our economy, government, defense system and to make it possible for individuals to have better lives, but we must stay diligent and make sure that we are protected against these cyber threats.

The digital age is a double-edged sword: a source of worry and a potential for a change for the better.

I would like to make a few comments about the United States. The United States has not fought alone since World War I, whether it was a kinetic fight or a fight for influence. We have strong links with our partners and allies and, concerning cyber security, working together across nations is critical. As several speakers mentioned, we cannot fight alone—no single organization or entity can do it by themselves. We must share information across nations with different cultural norms and work closely with them to accomplish that. I was happy to hear that NATO is conducting exercises to get an understanding of what the new norms look like and what the response should be. We will not be able to deal with a cyberattack if we have not thought through and understood how we should respond.

I do not believe that we have a good deterrence strategy. If we did, Russia and China would act quite differently.

Going forward, we need to worry about deterrence and resilience since the threat is not going to stop. We can try to protect against it, but it will continue, and I do not believe that we have a good deterrence strategy. If we did, Russia and China would not keep doing what they do to the United States, to Europe, and to our world security. We definitely need to spend more time thinking about a deterrence strategy in the cyber realm. We talk about using all levers of power, but we shake our fingers and say: “Don’t do that, there will be consequences.” Nonetheless, we have not come up with the right consequences. Someone mentioned the sanctions against North Korea. How much more can we do to get North Korea to understand that we are serious and that there will be more of a consequence than just yet another economic sanction that China will help them get through? Deterrence really needs to be looked at. Resilience has been discussed as well. We have a real opportunity to use technology to help us make our systems more resilient. I think this panel will address that too.

Attribution: The Importance of Forensic Proof

Mr. Marco Braccioli
Senior Vice President, Area SpA

As a first point, I would like to note that many of you have mentioned the importance of “attribution.” Twenty years ago, our company, Area, started in the law enforcement sector and today, it is also in defense. Consequently, “attribution” for us means “forensic proof.” During a recent NATO workshop in The Hague on networking and technologies for future NATO C3I and other capabilities, the most frequently mentioned word was “forensic.” This is because we need a forensic proof to effectively protest against another country that has committed some form of aggression against us.

Today, the technology of the internet is widely used by the military, by criminals, and many other groups. As a result, we now live in a kind of hybrid world and this applies to warfare, which can be hybrid. A perfect example would be in some countries of North Africa where local communications work, social media works but, at the same time, the cities are at the center of military action. So, in order to be effective, forensic technology and military technology have to work together because, in this hybrid environment, there is a mix of conventional forces, irregular forces, terrorists, criminals etc. and there are also tools like the use of local unrest, information warfare, propaganda, diplomacy, cyberattacks, and economic warfare that can be used together as well.

In the dark web, a sort of weaponization of the social media has taken place.

This includes the dark web, where a sort of weaponization of the social media has taken place. Specifically, there is a place called the Marianas web in which some countries sponsor hackers by giving them contracts to attack certain targets. This is more or less like what happened during the reign of Queen Elizabeth I: if you were able to bring a captured galleon back to London, you were a hero, but if you were caught by the Spanish Navy, you were considered to be a pirate. We are now in a similar situation where young people who are supposedly hacking on the internet are actually not young people at all: they are more likely to be university professors in their countries who have been given grants and other forms of support to attack Western targets. This is the clear strategy for the so-called troll factories.

We need a new generation of instruments to fight against such challenges. For example, we can develop a new platform to infiltrate digital devices inside criminal groups; with our forensic experience, we can support our government authorities against international criminal groups, which means obtaining information related to certain groups of criminal hackers. Another approach is to investigate the costs of developing a cyberattack by creating profiles of hackers who would likely join these groups. There are many workarounds that make it possible to do this. The most important tool for us, however, is a new generation of analytics. This is because we are probably going to have a Data Fusion Center combining the monitoring center that comes from the law enforcement world with defense command and control. From a single tweet, we have to do correlations to a list of airplane passengers or National Plate Register (PNR). This means going from internet unstructured contents to structured contents and this requires organization and a Data Fusion System.

