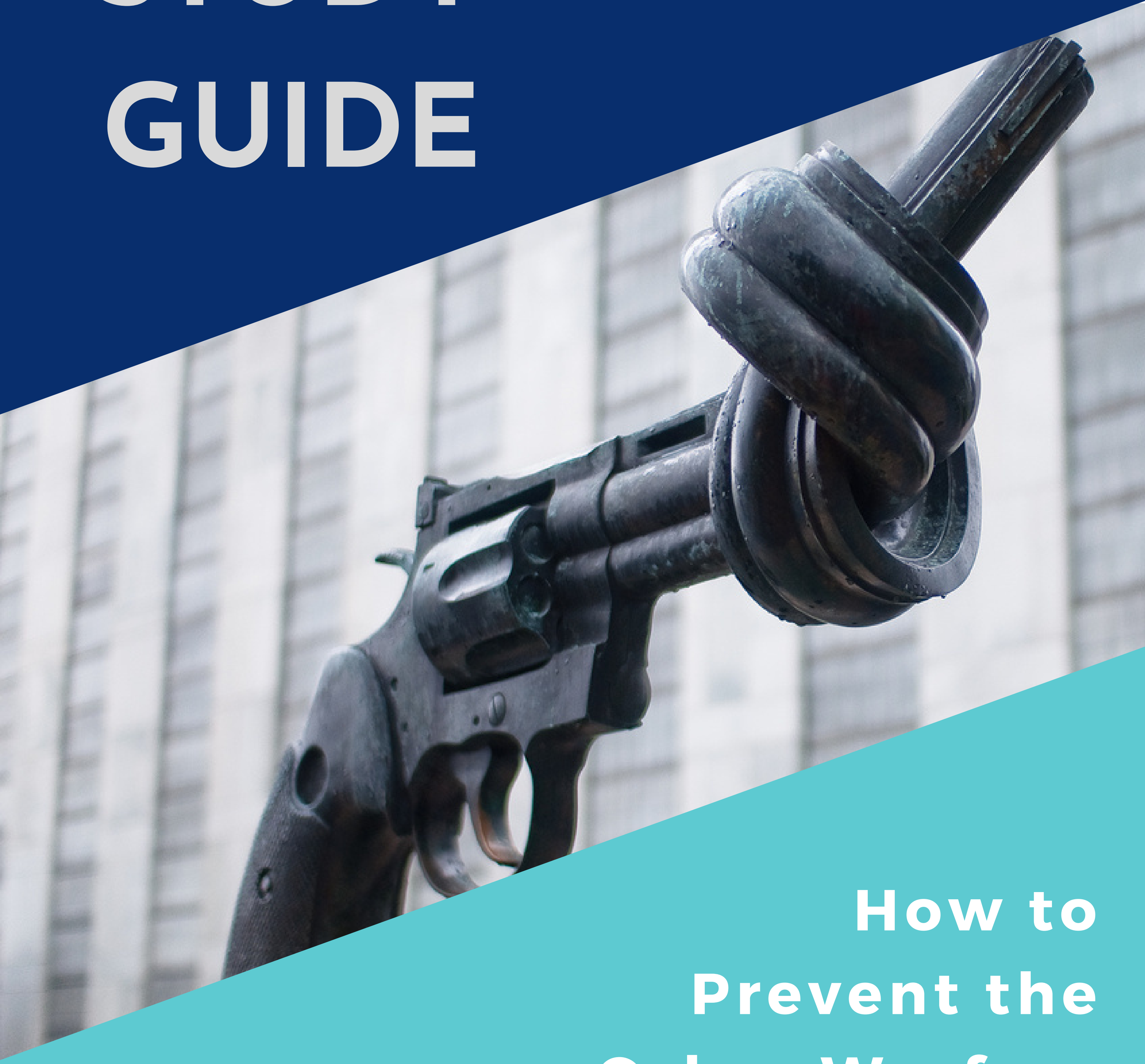
HASTRAIN'21

DISEC (GA1)

STUDY GUIDE



How to Prevent the Cyber Warfare

Table of Contents

LETTER OF SECRETARY GENERAL

Honorable participants,

At long last, it is my immense pleasure to invite you to the 7th iteration of Kadir Has University's train conference, which is set to be held from Saturday, December 4th to Sunday, December 5th of 2021 in Kadir Has University, Istanbul, Turkey!

