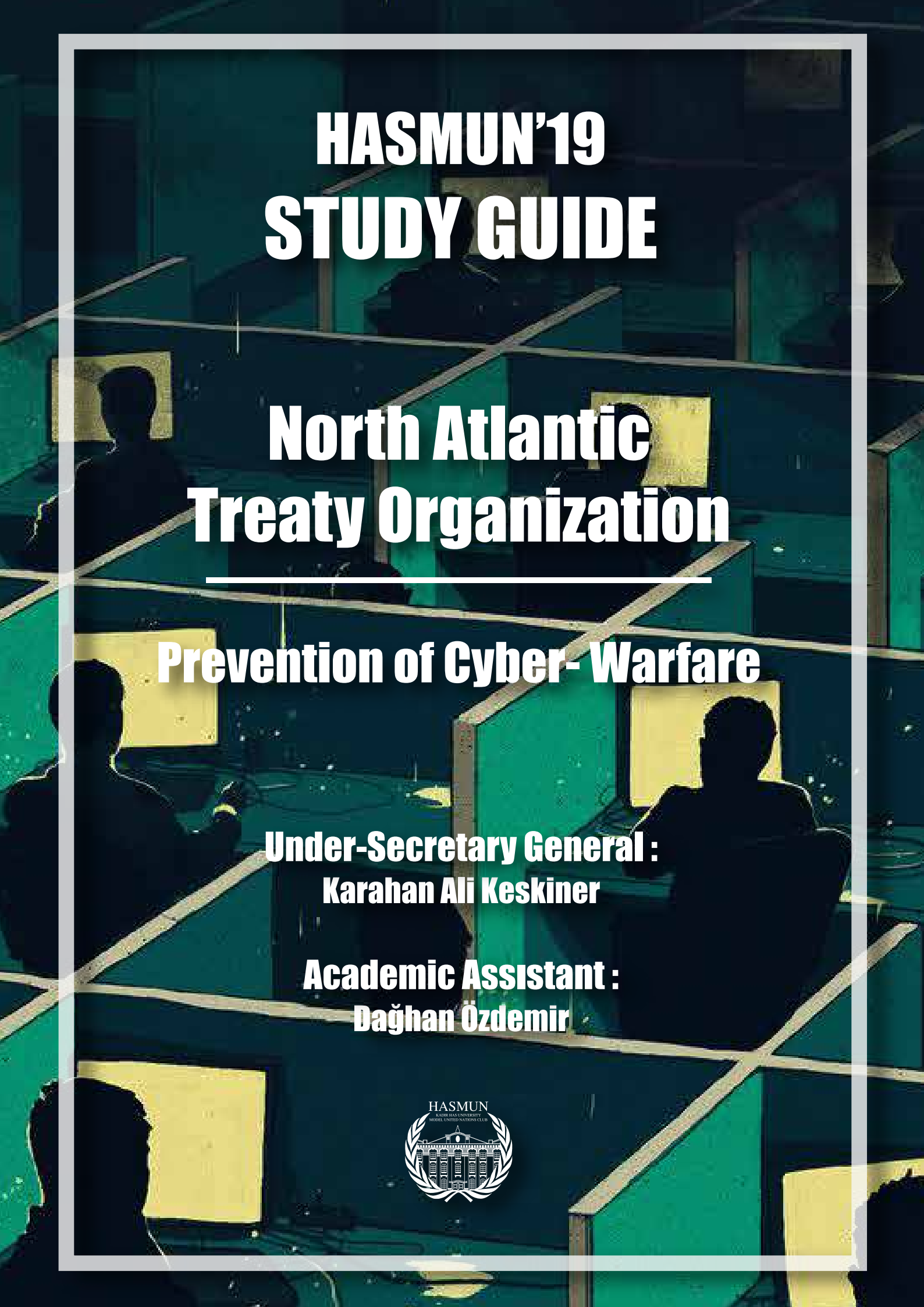


HASMUN'19
STUDY GUIDE

North Atlantic Treaty Organization

Prevention of Cyber- Warfare

Under-Secretary General :
Karahan Ali Keskiner

Academic Assıstant :
Dağhan Özdemir

HASMUN
KADIR HAS UNIVERSITY
MODEL UNITED NATIONS CLUB

Table of Contents

I)Introduction……..3

II)The North Atlantic Council……4

a. History of the council……..4

b. Mandate of the council……....5

III)Russian interference in networks of sovereign states…….6

a. Background……...……..6

b. The 2016 United States Presidential Elections……...…...……8

c. The Impact of Russian Interference on Germany's 2017 Elections……....8

d. Prevention of Rising Tensions Leading to Cyber-Warfare……..9

IV)The Issue of 5G Infrastructure……...10

V)Strengthening the Current Means of Communication……..12

Letter from the Secretary-General

Dear Delegates and Advisors,

It is a great pleasure and honor to officially invite all of you to HASMUN 2019 which will be held between **26th and 28th of April 2019** at Kadir Has University Haliç Campus in Istanbul which is located in the Golden Horn area.

