Agenda: Establishing a framework against information warfare
Chairpersons: Alex ROBIC and Devraj Singhania

DISEC
DISARMAMENT AND SECURITY

Table of Contents:

Introduction

The Disarmament and international security committee deals with disarmament, global challenges and threats to peace that affect the international community and seeks out solutions to the challenges in the international security regime. It considers all disarmament and international security matters within the scope of the Charter or relating to the powers and functions of any other organ of the United Nations; the general principles of cooperation in the maintenance of international peace and security, as well as principles governing disarmament and the regulation of armaments; promotion of cooperative arrangements and measures aimed at strengthening stability through lower levels of armaments.

Basic Definitions

The Committee works in close cooperation with the United Nations Disarmament Commission and the Geneva-based Conference on Disarmament.

Cyberspace - refers to the virtual computer world, and more specifically, is an electronic medium used to form a global computer network to facilitate online communication. Cyberspace allows users to share information, interact, swap ideas, play games, engage in discussions or social forums, conduct business and create intuitive media, among many other activities.

Cyberattack - is a deliberate exploitation of computer systems, technology- dependent enterprises and networks. Cyberattacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cyber crimes, such as information and identity theft. Cyberattack is also known as a computer network attack (CNA).

Cybercrime - is any criminal activity that involves a computer, networked device or a network. While most cyber crimes are carried out in order to generate profit for the cyber criminals, some cyber crimes are carried out against computers or devices directly to damage or disable them, while others use computers or networks to spread malware, illegal information, images or other materials.

Cyber Espionage or spying - is a form of cyber attack or crime which steals classified, sensitive data or intellectual property to gain an advantage over a competitive entity or a government entity. Hackers target computer networks in order to gain access to classified or other information that may be profitable or advantageous for the hacker. Cyberspying is an ongoing process that occurs over time in order to gain confidential information. It can result in everything from economic disaster to terrorism.

Cyber warfare: actions taken by a nation-state or other organization to attack and attempt to damage another nation’s computers or information networks through, for example, computer viruses or denial of service attacks. (source: RAND.org)

Computer virus: A computer program designed to be undetected and disrupt a computer system. Known categories are trojans, ransomwares (WannaCry)…

Denial of service attack: A computer attack involving a single or multiple (botnet) machines overwhelming a server or network by sending an overflow of requests with the intent to prevent legitimate users from accessing it through the virtual fog of traffic.

Encryption: A mathematical process consisting of the substitution of a byte string for another through a function involving a key (numerical value, character or string) used for encrypting and decrypting. Some functions are one way (hashing) and others are symmetric (cyphering). The reverse process is known as decryption. An encryption/decryption sequence follows 1 important rule: for an encryption function E, a decryption function D, a key K and a plaintext Pt, D(K, E(K, Pt)) = Pt.

False flag operation: a political or military action that is made to appear to have been carried out by a group that is not actually responsible.

Public choice theory: a theory by which government ownership (or control) of the media undermines political and economic freedom. A government owned media will most likely serve a purpose to persuade rather than inform.

Public interest theory: a theory by which government ownership (or control) of the media should maximize social welfare. A government owned media is seen more as a public service rather than a company.

Countries List

DISEC		
United Kingdom	Canada	New Zealand
China	France	Iraq
India	Brazil	Russia
Israel	Japan	Korea

Topic Background

The two most important and most mediatized aspects of information warfare today are psyops (psychological operations) and electronic warfare (cyberattacks). Both are incredibly cheap and easy to pull off which makes them that much more dangerous. All it takes is either a couple dollars that you wire to places like India, Macedonia or Romania to hire yourself an untraceable team at the other side of the world or a dedicated military branch to conduct attacks on a specific target.