Last year, to much proud, our club hosted two online conferences in a row for the reason of the COVID-19 Pandemic. Following our online season, we are now very thrilled to welcome our participants in our school's building. Our conference's main mission is to give our participants the best experiences in various ways, and show what Model United Nations conference is. As HASTRAIN'21 is a train conference, we are ready to help all of our participants on their MUN journey. Therefore, there is no need to hesitate in any circumstances, our team will accompany you in their best.

As our world is in an era that almost every crucial topic is related to technology, we aimed to focus two of our committees around it. Crypto market (in WTO) and the Cyber Security (in DISEC) will be discussed in our committees with current width. On the other hand, we have considered discussing the possible consequences of Taliban's new regime in SOCHUM. Last but not least, our fourth committee (UNODC) will be a special committee which will held the discussion about drugs in a world that Colombia is a renown narco-state.

Above all else, it is important to know that I and the entire HASTRAIN team is ready to meet with you. We hope that we will have the best experience together in the first weekend of the December.

Warmly,

Bulut Vize

Secretary-General HASTRAIN'21

LETTER OF UNDER-SECRETARY-GENERAL

Dear delegates,

I am Ahmet Arda Taşkireç and I am a junior in Hacettepe University in the department of English Linguistics also a senior of International Relations in Anadolu University. Initially, I hope you and your families are doing fine in these malicious times. It is my utmost joy to serve you as the Under-Secretary-General of GA-1 DISEC in one of the most well-known conferences in Turkey, Kadir Has University Model United Nations conference. All around the world reigning powers are taking various type of actions regarding various type of scenarios. These actions, time to time, being diplomatic actions, military or cyber actions. In this particular committee, we will mainly focus on cyber actions taking place within countless fields. The questions such as; How cyber-warfare occurs? Or What are the real urges and motives behind these cyber-attacks? Or How these attacks effect the balance of cyber-space? must be enlightened with the guilty and the victim all together. As a consequence of these attacks, no matter the conditions and how humane these attacks are operated, residents personal information being leaked, countries facilities being disrupted and intervened, governments harassed and forced to take counter-action. As it has always been, the warfare is expanding in different domains. Non-state actors gaining power, cyber warfare raising prominence in between countries. However, basic motives of war remains the same. Apart from other committees, The First General Assembly Disarmament and International Security Committee focuses on disarmament, global challenges and threats to peace that affect the international community and looks for solutions to the difficulties in the international security regime. Therefore, your duty is crucially important when it comes to peace, security and most importantly human life and its standards. I kindly urge you to promote peace and show what is cyber-warfare and how to eliminate or prevent it. During the conference, widen your perspectives of creativity in coming up with new methods of preventing mishaps in this particular subject. Attending this precious conference is only one tiny step in your path of developing analytical and practical intelligence. I advise you to use your time wisely and come up with magnificent solutions and not to be mediocre. I would like to thank the people that matters the most to me when it comes to this splendid conference. Bulut Vize, Efe Coştu, academic team and organization team. Last but not least, my dear hardworking academic assistants, Bora GEDİKLİ and Aruzhan AİSİNA for their efforts. If you have any questions, please do not hesitate to contact me via ahmetardataskirec@gmail.com

Best regards,

Ahmet Arda Taşkireç

Under-Secretary-General of GA-1 DISEC

INTRODUCTION TO GA-1 DISEC

United Nations General Assembly’s First Committee, DISEC, is one of the most important and central bodies of the United Nations. The First Committee deals with the issues that are related to disarmament problems, international security on a global scale and security problems threatening the national and international peace. The committee considers all of the disarmament and international security problems within the scope of the UN 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.

The aim of the committee is to maintain international peace and security with the actions taken by the member states. These actions can be either internal or external actions that are generally ordered by reports with suggestions like reducing the firepower in specific conflict zones or operations. Since DISEC is a General Assembly Committee, its power to take decisions is restricted. The most powerful authority is to inform and provide necessary establishments or authorities about agenda item-related events and operations.