I am personally thrilled to take part in the making of this conference and I am sure that the academic and organisation teams share my passion about this installment of HASMUN in which we have chosen to focus on topics that bring humanity together. And we have also included committees which will simulate historical events that can be considered existential threats which brought the international committee or some nations together. The general idea that we would like to introduce is that humanity can achieve great things in little time if we are united, or can eliminate threats that threaten our very existence.

I strongly believe that the first half of this century would be remembered in the human history where we enter into a new era through technological advance. Unfortunately we haven't quite grasped the importance of this generation, as we progress we leave a print on this world and for the first time modern world is facing an existential threat, for the first time every human being on the planet is facing the threat of a considerable change in their and their ancestors living or worse, our very existence being on the line. I believe it will be events like these marked down in history which bring humanity together if we unite with no ambition of national gains and handle these crises. Our highlighted special committee of World War Z will be based on the book with the same name written by Max Brook which tells the story of how world is affected by a Zombie outbreak and the Humanitarian Advancement and Security community or HASCOM will take place in the year of 2050 where the delegates will rebuild the world from it's ashes and have the chance of changing how it works.

The other committees will be focusing on current problems that are born out of neglect for an extensive amount of time either due to lack of public interest or because of economical reasons and solving these issues will have long lasting positive effects or if they are left unsolved they may have bigger consequences in the near future.

With that I welcome and look forward to seeing all of our participants and guests on the 26th of April, at HASMUN 2019, hoping that you will have an exquisite time, debates and most importantly have fun while changing the world, only you can do it.

Best Regards

Ata Mavi
Secretary-General of HASMUN'19

Letter from the Under Secretary General

Esteemed participants,

I take great pride in being able to serve as your Under Secretary General in HASMUN 2019 and I hope you will be enjoy it as much as I will. Through these four days, we will be working on problems that have plagued the world for years and looking for unique but plausible solutions. My job in the conference is to make sure that you understand the material well, not let you get bored, and guide you through your work. I will always be available whenever you need something, whether it be formatting your resolution or doing some wingman work for the guy/girl you've been eyeing.

Below, you will find a study guide that is simple and brief. Our academic assistant, Dağhan Özdemir, wrote some parts of it and did an excellent job. The guide will be complemented by articles, historical data, and research within the committee. Please try and read it all and if there is a part of it which confuses you, send me an e-mail at karahankeskiner@gmail.com. While HASMUN will give the Rules of Procedure to delegates either physically or online, I will again be available whenever you need to ask something; as will Dağhan and your committee directors.

Please just read the guide, it exists to make your job easier.

Karahan Ali Keskiner

I) Introduction

The issue of cyber-security has been discussed since World War II. Even though the machines have changed, the nature of the problems haven't. Still, the utility of technology compels people to use it and provides a noticeable edge over those who don't. This makes instruments of communication and information technologies extremely valuable targets for intelligence. With the volume of data being at the heights that it is at today, anyone who controls how the data is received or collected gains an invaluable advantage.

Hence, it is apparent why the North Atlantic Council spends so much time and money thinking about cyber security. In this guide, we will first begin with the recent turbulent events that cause concern about cyber security with a focus on Russian interference. Another hot topic of debate is the worrisome expansion of Chinese companies and their willingness to handle the new 5G infrastructural constructions.

After talking about issues, we will briefly touch on what NATO has already done to combat them. Investments, task forces, and already existing security measures will all be discussed.

II) The North Atlantic Council

The North Atlantic Council is chiefly responsible for the political decisions that the North Atlantic Treaty Organization (NATO) makes. Representatives of all the NATO states gather in meetings and whatever the resulting document is (whether it be press releases, military directives, or strategic roadmaps), it is agreed upon by all the members.

a. History of the council

The council was founded in April the 4th, 1949 with the establishment of the NATO. It oversees the execution of the Treaty. Since 1952, it regularly meets twice every week and discusses whatever issue is at hand. While representatives conduct these meetings, -depending of the magnitude of the situation- cabinet members (responsible for either military or foreign affairs) or even heads of state can attend them. It has expanded and keeps expanding since its inception into Eastern Europe and right now, Bosnia and Herzegovina and the Republic of Macedonia are in the process of joining.