To fight cyberattacks, the most important tool for us is a new generation of analytics.

Finally, what are the appropriate responses to hybrid attacks? Obviously, you can infiltrate and target the networks of hostile groups. You can do intelligence collection. You can do wide psychological operations (PSYOP) on the internet. Communications, including “post-truth” communications, are certainly useful. In the case of peacekeeping forces in a country, for a period of one hour, anything on the web can appear to be true or can appear to be false, which means that web psychological operations are very effective. In conclusion, none of this is simple, but I think that the web, together with human intelligence (humint), can help us greatly in understanding and preventing many of the threats that we are facing on the internet.

What are the appropriate responses to hybrid attacks?

Artificial Intelligence and Cyber

Mr. Maurice Cashman
Chief Strategist, McAfee

I think we are on the cusp of an evolution in our cyber defense strategy. Having the privilege of working with some of the leading customers and organizations in cyber, particularly in the financial sector and in government, I can see this happening first hand. It is an evolution that goes like this: from defense in depth, controls and sensors, enhanced with threat intelligence, and maybe with technical type intelligence, to one of interoperable security systems that are enabled with advanced analytics and empowered with continuous intelligence. They are permitting faster decisions and more autonomous actions. I think there is a key connection between analytics and action—and that is where we really get the benefit from this new capability.

Gartner defines four outcomes for analytics: descriptive, diagnostic, predictive, and prescriptive.

What does that mean in terms of analytics? Gartner defines four outcomes for analytics: descriptive—describing what happened; diagnostic—determining why something happened; predictive—telling what might happen; and then finally, prescriptive—what should I do? There is an evolution in terms of the humint input, the human-machine teaming aspect. In the descriptive field, much human interaction is necessary. In the prescriptive field, there is a more automated course of action in order to reach a determination, perhaps even with automated response actions when connected to the right infrastructure. So, the evolution is more in terms of the analytics, from a heavy emphasis on descriptive analytics to a greater emphasis on prescriptive capability. Both prescriptive and predictive analytics are considered advanced capabilities, but I personally see more prescriptive technology on the market than predictive.

As to other analytics issues, there is a lot of terminology. People will mention AI, but there are many levels: one is just collecting data and providing visualization—collecting statistics, doing correlations, or threshold analysis. But the new ways forward involve things like machine learning, the ability to learn from the data, to discover patterns. Deep learning or deep neural networking is another terminology and you can think of it as automated machine learning, with multiple nodes, multiple algorithms working together in a network, just like your brain might operate.

Four minutes was the time for a global manufacturing company to have 35,000 servers taken down.

And then there is artificial intelligence, which is the top end, with the most complex, self-learning systems that mimic human brain activity. There is very little actual artificial intelligence on the market in cyber defense tools, but, while we are starting to come out with those now, machine learning is more common for obvious reasons.

So, what has driven the evolution or the shift? I will give a few statistics. Four minutes: that was the time for a global manufacturing company to be disrupted and have 35,000 servers taken down in one of the attacks this year. That is an incredibly fast time. We used to say that four hours was the timeframe we were hoping to have and now the timeframe is minutes. So, you need to have systems that can leverage analytics to identify attacks and permit us to reconfigure or at least share information that allows the system to reconfigure itself. That is actually possible today and it is out there at several leading customers’ environments.

Another interesting statistic is a hundred milliseconds: That is a billing cycle for Amazon web servers and computing platforms. Think about that as the granularity of a timeframe. Normally, we are thinking about hours or days, in terms of deploying things or even in terms of billing cycles. But now, with computing and automation, you are talking about a hundred millisecond timeframes. Another statistic: 80 percent of the IT budget will be dedicated to cloud security or cloud applications by 2020, according to Forbes. So, we have to be able to leverage analytics across new kinds of operating environments and we may not have control over those environments. So, we have to apply the best advanced techniques to those environments. A machine learning and machine automation is a way to put security into those new operating environments.

80 percent of the IT budget will be dedicated to cloud security or cloud applications by 2020.

