The Nexus of Cyber Security and Disinformation

Speaker: Daniel Bagge, Cyber Attaché of the Czech Republic to the U.S. and Canada, National Cyber and Information Security Agency

Moderator: Sean Costigan, Director and Co-Founder, ITL Security

Rapporteurs: Simon Bracey-Lane & Sherwin Bothello

Speaker Bio:
Daniel Bagge is the Czech Republic's cyber attaché to the United States and Canada. Until August of 2018, he was the director of the Cyber Security Policies Department at the National Cyber and Information Security Agency in the Czech Republic. He has provided his expertise to NATO ACT, USCybercom, US AFRICOM, US Congress, military and national security entities in Ukraine, the Balkans and other nations. He has written a book called: *Unmasking Maskirovka: Russia's Cyber Influence Operations*

Introduction
The annual theme of this year's Cyber Security Summit is: 'the ripple effect'. How do the cascading impacts of today's world develop and how can we constantly manage our fields to stay ahead of threats?

The world is changing faster than many of our institutions can adapt. As our world changes, so too have methods of diplomacy, trade, industry, and warfare. Many in the West have failed to understand that war is no longer *exclusively* tanks, ships, and missiles. It is waged with a hybrid combination of disinformation, cyber, energy, corruption, organized crime, legal structures, and economics. We live in a world where everything can be used as a weapon. Whilst many of our revisionist adversaries are aware of this change, subsequently embracing and adapting to it, much of the west has been sluggish and flat footed.

It is why discussions regarding the nexus between two elements of this hybrid warfare are so vital. If you look at one mosaic piece at a time, all you will see is a single colored tile. To see the entire picture, you must see all the tiles together.

Thank you to our sponsor

CWT

Disinformation:

The word "disinformation" heralds from the Russian word, *dezinformatsiya* (**дезинформа́ция**). It is a method of sowing discord and chaos through the spread of intentionally false information.

Today, disinformation techniques are evolving rapidly. While the governmental and private sectors are admiring the problem. The fast-paced progress from non-digital means of spreading disinformation that were adopted for the digital age has caught our societies completely unprepared.

From Soviet concepts of active measures to the digital age and microtargeting, this discussion will examine the nexus of cyberspace and disinformation.

Problem Setting:

It is useful to break down an examination of disinformation into two parts. Firstly, that information as a weapon of war is an old concept and there is a great deal of understanding to be wrought from past masters, the USSR in particular. By examining the past, we can see how it has evolved into the threat it is today. Secondly, how has the current technological environment impacted this threat?

Historical:

Many are unaware of the history behind disinformation. Where it has come from, how it has changed and why it is so effective today.

The USSR, upon realizing it could not technologically keep pace with NATO, opened a new front: the decision maker. They believed that if you can alter the opinions and beliefs of your opponent and create structures to prod them into making favorable decisions, you will shatter the decision-making infrastructure. It would not matter how wealthy and technologically advanced the West was if the political/military leadership will have been incapacitated without firing a shot.

Assaulting the decision making algorithm was formalized into a framework as Soviet military scientists predicted the lessening significance of large scale, protracted warfare and the rise of intelligence and information based precision strikes or, Reconnaissance Strike Complex. In this new warfare, information would play a much larger role. To successfully compete, a revolution of military thinking produced a deployable framework called: Reflexive Control.

It is this military doctrine of 'attacking the decision makers' that lies at the foundation of many modern disinformation campaigns. Expand the notion of a decision maker beyond Western political and military leadership to everyone: voters, consumers and users and the potency becomes clear. To understand disinformation, you must first know what it was designed to achieve: the incapacitation of decision makers through chaos, deception, and discord.

Digitalization:

Take the military grade research that produced the concept of reflexive control and apply it to unsuspecting citizens and private sector interests, and you have a perfect storm.

In the past, it was incredibly difficult for foreign entities to know your hobbies, who you talk to, what you like, how you vote and what you spend money on. However, in today's world, this information is freely broadcast by almost everyone. This information has become a huge chunk of modern marketing

revenue. It has created a sector of our economies, companies who act as data brokers, that cluster all these data points and build behavioral patterns of users and consumers.

Data has become the new oil, but people are widely unaware of the power and influence they freely give away. The information shared on social media and other means is not only profitable to corporations, but also to foreign actors.

This mass availability of public information is a problem in its own right, but it is further compounded by the rise in micro targeting and Geographical Information Systems (GIS). With the increasing technological prowess available to commercial entities, businesses now possess the capability to home in on specific pockets of the population. From a marketing perspective this is valuable, whilst advertising platforms like TV was a blunt instrument, you now possess the capacity to produce highly specific content, catered to each consumer.

From an intelligence standpoint, however, this becomes the perfect petri dish for any disinformation operation. A foreign actor can, with some ease, pretend to be a third-party business and purchase information from data brokers. They then have access to all the pressure points within our societies, that they can apply the lessons of reflexive control to on a massive and highly nuanced proportion.

This is further compounded when combined with Geographical Information Systems, the ability to capture and analyze spatial and geographic data. You can pinpoint specific users where they live and look at what issues they are discussing by each household. This can prove to be disastrous if in the wrong hands.

Social media outlets have become public opinion shaping vehicles that are accessible to foreign adversaries. It has significantly widened the scope of the 'decision maker', allowing them to influence elections in democratic nations because they can run campaigns designed to divide populations that have been focused to an incredibly specific degree.

The Nexus of Cyber & Disinformation:

A great deal of the cyber security community focuses on the physical and digital infrastructure of cyberspace. Rather, we must widen the lens to include the information layer. Cyber security hasn't contributed enough to the conversation about how we protect the *content* that passes along our networks.

This is a difficult thing for the cyber security community to do. It comes close to posing a significant risk to our liberal democratic values. Raising questions about whose role it is in society to regulate/control information. This is a stark example of how the strengths and weaknesses of our liberal societies impact our ability to protect ourselves.

Furthermore, we often overlook the interaction between the information and users. The databases that contain information harvested from social media are some of the most commercially valuable and best protected databases in the world. However, there are few mechanisms in place to ensure that the information itself within the databases has been protected from corruption and falsehood. Is there also a role for cyber security in protecting how that data is then used?

Cyber security has prominent a role to play in protecting our societies from disinformation. Whether that is safeguarding how information is collected or protecting people from false information. It is a fine balance and not without risk, but the benefits to our societies would be huge.

Conclusions:

Mark Twain has said that 'a lie makes it twice around the world while the truth is tying its shoelaces'.

What chance do we have to combat lies and disinformation? The answer is that there is no silver bullet. No single tool, no one specific blueprint to follow. It is vital that the private sector contributes to these conversations, but it is hard to bring them to the table because of how lucrative the collection and targeting mechanisms are.

Many will say the best way to combat disinformation is education, but this is difficult to apply universally as campaigns are highly specific addressing complex topics. They play on cognitive bias, targeting an issue designed to elicit an emotional response rather than a logical one.

Social media outlets have a responsibility to curb the spread of disinformation on their platforms. Whilst we must encourage deeper collaboration between governments, organisations and corporations to facilitate a greater regulatory response.

Finally, one of the best ways to communicate the threat posed by disinformation to both governments and the public are case studies. Efforts to outline how much our democratic processes are threatened by throwing long winded examinations of Soviet Russian psychological warfare will be ignored. Conversely, if it is trivialized, continuously referred to as 'fake news' the danger will not be realised. That is why examples of hacked billboards in downtown Kyiv, the riots after the LISA case must be used in conversations with the private sector, political figures and the general public to demonstrate how foreign adversaries use information as a weapon of war to attack our democracies.