Agenda Item: How to Prevent Cyber Warfare

As being one of the most prevalent topics of discussion owing to the abundance of cyber attacks that peril sustainable development and overall stability of countries, cyber warfare ensures the United Nations' acknowledgement upon the efforts of GA-1 DISEC. Henceforth, General Assembly First Committee shall focus predominantly on securing critical cyber infrastructure and information and communications technologies (ICTs) that occupy a prominent proportion of our lives. Two leading heads of the problem are striking and intriguing. First one is the escalation of cyber warfare and the second one is terrorist and criminal activities in cyber space. Terrorist groups and organizations are actualizing their criminal activities directed to critical infrastructure such as financial services, water and energy systems, hospitals and the other organizations and institutions. Furthermore, these terrorist organizations utilize cyber sphere to make their massages, points and motives known by civilians and mobilize human and financial resources. The act of cyber terrorism is mostly distinguished by the motives of the groups. It is usually undertaken with the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to force or intimidate a government or a specific population. To give some detailed insights to the subject, In 2015, the United States Office of Personnel Management was hacked and that act resulted in over 20 million government employees' sensitive information leakage together with a significant amount of confidential information about intelligence community officials. Whilst government officials and experts have declared press that the evidence indicates that the Chinese government was responsible for this breach, the US government has not made an official statement on participation of Chinese government, and Chinese state media has refused any allegation regarding government involvement in the hacks, declaring it was attempted by criminals within China. The number of the hacks against businesses around the world have also been identified, perpetrated by groups ranging from underground hacking collectives like Anonymous, to cyber-wings of military organizations such as the Syrian Electronic Army or ISIL. The objective of these hacks has been to steal or government secrets, cripple infrastructure, or co-opt communications systems, which angers corporations and governments wishing to protect their interests, their information, and their security.

Definition of the Key Concepts

O Cyber-security : Cyber security refers to the body of technologies, processes, and practices designed to secure networks, programs, devices, and data from damage, attack, or unauthorized access. Cyber security can also be defined as information technology security.

O Cyber-attacks : An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information (NIST, 2019).

O Cyber-crime : Cybercrime, also known as computer crime, the use of a computer as an instrument in intention of further illegal ends, such as trafficking in child pornography, and intellectual property, committing fraud, stealing identities, or violating privacy. Cybercrime, especially through the Internet, has gained importance as the computer has become central to commerce, entertainment, and government (Britannica, 2019).

O Cyber- defence : Cyberwar, also known as cyber war, also spelled as cyberwarfare or cyber warfare, war conducted in and from computers and the networks connecting them, waged by states or their proxies against other states. Cyberwar is generally waged against government and military networks in order to disrupt, destroy, or deny their use. Cyberwar should not be confused with the terrorist use of cyberspace or with cyberespionage or cybercrime. Even though similar tactics are used in all four types of activities, it is a misinterpretation to define them all as cyberwar. Some states that have engaged in cyberwar may also have engaged in disruptive activities such as cyberespionage, but such activities in themselves do not constitute cyberwar (Britannica, 2016).

NATO Policy on Cyber Defence

Cyber threats to the security of the Alliance are quite complex, coercive and destructive , and are becoming ever more frequent. NATO will move on to adapt to the evolving cyber threat landscape. NATO and its Allies depend on sustainable and resilient cyber defences to fulfil the Alliance’s core mission of collective defence, crisis management and cooperative security. The Alliance needs to be prepared to defend its networks and operations against the growing sophistication of the cyber threats and attacks it faces.

- Cyber defence is part of NATO’s core task of collective defence.
- NATO has affirmed that international law applies in cyberspace.
- NATO's main focus in cyber defence is to protect its own networks (including operations and missions) and enhance resilience across the Alliance.
- In July 2016, Allies reaffirmed NATO’s defensive mandate and recognised cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea.
- Allies also made a Cyber Defence Pledge in July 2016 to enhance their cyber defences, as a matter of priority. Since then, all Allies have upgraded their cyber defences.
- NATO reinforces its capabilities for cyber education, training and exercises.