And then what is the last statistic? 1.5 million and that is a predicted cybersecurity talent shortage. My personal belief is that adding more people is not the answer to the problem. We have to figure out the root causes. Are we providing those people with the right data? I think that leveraging analytics to provide humans with better data so that they can make better decisions is the way forward.

I would like to leave you with a few considerations when thinking about acquiring analytics for your cyber strategy. First, think about it from a recruitment standpoint. Maybe you need to think, where do I get the data scientist? where do I get the guy that can do the coding versus just the security analyst?

Another really important point is that it is an emerging field, in fact, on the Gartner Hype Cycle, this is called adversary machine learning. There are two aspects: first, it is adversaries who use analytic techniques like AI, or machine learning, to discover vulnerabilities, discover weaknesses in our attack surface, for example using social media analysis. Adversaries have been doing that forever. They have been trying to bypass spam systems with these techniques. But another more worrying field is what they can do to the data that we use to train an algorithm. For example, we as a company and others in the room have to be really aware of how adversaries might try to disrupt or corrupt the data that we use for training our algorithms, how they might want to bypass our systems, bypass classification models and so forth. Because a lot of systems that are on the market today are two-fold: they have a sensor and a cloud component, and that is very ripe for denial of service activity.

Adversaries use analytic techniques like AI, or machine learning, to discover vulnerabilities and weaknesses in our attack surfaces.

And then finally, I would like to make sure that you do not think of analytics as a silver bullet. We have done this so many times in security where we said, I have a sandbox, or I have another great tool, and we are good because we have the latest stuff. Analytics has to be applied throughout your whole security staff, in your endpoint controls and network controls for classifying anti-malware or finding attack patterns but also in user behavioral analytics or entity analysis to find traffic anomalies, data anomalies, or user anomalies. And then finally, I would like you to think about other areas in the Security Operations Center (SOC) that are important such as learning, especially since most people do not like cyber security training.

Cyber Threats to Connected Cars and Autonomous Vehicles

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

Introduction

I am the Information Security Research Lead in a think tank within AXA (the insurer company) which focuses on future trends in cyber security. Currently, I am working on a study on connected cars and, to a certain extent, driverless cars. These vehicles will provide tremendous safety benefits and they will significantly reduce traffic congestion, but not enough attention has been paid to their cyber vulnerabilities

When I began this study, I found that the automotive industry seemed to have convinced many underwriters that they did not really need to worry about cyberattacks on connected vehicles. Digging a bit deeper, I realized that there is a significant culture of denial within the automotive industry. Partly, it is because they do not have a lot of experience with cyber security, at least among the traditional vehicle manufacturers. In fact, there is some covering up as well: some car manufacturers, including Volkswagen, have used litigation to prevent researchers from publishing the vulnerabilities that they discover (even though the researchers had given them half a year to fix the vulnerability before they planned to publish it).

Volkswagen has used litigation to prevent cyber researchers from publishing vulnerabilities.

For these reasons, I thought it would be useful to give a broad overview of where the cyber security vulnerabilities are in connected cars, and I will also talk about some of our projections about the future.

Definitions

Before beginning my discussion of cyber threats, it may be useful to begin with a few definitions: As you might expect, a *connected car* is simply a car that has internet access. Features typically include smartphone interfaces, so people can connect their phones to the car to stream music or find restaurants nearby. You can often turn a car into a Wi-fi hotspot, and on-board navigators may get internet updates about traffic jams or collisions. There are roadside assistance systems that connect you to the service via a cellular connection if you are in an accident. *Driverless cars* are one type of connected car, and they typically make use of technologies like GPS and radar to understand and sense the environment around them, so they can operate without a human driver. While they are currently being tested on roads, we do not see them on the market yet.

The Controller Area Network, or CAN bus, is a key vulnerability—it is the car's "central nervous system."

Cybersecurity Challenges

I am now going to sketch out some of the main areas where connected cars are vulnerable from a cyber perspective. Perhaps the first concern is the Can bus. All modern cars have a Controller Area Network, or CAN bus, that is basically the "central nervous system" of the vehicle. It serves as a central point which enables every system in a connected car (the brakes, steering, etc.) to communicate with each other. Before the adoption of the CAN bus, the car's different systems had to be hardwired/connected directly in order to talk to each other. So, the introduction of the CAN bus really increased efficiency, but this also means that the CAN bus is also a central point of vulnerability. If a hacker can access the CAN bus, they can send commands to all other systems connected to it. In fact, it can be said that the CAN bus is "insecure by design." It was first developed in 1983, when security was not a major concern, which means that it lacks basic security features like authentication and encryption.