Information warfare as it's being portrayed is so recent, it only started entering the debate about 10 years ago with governments even creating new agencies to start dealing with offensive and defensive capabilities just like in the 1950s and 60s when nuclear weapons were being heavily developed by both the US and Soviet Union. Although that may be the case for media propagated psyops (fake news operations) and cyber-attacks, warfare through information is what made the cold war. Between 1947 with the creation of the CIA and 1991 when the Soviet Union dissolved, spying, exchanging and stealing information from one another was common not just between the 2 superpowers but everywhere else in the world with Berlin being the capital of such activities. Grabbing information from an adversary would serve as a preventive strike by knowing what technology was available on the other side and thus better preparing against it. Two very famous examples of this come from the world of aviation. A Taiwanese sidewinder missile was lodged unexploded into a Chinese MiG 17 during the second Taiwan strait crisis in 1958. Lacking an infrared missile to rival the American made one, the Chinese were able to reverse engineer it and is now still used throughout the world as the K-13. The second most widely known example of technology theft was when the Israelis captured a Mig-21F during the six-day war in 1967. From this, the US Air force was able to figure out the engine was poorly armored as well as the fuel tank. Technological details weren't the only precious information goods during the cold war, diplomatic information was as well. Operation Gold was a joint CIA MI6 operation that involved tunnels under Berlin until 1956 when a mole informed the Soviets about them with the objective of gaining intelligence about the Soviet Army's movements from their headquarters in Berlin. The same kind of operation went on in Vienna under the codename operation silver.

Although the information theft still goes on today, rather than being copies of blueprints passed physically from hand to hand or left in dead drops, it's stolen from computers or passed along in storage devices. The most blatant example of such theft can be seen in China's Chengdu J-20 fighter jet that takes the cockpit and air intake from the F22, the engine exhaust from a F18, canards from the Rafale and a rudder from the F35.

As well as trying to steal data from other governments, a new trend has recently emerged tracing back to as early as WW1 but adapted to today's technologies and topics: psychological warfare

(or now called media warfare). As opposed to propaganda which is when a government actively tries to change the minds of its own citizens, psychological warfare is aimed at citizens of another country or a certain group outside of the country of origin. From radio stations in a foreign language aimed at enemy soldiers (Tokyo Rose for example was a Japanese woman who would broadcast on the air in English with American troops as her main target and would try to discourage them from fighting by saying things like “while you’re fighting abroad, your loved one is in another man’s arms”) to leaflet droppings in war zones (the US would drop leaflets in Vietnam encouraging Vietcong defection) to more modern and adapted techniques like information flooding (filling the internet with fake news for example, common before elections). Information, rather than being distributed with the intent of teaching and being beneficial, is being used to divide people and cause chaos.

Facing the potential that people are now targets and weapons and that significant discoveries in the fields of computer security and cryptography have made hacking more complicated, a new question has emerged: what is there to do concerning this problem? After all, writing a story and sharing it online, whether true or false, falls under freedom of speech but can be propaganda which is a tool of war. The recent Covid-19 pandemic has not made this easier either. Some countries or groups may want another country to be deliberately given fake news about the pandemic for it to last longer thus creating havoc longer.

With the world going into confinement and many classes being moved online, cybersecurity has become more important now than ever since an attack doesn’t mean paralysing transport infrastructure or power grids anymore but now also affects the education system as well as the ability for many to be able to work from home. The rise in the use of video conferencing software has also meant an increase in the risk of attacks from malicious individuals. Before April 2020, Zoom was still using 2DES encryption which was vulnerable to brute force attacks and only switched to AES when that major flaw was pointed out.

Case study: Russian Media influence in the Ukraine

On December 31st, 1999, the Russian federation’s leader Boris Yeltsin resigned from the office of President of Russia. According to the constitution, his prime minister took over under the program that he would end the oligarchy in Russia and the corruption associated with it. On the following day, Vladimir Putin would take control of Russia and change it into the Russia we know and love today.

A Russian show by the name of Куклы (translated becomes « dolls » or « puppets ») was a very popular and beloved show in Russia based on the British TV show « spitting image » at the time

of his inauguration and used puppets in order to mock political personalities. The show regularly made fun of him in it so much that some reported he would be infuriated at how he was depicted.