The council took an active role in combating many incidents since its inception, including the Bosnian War, the Kosovo War, the War in Afghanistan, and the intervention in Libya. All of these are perfect case studies for understanding how the decision making mechanisms work within the council, some of which we will get into during the conference.

The Secretary General (presently, this is Jens Stoltenberg) is in charge of running the meetings. Reports from subordinate committees are presented during meetings, which helps the decision-making process through better understanding of the geopolitical landscape, logistics, and financial implications.

b. Mandate of the council

NAC is the only organization in NATO that was established by the Treaty itself (Article 9) and its capabilities vary from the other sub-bodies quite strongly.

First and foremost, it is the only sub-body that can create other subsidiary bodies. This means the committee will be able to create chambers of its own to assist themselves however they see fit. Only the Nuclear Planning Group has a similar amount of freedom, but only in their area of expertise.

In the conference, you will be representing heads of states, not PermReps (which are the bureaucrats that normally conduct the meetings), which means you will be relatively autonomous in your decision making. This, however, does not mean that you can do whatever you want. You must still remember that you are operating under political frameworks and representing a country. With that said, the council has another advantage in that you can make decisions regarding your country. These are done through individual directives, which we will get into in the final part of the study guide.

III) Russian interference in networks of sovereign states

a. Background

[1]The Soviet Union and now Russian Federation under Vladimir Putin have waged a political power struggle against the West for nearly a century. Spreading false and distorted information – called *"dezinformatsiya"* after the Russian word for disinformation – is an age-old strategy for coordinated and sustained influence campaigns that have interrupted the possibility of level-headed political discourse.

[2]Before the 2016 United States presidential elections, Special Agent Adrian Hawkins of the Federal Bureau of Investigation (F.B.I.) called the Democratic National Committee (D.N.C.) in September 2015 to pass along some troubling news about its computer network. His message was brief, if alarming. At least one computer system belonging to the D.N.C. had been compromised by hackers federal investigators had named *"the Dukes,"* a cyber espionage team linked to the Russian government. The bureau had spent the last few years trying to kick the Dukes out of the unclassified email systems of the White House, the State Department and even the Joint Chiefs of Staff, one of the government's best-protected networks.

[3]Germany's foreign intelligence chief had warned that Russia could seek to disrupt subsequent German elections with cyber-attacks. Bruno Kahl said his agency was aware of cyber-attacks with no other purpose than causing political uncertainty.

---

[1] Rappler. (2019). *A hacker explains Russia's use of cyber warfare in 2016 U.S. election*. [online] Available at: https://www.rappler.com/technology/features/208418-russia-cyber-warfare-disinformation-campaign-2016-us-election [Accessed 4 Mar. 2019].

[2] Nytimes.com. (2019). *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*. [online] Available at: https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?login=facebook [Accessed 4 Mar. 2019].

[3] BBC News. (2019). *Spy boss warns of Russian vote hacking*. [online] Available at: https://www.bbc.com/news/world-europe-38142968 [Accessed 4 Mar. 2019].

[4]In January 2015, the pro-Russian hacker group *"CyberBerkut"* undertook a two-day DDOS (distributed denial of service) attack on German government computers—timed precisely to coincide with a visit of Ukrainian Prime Minister Arseniy Yatsenyuk; the hackers called: *"All Germans and the German government to end financial aid for the criminal government in Kiev."*

5

b. The 2016 United States Presidential Elections

Hackers affiliated with the Russian military intelligence service (GRU) penetrated computer systems of miscellaneous governmental networks, and Clinton campaign officials. Thousands of private emails and attachments were released to the public during the final months of the 2016 campaign, via *"DCLeaks, Guccifer 2.0 and Wikileaks."* The exposed information revealed internal bias against Clinton's primary challenger Bernie Sanders, which led to the resignation of the DNC chair and lukewarm backing of Clinton by Sanders supporters. Russian government officials have repeatedly