First developed in 1983, when security was not a major concern, the CAN bus is "insecure by design."

With connected cars, most people do not realize just how many parts of the vehicle have some form of wireless connectivity. All of these could provide routes of entry for a hacker, and from there they can access the CAN bus and send commands to other parts of the vehicle.

Infotainment Systems. One major risk is the infotainment systems (which provide entertainment and information features) and typically have Wi-fi or cellular connectivity. There is a famous example of an infotainment vulnerability from 2015, where a team of researchers at Black Hat showed that they could hack a Jeep Cherokee. They were able to take control of the car remotely over the internet irrespective of distance, without any need for physical access. The attack exploited a vulnerability in a proprietary platform that controls the car's infotainment system. The vulnerability allows anyone who can obtain a car's IP address (which can be obtained by brute force within an hour) to access the platform. Once the hacker has gained entry, he can implant malicious code allowing him to send commands through the CAN bus to the engine, wheels, and other physical components. The hackers were able to control the brakes and to fully shut down the engine at lower speeds, and the researchers were later able to expand the attack to other Jeeps, Dodges and Chryslers, as they also made use of the same proprietary platform.

Entering through a Jeep's infotainment system, hackers were able to control the brakes and to shut down the engine.

Telematics. Telematics systems (which provide monitoring and safety) are another route of entry, because they tend to make use of cellular or Bluetooth connections. For example, in roadside assistance systems, which have cellular connectivity, researchers found a vulnerability that allowed them to gain access if they called the system multiple times. Another example: Bluetooth enables a driver's cell phone to connect to the vehicle to enable hands-free calling. This means that if a hacker infects a phone through a phishing attack and the phone is paired to the vehicle, the malware could then find its way onto the vehicle.

A hacker can install malware by infecting a phone through a phishing attack, if the phone is then paired to a vehicle.

USB Ports. Given that most connected cars have USB ports, we are also considering scenarios where a user's mobile phone is infected with malware and they plug it into the USB port to charge, inadvertently infecting the vehicle.

Mobile Applications. There are also a number of mobile applications that enable vehicle owners to interact with their connected cars, and that of course provides an entry point for hackers. Last year, researchers showed how they could hack Tesla's official app to steal a car.

Connected cars can be infected when updates are downloaded over the internet, or even over an EV's charging cables.

Updates. Connected cars need frequent updates in order to fix bugs in the software and provide new features as well. When these updates are downloaded over the internet, hackers could insert malware into an update

Charging Cables. It is likely that a growing number of vehicles in the future will be electric, and many will need charging cables. The charging cable offers another opportunity to introduce malware.

Vehicle to Vehicle Communications (V2V and V2I). We are also considering the vulnerabilities in Vehicle-to-Vehicle (V2V) communications that are currently being developed. V2V communications allow nearby cars to communicate with each other over wireless networks, sending each other information on their speed, position, etc. If a number of cars ahead suddenly apply the brakes and steer to the left, a following car can deduce there is an accident or obstacle in the right lane. There are also Vehicle-to-Infrastructure (V2I) communications which enable cars to communicate with highway infrastructure like cameras, streetlights, and lane markers. Some of the theoretical possibilities include the following: A hacker could gain access to V2V or V2I communications and feed false information into the network. For example, they could falsify a car's position data and cause a crash with other vehicles or introduce malware onto a vehicle. If all vehicles are eventually linked together with V2V and V2I, these networks can be used to infect vehicles on a massive scale, since one infected car could spread the infection to all of the other nearby vehicles on the network.

A hacker gaining access to V2V or V2I communications could feed false information into the network.

Tricking AI. One area we plan to study is whether it would be possible to fool the AI algorithms in driverless cars, perhaps tricking them into believing that a stop sign is actually a green light.