Putin, who values his image more than anything (cf the shirtless photos of him) decided after that private media in Russia shall no longer be, launching a campaign to change the constitution and legally acquire every media company in Russia (at least be the majority shareholder for every company). This would ultimately end the puppets show and rank Russia as one of the worst countries for freedom of the press (ranked 149/179 according to the 2020 report by Reporters without borders). TV6's owner at the time Boris Berezovsky would eventually go into exile in England and die under unusual circumstances in 2013. This control over Russian Media would give Vladimir Putin a great platform for expression and cult of personality. Since his first days in office, he was obsessed with the media, going as far as to organize photo shoots in the Kremlin to put himself forward.

In 2014, between February and March, an army of mercenaries entered Crimea and took control of the local parliament as well as other key locations and evicted the local parliament. Not wearing any identification (which goes against the Hague convention stating that a combatant should wear an identification linking them to a faction or they will be able to invoke the Geneva convention), these forces would eventually occupy the entirety of Crimea by mid-March and by the end of the month, Crimea would become part of the Russian federation. This takeover from Russia would cause a war in the region that would bring rebels from around the world fighting for Crimea's freedom as well as for Russia. Putin justifies his actions by stating that the « little green men " do not belong to him as they wear no form of identification as well as by the fact that Crimea houses a certain percentage of 67% in 2014 (source: Crimean census). Annexation of Crimea can also be linked to Putin's will to divert Information warfare : valid use of media or illegal interference ? October 2, 2020 6 attention from the economy (inflation would reach 13% in 2015 and the ruble would collapse).

As Ukraine is populated by 17% of Russians (2001 census, that number has most likely changed especially due to the events of 2015) and being nostalgic for the Soviet Union which he first saw collapse in Berlin as a young intelligence officer, Putin today continues his campaign to recreate the easter superpower of the 20th century and that includes reconquering Ukraine.

Many Ukrainian media outlets have been replaced by Russian owned ones in Crimea in what journalists call an « information war » organized by Russia who in return says the west legitimized the actions against the country's current government of the time (which had decided to sway away from the EU and closer to Russia). These actions were condemned by the OECD (Organization Européenne pour la Coopération et le développement économique) who said that this would open the doors to « the worst kind of propaganda ».

The problem with the situation is that at times, western media and Russian backed media have described completely different scenarios which journalists on both sides have condemned. Liz

Wahl, a journalist for the American division of RT (Russia Today) resigned on air due to those actions, claiming that she disagreed with the way Putin's actions were being « white washed ».

The propaganda that OECD refers to is the fact the intervention was labeled as a humanitarian action against the persecution of ethnic Russians living in Crimea and claim this fact is being ignored by the west. Some go as far as to claim that facts are only presented in a biased way and the truth is being half told.

The case in Ukraine is not a completely isolated one. Russia today (or RT as it's referred to by its domain name to not reveal its Russian ties in its name) continues to broadcast internationally and does the bidding of Russia's foreign policy. The constant attacks on western institutions and governments can be compared to the broadcasts of Tokyo Rose during WW2. This impact was especially felt during the US elections of 2016 and is still felt today concerning subjects like gun control in the US, Covid-19 throughout the world and Brexit in the UK. Fearing a similar consequence, Estonia (where Russians make up 25% of the national population) has increased its ties with NATO. Lithuania has also prepared for similar events with operation Lightning Strike.

Other Cases to look at

1. Presidential elections in the USA, 2016.
https://www.rappler.com/technology/features/russia-cyber-warfare-disinformation-campaign-2016-us-election

https://www.youtube.com/watch?v=GYIgmua-J7o

2. Multiple cyber incidents between Israel and Iran (Operation Nitro Zeus)

https://www.youtube.com/watch?v=qh-er7BAqVA

https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html

3. DNC hacking of 2015

https://www.youtube.com/watch?v=cCxZ0jM-FXU&t=3s

https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html

4. Sony hack by DPRK

https://www.vanityfair.com/news/2019/10/the-untold-story-of-the-sony-hack

https://www.youtube.com/watch?v=EAQxElHsySw

Possible Solutions

There really is no possible solution to this problem. Unlike diseases that can be cured with a vaccine in most cases, there is no real way to prevent cyber intrusions. The best one can do is employ advanced cryptography (AES is the most commonly used one today) to delay intrusions.