- Allies are committed to enhancing information-sharing and mutual assistance in preventing, mitigating and recovering from cyber-attacks.
- NATO Cyber Rapid Reaction teams are on standby to assist Allies, 24 hours a day, if requested and approved.
- At the Brussels Summit in 2018, Allies agreed to set up a new Cyberspace Operations Centre as part of NATO's strengthened Command Structure. They also agreed that NATO can draw on national cyber capabilities for its missions and operations.
- In February 2019, Allies endorsed a NATO guide that sets out a number of tools to further strengthen NATO's ability to respond to significant malicious cyber activities.
- NATO and the European Union (EU) are cooperating through a Technical Arrangement on Cyber Defence, which was signed in February 2016. In light of common challenges, NATO and the EU are strengthening their cooperation on cyber defence, notably in the areas of information exchange, training, research and exercises.
- NATO is intensifying its cooperation with industry through the NATO Industry Cyber Partnership.
- NATO recognises that its Allies stand to benefit from a norms-based, predictable and secure cyberspace.
- At the Brussels Summit in 2021, Allies endorsed a new Comprehensive Cyber Defence Policy, which supports NATO's core tasks and overall deterrence and defence posture to further enhance the Alliance's resilience(NATO, 2021).

Historical Background of the Topic

Cyberwarfare is the use of computer technology to sabotage a country's or organization's physical or electronic resources. Viruses, worms, malware, ransomware, and denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks have all been used to demonstrate this. We've seen a range of cyber warfare examples during the last 15 years. The first cyber incident that took part in the history books actually happened back in 2003 when the Chinese hackers hacked the US Naval Air Weapons Station China Lake. National security data, such as nuclear weapons experiment and design data, and stealth aircraft data, was hacked from Naval Air Weapons Station China Lake by Chinese hackers.

In 2005, Chinese hackers also hacked many US Army organs. In an operation labeled "Titan Rain," Chinese hackers hacked into US Department of Defense networks. They aimed after US defense contractors, and also the Army Information Systems Engineering Command, the Defense Information Systems Agency, the Naval Ocean Systems Center, and the US Army Space and Strategic Defense facility.

In May 2006 with the contribution of Russian spies and Chinese hackers started to hack the US Defence Systems again. The systems of the Department of State were hacked, and unknown foreign invaders downloaded terabytes of data. It would be a war crime if Chinese or Russian spies pulled up to the State Department, smashed the glass doors, tied up the guards, and spent the night hauling out filing cabinets. When it occurs online, though, we hardly notice. For the rest of 2006, Chinese and Russian hackers hacked NASA, NIPRNet, U.S. Naval War College and House of Commons. In addition to the hacking they also stole data, making them inaccessible for a few hours or a few days. These events can actually be considered the beginning of Cyber Warfare because after these events, Cyber War started to spread to countries other than the US. In 2007 the Estonian government was hacked and harassed by foreing intruders. The British Security Service, the French Prime Minister's Office, and Chancellor Merkel's office all complained to China about penetration into their official networks. Merkel proceeded so far as to raise the issue with China's president.

After 2007 many countries were hacked by different foreing hackers. However the main countries that hackers live in are located as China, Vietnam, Russia and surprisingly U.S.

One of the biggest cyber wars in 20 years is Edward Snowden leaking his own country's data. Currently, Edward Snowden is under the protection of the Russian Government. In addition to this, the other big event that has happened is the WikiLeaks event, which affected the whole world. WikiLeaks published 10 million documents between 2006 and 2016. This event could not be prevented in any way and went down in history as the biggest data leak in the world. Precautions that have been made for Cyber Warfare were first started by the U.S. Government One of the biggest cyber wars in 20 years is Edward Snowden leaking his own country's data. Currently, Edward Snowden is under the protection of the Russian Government. In addition to this, the other big event that has happened is the WikiLeaks event, which affected the whole world. WikiLeaks published 10 million documents between 2006 and 2016. This event could not be prevented in any way and went down in history as the biggest data leak in the world.