Attack surfaces. A connected car presently consists of over 100 million lines of code, which is more than in an F-35 fighter jet. The sheer size means there are likely to be a considerable number of bugs, with anywhere from 15-50 errors per 1,000 lines of code.

As connected cars become increasingly ubiquitous, there are going to be more and more incentives for hackers to attack them.

Future Threats

For the future, we are concerned about the potential use of connected cars as weapons by terrorists, especially for driverless cars. We are also predicting a surge in ransomware attacks, with scenarios in which the owner of a car might find himself locked out (or even locked in) and have to make a ransom payment to regain access. In some such instances, there are likely to be fleet-wide attacks, since a vulnerability in a Jeep Cherokee will extend to all Jeeps in that range. The theft of customer data is also something we think a lot about, given the very large amounts of data generated by connected cars.

Finally, we do predict a large number of attacks on connected cars in the next five years. At present, there have not been a significant number, but as they become increasingly ubiquitous, there are going to be more and more incentives for hackers to attack them.

Is It Time to Develop a “Moral Compass” for Software?

Mr. Don Proctor
Former Senior Vice President, Cisco

The genesis of this question is a talk I gave recently in San Francisco. As the event got underway, I was somewhat surprised to find that the two speakers who preceded me were a theologian and an ordained minister speaking about the value of ancient wisdom in an uncertain universe. This is a pretty hard act to follow when you are a nerd from the Silicon Valley coming to talk about software innovation. So I pivoted just a little and talked about the need for technology developers to incorporate a moral compass into the software that enables our increasingly automated world.

In order to survive and prosper, we must start designing software with a moral compass.

I could not think of a better place to issue this challenge to industry and government than at the 34th International Workshop on Global Security at the Hôtel des Invalides in Paris, in the former Council Chamber of King Louis XIV. With the Sun King’s likeness and his armor on the walls, there would be no better opportunity to throw down the gauntlet in a room with, well, actual gauntlets.

To set the context for this topic, I will mention the names of five prominent people who will probably be familiar to you. The ideas I will propose are building on the shoulders of giants, and they all play a part of what I will call the emerging moral landscape of software.

Marc Andreessen, venture capitalist and creator of the Mosaic web browser, famously said in his August 2011 Wall Street Journal article, “Software is eating the world.” This is certainly evident in the Silicon Valley, where I have spent most of my career. We have the Internet of Things, we have self-driving cars, and we have more drones than we can count. But Andreessen’s comment also begs the question, “If software is eating the world, what is eating software?” I am going to float the idea with you that in order to survive and prosper, we must start designing software with a moral compass. Here is why.

In 2014, theoretical physicist *Stephen Hawking* told the BBC that “The development of full artificial intelligence could spell the end of the human race.” Later that year, *Elon Musk*, founder of Tesla and SpaceX, said at an MIT conference that “With artificial intelligence we are summoning the demon.” These are strong words from some pretty smart guys. But we are living in an increasingly autonomous world. We have smart homes, smart devices, and smart vehicles. The future is here, although it is of course not yet evenly distributed.

Many people now accept the notion that self-driving vehicles make better decisions than person-driven vehicles. But who gets to decide, in the case of an unavoidable collision, whether your car crashes into a school bus or a church? The answer, whether we like it or not, is that in many cases it is a coder (a software developer), working somewhere for some organization, and using his or her best judgment in deciding what kind of algorithm to create.

It gets even trickier. The UN has recently convened a panel, under the Convention on Certain Conventional Weapons, to help determine under what circumstances a military drone can decide autonomously to drop a bomb on a particular target. There is little doubt that a drone has better identification abilities, better reaction time, and less subjectivity than a human pilot in a manned aircraft, or a drone operator sitting in a bunker in Nevada. But in the case of the Internet of Things, autonomous cars, and military drones, just because software can do a better job, does that mean we should let it?

Just because software can do a better job, does that mean we should let it?

Hippocrates, the father of modern medicine, said in the BCE millennium, “First, do no harm.” Maybe there is something we can borrow from him. Our software should not be written in a way that causes unintentional harm to people. This seems obvious, but how many companies have a formal policy that says their software will not intentionally hurt people? There is a paradox here.