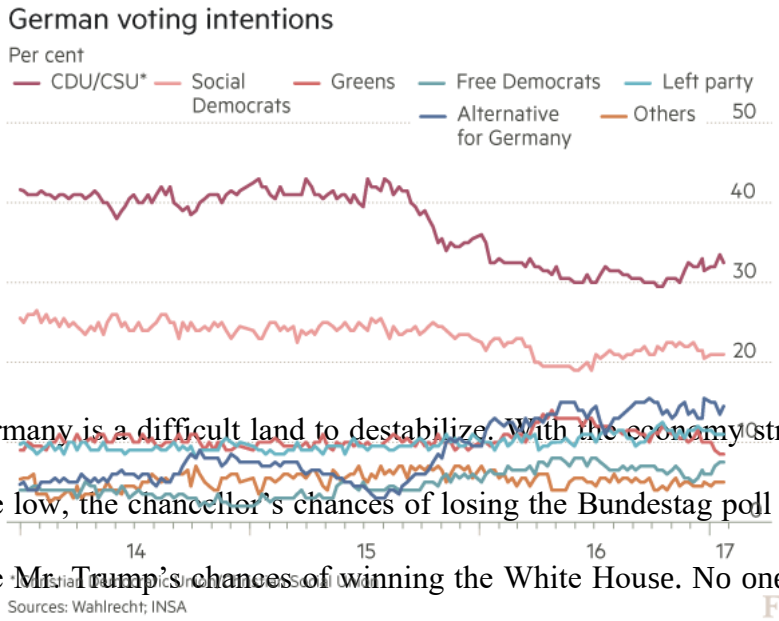
[4] Stelzenmüller, C. (2019). *The impact of Russian interference on Germany's 2017 elections*. [online] Brookings. Available at: https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/ [Accessed 4 Mar. 2019].

[5] Figure: President Vladimir Putin's Russia appears to have meddled less in the German elections, in which Chancellor Angela Merkel is expected to retain power, than in other countries' recently. *Sean Gallup/Getty Images*

denied involvement in any DNC hacks or leaks. In addition to these two operations, Russia-connected individuals reached out to various Trump campaign associates, offering damaging information on Clinton or business opportunities.

c. The Impact of Russian Interference on Germany's 2017 Elections

The Italian constitutional referendum on December 4, 2016, the election in the Netherlands on March 15, 2017, the French presidential, and the British polls on June 8. But without doubt none was quite as consequential for the future of Europe as the September 24 federal elections in Germany, in which Chancellor Angela Merkel won for a fourth term.



[6]Ms. Merkel's Germany is a difficult land to destabilize. With the economy strong, unemployment minimal and crime low, the chancellor's chances of losing the Bundestag poll are considered to be small. But so were Mr. Trump's chances of winning the White House. No one knows whether the Kremlin tipped the balance there, or what it might attempt in Germany.

d. Prevention of Rising Tensions Leading to Cyber-Warfare

Russian state authorities give quite specific and detailed orders and instructions regarding interference. Moreover, execution is more often than not loosely organized, and delegated to a broad

[6] Ft.com. (2019). *German politics: Russia's next target? | Financial Times*. [online] Available at: https://www.ft.com/content/31a5758c-e3d8-11e6-9645-c9357a75844a [Accessed 4 Mar. 2019].

variety of actors. Some are tied closely into a chain of command, others are linked much more tenuously to government authorities, freelancers, and even organized cybercrime networks.

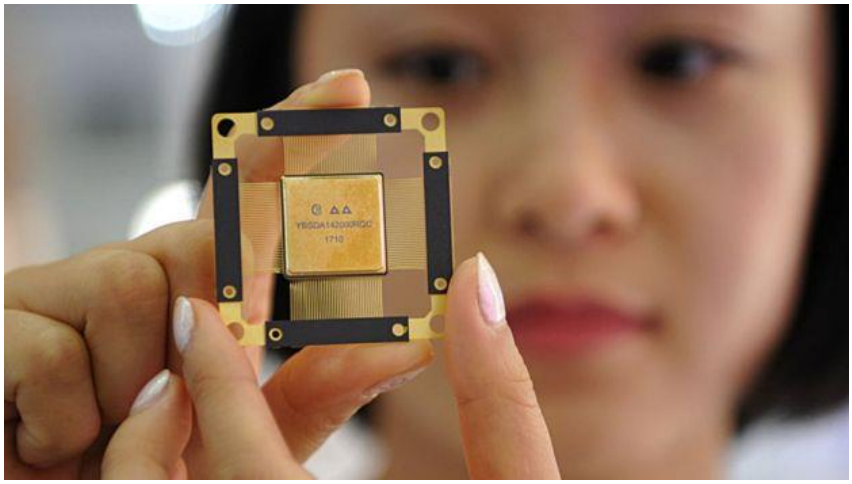
Cyberwarfare by Russia includes denial of service attacks, hacker attacks, dissemination of disinformation and propaganda, participation of state-sponsored teams in political blogs, internet surveillance using SORM technology, persecution of cyber-dissidents and other active measures. It has been claimed that Russian security services organized a number of denial of service attacks as a part of their cyber-warfare against other countries, such as the 2007 cyberattacks on Estonia and the 2008 cyberattacks on Russia, South Ossetia, Georgia, and Azerbaijan.