Precautions that have been made for Cyber Warfare were first started by the U.S. Government which is spending more than 100 million dollars to repair cyber damage and taking precautions for cyber warfare via using Cyber Defense systems back in April 7th 2009. After the repairing and improving cyber defense phase, for the very first time, lawmakers in the United States pushed for the establishment of a White House cybersecurity "czar" to massively increase the country's defenses against cyber-attacks, developing plans that would allow the government to set and enforce security standards for private business.

After the cyber war that happened against Estonia, NATO established the Cooperative Cyber Defence Centre of Excellence (CCD CoE) in Tallinn. That was the first precaution made by an International Organisation. The main reason was to enhance the organization's cyber defence capability. After these precautions every country started to take their own measures. The main measures that countries take are installing firewalls, ensuring endpoint protection and basically making the network safer with hiring a cyber defense member to the Ministry of Defense.

Role-Playing Countries and Blocks’ Positions

The sphere of international politics has historically been shaped by State actors, especially in security matters. The traditions of political realism have firmly consolidated the privileged position of States not only in conducting international politics but also in establishing the norms of international law. Even with the emergence of influential transnational actors from the private sector and civil society and their recognition as full-fledged participants in international relations by the latest neo theories of international relations they were still not considered as actors capable of formulating and consolidating the norms of international law for any of the areas. The emergence of new information technologies, which have entailed challenges to the security of states, has added new participants to the negotiating table on cyber norms and responsible behavior in cyberspace.

Over the past twenty years, States have made many attempts to reach a compromise on the issue of regulating the use of information and communication technologies (ICT), so the international community has been debating cyber security for the last two decades. It is noteworthy that initially ICTs were viewed from the point of view of new opportunities and innovations for the development of the country's potential and economy, while only a small handful of countries paid attention to the potential risks of the misuse of ICTs for military purposes to violate international peace and security. However, today the risks have turned into a harsh reality — States not only use technology for intelligence and military superiority but also commit illegal actions, the assessment of which is ambiguous from the point of view of the application of international law since the mechanism for this has not yet been developed. Nevertheless, this does not stop other States from threatening to use force in response to cyber-attacks. While the problems of reliable technical attribution of cyber-attacks have not been solved, we are seeing cases of political attribution of incidents. In early October, the UK's National Cyber Security Center issued a message providing information on the attribution of several cyberattacks, including on WADA and the US National Democratic Committee in 2016, as well as the OPCW in 2018, stating that with a "high degree of confidence" and "almost definitely" these attacks are related to the activities of the GRU. International support for such accusations in the form of official charges brought by the United States against seven GRU officers only aggravates the situation from the point of view of international security. Accusations based solely on indirect facts and political attribution of incidents, and the sanctions measures that follow them, create a dangerous precedent for world politics.

The United States of America

US President Joe Biden signed a decree to strengthen government cybersecurity, which, among other things, obliges IT, service providers, to report hacked systems to the authorities. The administration spokesman announced this on a teleconference at the White House on May 12, 2021.

The Pentagon's Cyber Strategy

At the end of April 2015, the Pentagon presented a new cybersecurity strategy, which was an expanded version of a similar document from 2011. There are three main areas of activity in this area:

The first is to protect your information systems from hacker attacks from the outside.

The second is working with other agencies and foreign allies to collect intelligence information, joint operations with the FBI, CIA, NSA, and foreign intelligence agencies up to the creation of an automatic information exchange system, as well as the creation of a special cybersecurity task force in the US Strategic Command.

The third area is cyber support for US military operations and the involvement of qualified civilian specialists.

The new document, unlike its predecessor, directly names the main opponents of the United States in cyber warfare: China, Russia, North Korea, and Iran. Moreover, non-state actors are also mentioned, such as hackers from ISIS (a terrorist organization banned in Russia - EADaily) and criminal syndicates.

At the same time, the strategic goals of the last cyber strategy from 2011 remain in force:

- creation and support of combat readiness of forces and the ability to conduct operations in cyberspace.

- ensuring the protection of military networks.

- strengthening interagency cooperation to counter cyber threats.

- strengthening international cooperation in the field of cybersecurity.