Our software should not be written in a way that causes unintentional harm to people.

A company founded in the small city I grew up in near Los Angeles, California, is the top supplier of drones to the Pentagon. Virtually every major defense contractor is also in the military drone business. Some of those drones are used for surveillance, but some are also of the weaponized variety. Weaponized drones are generally controlled by a remote-control pilot at a military base, often thousands of miles away. Does the Hippocratic Oath help us with machines that are designed to keep certain people out of harm’s way, but to hurt others?

Permit me to fast-forward 2,000 years from Hippocrates to call upon *Isaac Asimov*, the American science-fiction writer, to dig a little deeper. Some of you have no doubt heard of Asimov’s “Three Laws of Robotics” from his famous1942 story, “I, Robot.” In short, the three laws say that robots have to do what people tell them to do, and that they cannot hurt people.

Is software providing a net benefit to humanity, or not?

Perhaps even more interesting is something Asimov came up with a little later, which he humorously called the “Zeroth Law: “A robot may not harm humanity, or, by inaction, allow humanity to come to harm.”

So the “zeroth law” is not actually about humans, but about *humanity*. I do not mean to make this a commentary on science fiction, but Asimov was by all accounts an insightful critical thinker and felt that it was important to address the impact of machines on people not just *in the specific*, but *in the aggregate*.

Individual cases aside, is software providing a net benefit to humanity, or not? There is of course no one answer to this question, but I will propose three possible approaches to the question about how to begin developing a moral compass for software:

- Legislate the conditions under which software is allowed to make decisions. Make the legislative process flexible enough to keep up with daily/weekly advances in technology;
- Leave humans in charge. Let a person decide when to enable the security camera, when to turn the wheel, or when to push the button;

- Take the open source approach to enable the moral compass as a set of transparent software stacks, like LAMP (based on Linux) or Android, under the premise that "sunlight is the best disinfectant."

Open source presents the best collaborative framework we have in software development today. When hundreds or thousands of developers have access to source code, it receives almost unlimited distribution, analysis, and improvement. Software builders will be motivated to use the open source stack as a matter of efficiency but could also be encouraged to disclose when they do so as a matter of legal liability.

None of these answers is perfect, and we can think of valid counter-arguments for each of them. Can lawmakers keep up with the pace of technology change? Will the global marketplace agree to curtail innovation in favor of leaving humans in charge? Do we sacrifice security by using an open source model? It is important to start the dialog now, because the future is coming faster than we think.

Concluding Remarks

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

As the Deputy Director of the Institute for Higher Defense Studies (IHEDN) within the Prime Minister's organization, I am pleased that we are partnering for the fifth year with the Center for Strategic Decision Research (CSDR). I would like to take this opportunity to thank all of you for your contributions to our discussions, and for joining us from nearly 20 countries including the U.S., our European neighbors, and Japan. We are meeting here under the watchful eyes of King Louis XIV and Emperor Napoleon III. Across the courtyard, Napoleon observes us as well. These are men who led France to fame and glory. Yet, both Napoleon I and Napoleon III ultimately suffered great losses from ill-considered ventures that forced them into defeat and exile. Perhaps it is worth remembering the lessons that they acquired at so great a price—that early victories in battle or other gains can be mirages.

This year's theme of "Global Security in the Age of Hacking and Information Warfare: Is Democracy at Stake?" initially surprised me. In fact, just one year ago, we were focused on cyber threats to our economies, our militaries, or individuals. Only now are we beginning to understand that our national sovereignty, the cohesion of our societies, and our democratic values and institutions are at risk. In fact, the new U.S. National Security Strategy released yesterday announces for the first time the need to deal with a "New Generation Warfare" that seeks to divide and weaken nations with cyber influence operations. According to U.S. National Security Advisor General McMaster:

Our national sovereignty, society cohesion, democratic values and institutions are at risk.