A few examples of aftermath decisions taken include the complete replacement of hardware at the DNC (Democratic National Committee) after an intrusion in 2015 during the campaigning period. Such intrusions could have been prevented through meticulous training on phishing campaigns which is how the whole debacle started. Generally, when dealing with complex security systems, the best way to get inside is to use someone who is already there through a process called social engineering. This involves the use of either corrupted USB keys (which led several agencies to super glue the USB ports on all computers) or someone on the inside. The best ways to fight both of those intrusions is through vigorous employee screening as well as regular inquiries into what they do outside work.

When it comes to media warfare, some argue it's the job of the social media platforms to do the hard work of filtering posts, information and accounts.

During the 2016 elections, Facebook was used as one of the main platforms to spread false information from both sides of the political spectrum. Pages like Eagle Rising would tell the tales of thousands of Syrian migrants wanting to come to the US to take advantage of the system and others would claim that Trump was not mentally fit to be left with the nuclear codes.

Some of the solutions provided include but are not limited to:

-Better identifying false news by submitting posts to 3rd party fact checkers

-Making it harder to monetize fake news (restricting advertisement purchases for pages known to produce that kind of content)

-The use of machine learning to better assist response teams in finding accounts that produce fake or « click bait » content

-Ranking improvements: making sure that the top-rated content is not just rated because of the traffic it generates. Fake news articles will tend to include every buzzword they possibly can in order to draw attention thus generating more traffic and increasing the probability that more people will think it's true.

-News integrity initiative: A tech industry and scholar backed initiative to better help the public make « informed judgement »

Under certain videos published by well-known media companies, YouTube will include a small div stating where a news channel is from and who funds it. The google owned video sharing platform has been known to voluntarily keep fake news videos up. Although a video that is obviously fake news will not be taken down (unless it violates community guideline standards), it will be dereferenced from the trending section. The reason behind this is purely economic: the more news a video gets, the more attention the platform gets. This was especially made true 2 years ago when a youtuber named Logan Paul filmed a hanging man in the « Japanese suicide forest » and uploaded it on the platform. Many news agencies linked the video in their articles which in turn increased traffic on youtube.com.

Questions

1. To what extent is it the government's role to respond to attacks on privately owned information infrastructure? How can and should government and private industry coordinate a unified response to cyberthreats ?
2. What should be the thresholds for response in different situations by States?
3. To which extent should a free press be free? Should there be some kind of government control on what is said and if so, to which extent?
4. Should a government be able to own a media company or be its majority stockholder? (Public choice theory VS Public interest theory)
5. Should a country's government-owned media's propaganda be deemed as an act of war? If so, what should the consequences be? How shall one respond?
6. Should there be a period of mediatic truce before an election in order to prevent unverifiable fake news?
7. Should a news outlet be able to report on news in a foreign country and then be able to publish in the country that is being reported on?
8. To what extent is it a government's job to prevent the spread of fake news or that of the website provider/administrator?
9. What about the UN in all of this? Is it equipped to deal with false information? Should a new body be created? Is there already an existing one that can receive that mission?
10. If you were to look at media warfare and cyberwarfare as an invasion of a country, should a country's borders include its communication lines? Should the UN redefine national sovereignty?

Contact us: Devraj Singhania - devraj.singhania@sciencespo.fr

Alex Robic - alexandrerobic312@gmail.com

Bibliography

1. The perfect weapon by David E. Sanger
2. Facebook for media
3. Information warfare : valid use of media or illegal interference ? By Alex ROBIC