The financing of cyber units in the US army and special services will increase, the training of civilian specialists in this industry and their recruitment will be intensified, work will be carried out in this direction with NATO allies. It should be noted that the Americans, having designated China, Russia, Iran, and the DPRK as their opponents, thus officially recognized that cyber operations are being carried out against these states and will be carried out in the future. It is obvious that the United States, recognizing the effectiveness of the so-called "hybrid war", one of the elements of which is fighting in cyberspace, will increase efforts in this direction.

In July 2021, the NSA, the FBI, and the National Cyber Security Center of Great Britain published a report on the methods of hacker attacks in the last two years. The document says that the Main Directorate (GU, former GRU) of the General Staff of the Armed Forces, the 85th main Special Operations Center of the GU, as well as military unit 26165, are behind the cybercrimes.

American and British intelligence agencies claim that from 2019 to 2021, hackers used a combination of well-known tactics, methods, and procedures for hundreds of penetrations into the network infrastructures of government and private facilities. Hacker groups FancyBear, APT 28, and Strontium were called involved in the attacks. Thanks to their actions, according to the authors of the report, Russian intelligence gained access to accounts and classified information, including the correspondence.

The fight against cybercrime was discussed by the American and Russian presidents during a meeting in Geneva in June 2021. Before that, Vladimir Putin claimed that all of Washington's accusations of cyberwar are unfounded since they never contained any evidence.

Snowden’s Case

Edward Joseph Snowden is an American technical specialist and special agent, a former employee of the CIA and the US National Security Agency (NSA). At the beginning of June 2013, Snowden gave the newspapers The Guardian and The Washington Post classified information from the NSA regarding the total surveillance of information communications between citizens of many states around the world by the American intelligence services using existing information and communication networks, including information about the PRISM project, as well as X-Keyscore and Tempora. According to a secret Pentagon report, Snowden stole 1.7 million classified files, most of the documents referring to "vital operations of the US Army, Navy, Marine Corps, and Air Force". In this regard, in the United States on June 14, 2013, Snowden was charged in absentia with espionage and theft of state property. He was put on the international wanted list by the US authorities Soon he fled from the United States, first to Hong Kong, then to Russia, where he spent more than a month in the transit zone of the Sheremetyevo airport. On August 1, 2013, he received temporary asylum in the Russian Federation, a year later - a three-year residence permit, which in 2017 was extended until 2020, and in October 2020 he received an unlimited residence permit. Lives in Russia, his exact whereabouts were not disclosed for security reasons.

Snowden's revelations sparked heated debates about the permissibility of mass surveillance, the limits of state secrets, and the balance between personal data protection and national security in the post 9/11 era. By his actions, he revealed the secrets of the American secret services to the whole world and put the cyber security of the United States at risk. Therefore, the case of Snowden keeps relations between Russia and the United States in suspense

Germany

During the pandemic in Germany, the number of crimes committed on the Internet increased. 108,474 cybercrimes were registered in Germany in 2020. Such data are contained in the annual report of the German Federal Office for Criminal Affairs (BKA). This is almost 8% more than in 2019. At the same time, the number of unregistered crimes on the Network may be much "above average," says the expert of this department, Carsten Meywirth. Since April 2020, he has been heading a special department at BKA that investigates cybercrimes, the number of which is growing rapidly.

Germany, as one of the economic and innovation centers, is an attractive target for hackers from all over the world. Its geostrategic position also plays a role - in the very heart of Europe. "Influence in the EU and NATO membership makes Germany one of the main targets for cybercriminals," says Carsten Meiwirth.

He notes that during the pandemic, hackers had new goals: portals related to the production and distribution of vaccines, training platforms, servers that allow working in home office mode. Cybercriminals are particularly interested in the entire supply and distribution chain of coronavirus vaccines, because "if at least one enterprise involved in this fails, it will have huge consequences for society," says Maywirth.

Germany presented its first cybersecurity strategy in 2011. The second version of the cybersecurity strategy has been in effect since 2016. The Interdepartmental Cybersecurity

Strategy of 2021 sets out the directions of work for the next five years. That is, the new strategy is valid until 2026. The strategy contains four main principles:

1. Make cybersecurity a joint task of the state, business, society, and science.
2. Strengthen the digital sovereignty of the state, business, science, and society.
3. Make digitization safe.
4. Goals should be measurable and transparent.