> *"These are very sophisticated campaigns of subversion and disinformation and propaganda using sovereign tools, operating across global domains that attempt to divide our communities within our nations and pit them against each other."*

In representing IHEDN, it is not my role to summarize the discussions of the last two days. Nonetheless, I would like to emphasize a few points concerning Russia because the panel on Russia had a very broad approach:

- *A major cyber-attack is nearly certain.* An attack of the highest level (category one) has been predicted by the U.K. National Cyber Security Center, and it will not be in the distant future. Attacks against individuals and companies are larger and more frequent. For example, the Equifax hack hit 143 million users; Yahoo lost data on 3 billion users. Some of the most dangerous attacks will be against states or critical infrastructure. Hillary Clinton warns of a new cyber cold war, and we must recognize that the West is not winning this war yet.
- *In order to make sure that a cyber cold war does not become hot,* we will need better International cooperation among governments and industry, including collaboration in areas ranging from academic research—like that of the Castex Chair of cyber strategy at our IHEDN institute—and perhaps more workshops like this one. The sharing of cyber information needs to be automated—and some of our participants are working on it. Sharing with smaller countries needs to be improved, but cooperation is slow—partly because countries want to spy on allies as well as on enemies, but

especially because of a lack of *trust,* which we must build together. To sum up, we need cyber pedagogy for everybody and the associated training activities and for sure toolboxes.

- *Cyber risks to critical infrastructure are growing.* The vulnerability of nuclear power plants is significant, since operators are now linking their business systems to the internet to increase efficiency. Already, the electrical grid is "on the radar" of hackers and potentially of cyber terrorists. Even though nuclear weapon systems are being modernized, there is no 100% guarantee that they are safe from a cyber-attack. Worse, countries are developing cyber technologies to attack the command and control of the nuclear weapon systems of their adversaries.

Cyber information sharing needs to be automated but cooperation is slow, partly due to lack of trust.

- *Security in the cloud.* Organizations are moving toward the cloud for economic benefits, but there are risks. As data migrates to the cloud for security, financial, and other benefits, the cloud may become a high value target—which could attract sophisticated attacks by groups with large resources.
- *Privacy.* Should individuals have more control over their own data—or does it belong to Google, Facebook, Twitter and the organizations that harvest it? According to new EU regulations, citizens have the right to be forgotten, to transport their data, to be protected against automatic profiling, to be protected against data leaks, and to be notified if leaks occur. So, it is mandatory now to find a fair balance between security and liberty.
- *Artificial intelligence***.** As artificial intelligence (AI) is increasingly applied to cyber security, it will introduce new risks and opportunities that are not yet understood. Artificial intelligence and Big Data will make it possible to extract and utilize far more personal information about individuals. Most likely, it will be necessary to design cyber defense systems that will achieve a new level of resilience.
- *Dealing with cyber influence operations, including "fake news" which are becoming more and more "realistic."* Cyber influence operations, including fake news, have emerged as a serious threat to our democracies, a real ramp up of clever attacks. Fake news can be amplified by retweeting or bots or by clever exploitation of social media algorithms. We need to mitigate the impacts of such fake news. Since some communications can be deleted immediately after being sent, there can be a mass effect without leaving a large footprint. In Spain, it is only in the last few months that Russian involvement in the Catalan referendum has been understood; In the U.K., possible influence on Brexit voting is also recent. One of the most serious concerns is the reluctance, or even unwillingness, of social media companies such as Facebook, Twitter or Google to cooperate fully.

Cyber influence operations, including fake news, have emerged as a serious threat to our democracies.

- *A New Security Priority for Governments and for NATO.* The just-announced U.S. National Security Strategy includes among one of its pillars the need to deal with "…sophisticated campaigns of subversion and disinformation and propaganda … that attempt to divide our communities within our nations and pit them against each other."[44] Yet, this is not an issue for the U.S. alone, it should be adopted now as a priority for all of our countries, and NATO, the European Union, and other international organizations. As Napoleon I said *« Se faire battre est excusable, se faire surprendre est impardonnable » or " To be beaten is excusable, to be taken by surprise is unforgivable.* " So, people need to be more aware, people need to strive for trust and then deterrent and resilience will naturally follow.

[44] General H. R. McMaster, *op.cit.*