24 Dec 16

33rd
International Workshop
on Global Security

Global Security in Crisis:

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

Summary and Findings

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

intel Security

MITRE

AREA

ASSOCIATE SPONSORS

CAST

ARES CORPORATION

AXA

ACKNOWLEDGEMENTS TO PAST HOST AND SPONSOR GOVERNMENTS

Czech Republic
Kingdom of Denmark
Federal Republic of Germany
Republic of Hungary
Kingdom of the Netherlands
Kingdom of Norway
Republic of Greece
Republic of Poland

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