Preventing intrusion, detecting intrusion and responding, improving resilience… Infrastructures are already insufficient and the recovery capacity is poor. The private sector is responsible for advocating critical infrastructure, and it must adopt a voluntary cybersecurity framework and share first-line information once a breach is detected. The governments are required to implement better regulations too, and not just in terms of election systems while the sovereign states' defense departments are even under massive attack, with attack sophistication rising.

IV) The Issue of 5G Infrastructure

[7]5G is an umbrella term for new and more advanced forms of transferring data, and is a new form of radio transfer. The technology -at the expense of getting too technical- employs a higher density of transmitters and receivers, higher frequency bands, a superb decrease in latency, and an unprecedented increase in bandwidths. In essence, this means up to 10 to 20 times faster connection. Which will be used in hundreds of sectors in the 21st century. The industries that will utilize this technology are chiefly medicine, online streaming, automobile, and telecommunication. However, there is not a single field which will remain unaffected by the revolution. How expansive

[7] BBC News (2018). *What is 5G and what will it mean for you?*. [online] Available at: https://www.bbc.com/news/business-44871448 [Accessed 14 Mar. 2019]



this technology is going to be gives us an accurate estimation as to how important it will be in security.

Therefore, it is by no means a surprise that controlling the infrastructure of 5G would provide an enormous advantage. Being one of the most critical improvements of the century, whoever is in control of the technology when users start moving to 5G, is likely to yield great influence in matters of economics, science, and intelligence. [8]Currently, the Chinese company Huawei seems to be on the frontline in matters of both research and commercial dominance. Over half the world's 5G infrastructure is built by them, and almost all of them use parts of it for their own system. Even before this, the United States had suspicions over how reliable the company was. In 2010, the NSA even infiltrated servers of Huawei in order to prove a link to the Chinese government (which they couldn't). Now with the company dominating the area of 5G, the United States are pressuring other countries (most of them members of NATO) to not allow Huawei to help build their own infrastructure.

[8] NY Times (2019). *In 5G RaceRace with China, U.S. Pushes Allies to Fight Huawei.* [online] Available at: https://www.nytimes.com/2019/01/26/us/politics/huawei-china-us-5g-technology.html [Accessed 14 Mar. 2019]

The US was partly successful in its endeavor, in that they got the United Kingdom to stop using Huawei products, and the telecommunications Vodafone (based in London) significantly reduced their use of Huawei parts for their 5G network all around the world.

[9]This however was not the case for some of the other NATO members. Germany, for instance, refused to act on the matter. Even though they asked for guarantees on many issues, their stance on Huawei isn't nearly as strong as the United States wants it to be. [10]Later, a more serious warning by the German intelligence agency caused the government to change its perspective and European nations seem to be shifting towards excluding Huawei from being involved in the buildout. The move doesn't come without a cost, though, as having other companies in state auctions helps decrease prices for the people, especially if government subsidies are in play.

V) Strengthening the Current Means of Communication

NATO is based upon the common belief that all allies communicate with each other and in a more limited sense, the public.

One of the most prominent ways that states can communicate with each other -and that yields the best results- is through intelligence sharing. This is another topic which will be debated extensively during the conference.

[9] Reuters (2019). *Germany does not want to exclude Huawei from 5G buildout: Handelsblatt*. [online] Available at: https://www.reuters.com/article/us-huawei-europe-germany/germany-does-not-want-to-exclude-huawei-from-5g-buildout-handelsblatt-idUSKCN1PW1TA [Accessed 17 Mar. 2019]

[10] Bloomberg (2019). Huawei Isn't Trustworthy 5G Partner, German Spy Agency Says. [online] Available at: https://www.bloomberg.com/news/articles/2019-03-13/huawei-isn-t-a-trustworthy-5g-partner-german-intelligence-says [Accessed 17 Mar. 2019]

In early 2017, a new sub-body with the name Joint Intelligence and Security Division (JISD) was formed. The division aims to share intelligence in a more efficient manner with a focus on the Middle East. While JISD has proved useful, the NAC will have to find a way to expand the current amount of information that is shared -while staying committed to their respective countries' interests- and to better integrate JISD into NATO's Command Structure.

Another issue regarding dialogue is communication with countries that are outside of NATO. Even when partnership in many organizations were stopped as a result of its aggression, the channels of diplomatic communications were never closed with Russia. The reason for that is that misunderstandings on a global scale tend to work out terribly, and when the country in front of you needs to be informed, it's always better to do it through diplomatic channels.