The joint mandate of Germany's government and business :

13 strategic goals of the second line of action provide for strengthening cybersecurity in the economy as a whole. In addition to focusing on critical infrastructures, the failure or damage of which can lead to supply disruptions and, consequently, to a threat to public safety, small and medium-sized companies are also being considered. Cooperation between the state and business will continue here.

India

The onset of the pandemic in 2020 has led to increased reliance on technology, coupled with the wider adoption of interconnected devices and hybrid work environments. According to the Government of India, 1.16 million cybersecurity cases were reported in 2020, which is 3 times more than in the previous year.

The National Cyber Security Policy (NCSP) published by the Government of India in 2013, had established several strategies to counter security threats from cyberspace. The lack of a comprehensive cybersecurity strategy/policy is flashy and raising vulnerability.

The Government of India has already shared its vision to ensure safe, reliable, resilient, vibrant, and trusted cyberspace, through a new strategy that would serve as a guideline to control data as a national resource, build indigenous capabilities, and for cyber audits.

Russia

Russia has been promoting a global cybercrime treaty for at least a decade, presumably to replace the Budapest Convention, a treaty developed by the Council of Europe that opened for signatories in 2001 and entered into force in 2004. Since then, 65 countries have ratified it, including governments in other regions. Russia has not joined, even though it is a Council of Europe member. While it is sometimes referred to as the “gold standard” because it is the most comprehensive multilateral cybercrime treaty, human rights experts have long criticized it for not having stronger safeguards for human rights.

Russia and the United States have submitted a resolution to the UN on responsible behavior in cyberspace. Andrey Krutskikh, Director of the Department of International Information Security of the Russian Foreign Ministry, said during the presentation of the resolution during informal UN consultations that it was a "historic moment". He stressed that this document is important not only in terms of content, ut also in strategic terms since its adoption could put an end to the period of operation of two sites dealing with cybersecurity issues in the UN.

Now, a Group of Governmental Experts (GGE), supported by Washington, and an Open-ended Working Group (OEWG), functioning on the initiative of Moscow, are working out rules of conduct in cyberspace within the framework of the UN.

Earlier, Microsoft experts reported that more than half of the detected cyberattacks sponsored by states were carried out from Russia. According to their data, hackers from Russia were behind 58 percent of such attacks. It is noted that most often "Russian hackers" attacked the United States, Ukraine, the United Kingdom, and the European states that are members of NATO.

Russia's position is to promote the adoption of norms of international law prohibiting cyber weapons so that countries are deprived of legal grounds for using the right to self-defense in the event of a cyber-attack. The United States does not believe that Russia is not developing its military potential. Numerous accusations of cyber-attacks against Moscow are linked precisely to the activities of Russian military departments with the GRU

The Questions Resolution Should Cover

How the operations in cyber space can be regulated?
What measures can be taken in order to strengthen global cyber-security?
In which parameters disarmament in cyber-warfare can be achieved?
In which steps of regulations limited armament in cyber-warfare can be achieved?

REFERENCES

Developments in the field of information and telecommunications in the context of international security (2017), *UNODA.*

Unexpectedly, All UN Countries Agreed on a Cybersecurity Report. So What? (2021, March 18). *The Council on Foreign Relations (CFR)*.

Brown, D. (2021, August 13). *Cybercrime Is Dangerous, But a New UN Treaty Could Be Worse for Rights*. Retrieved from https://www.hrw.org/node/379677/printable/print.

Nato. (2021, July 19). *Cyber defence*. NATO. Retrieved November 13, 2021, from https://www.nato.int/cps/en/natohq/topics_78170.htm.

Sheldon, J. B. (2016, May 25). cyberwar. Encyclopedia Britannica.

https://www.britannica.com/topic/cyberwar

Dennis, M. Aaron (2019, September 19). cybercrime. Encyclopedia Britannica.

https://www.britannica.com/topic/cybercrime