Disarmament and International Security

Preventing cyber attacks on governments and personal data

Approved by president of the general assembly

Letter from the President of the General Assembly

In the words of George Monbiot " The only thing that can replace a story is a story ", After The financial crisis of 2008, a lot of us have been left wondering what's next, who is the hero that defeated the villain and who is this mysterious figure that is going to lead us into the modernization era. Now for us, it seems that the recently defeated neo-liberalism is an immortal ideology that's never going to leave and is the only way to progress into modernization, but with the rise of a new generation, a generation that grew up under a fragile economy, decays long disputes, and safety threats even within their own homes because of unauthorized weaponry, this idea of immortalization is slowly but surely starting to fade away. This generation is determined to get results no matter what it takes. They have made it their long life goal to resolve decays of dispute in hopes of finding the peace and prosperity they have never gotten the chance to taste and are keen on building a world where we prevent making the same mistakes like the ones we inherited.

Here we invite you to join us in creating our own story engraved with equality, equity, justice and peace where everyone's voice matters.

Mohamad Hachem
PGA of SafirMUN

Introduction:

Cyber Attacks has been one of the main concerns of the nations. And this regards all of the major countries as well. The unclear power and limits of the Internet and Information. Technology makes it harder to defend against. That is why GA:1 DISEC committee is gathering up to solve this crucial issue. Cyber Attacks can cause information breaches, exploitation of people and even bank heists. Information breaches could be identity theft of an individual or leak of a governmental secret document to the public. On the other hand, attacks done to individuals could be devastating as well. Exposing and blackmailing are the most common ways of exploiting the stolen information from a person. There has been five resolutions regarding the issue being: Resolution 55/63, January 2001 Resolution 55/63, January 2002 - Combating the criminal misuse of information Technologies, Resolution 57/239, January 2003-Creation of a global culture of cybersecurity Resolution 58/199, January 2004 - Creation of a global culture of cybersecurity and the protection of critical information infrastructures Resolution 64/211, March 2010 - Creation of a global culture of cyber-security and taking stock of national efforts to protect critical information infrastructures. Possible solutions are creating a global fund to prevent any attacks aiming towards the people, establishing a worldwide security system to all governmental organizations to use in order to protect the information of masses.

Key Vocabulary

Cyberattack – A sequence of actions that lead to the violation of the security policy. This violation often takes the form of a computer system or network malfunction (inability to connect, a service that is no longer available, or data being encrypted using ransomware). A cyberattack can also be invisible, but lead to serious consequences, such as the theft of confidential information.

Cyber range – A training platform for cyberattacks and defense.

Distributed Denial of Service Attack– An attack aimed at overloading a service provider's resources (often related to the network), making it inaccessible.

Electromagnetic injection – An electromagnetic signal sent to disrupt the operation of an electronic component (processor, memory, chip card...).

Firewall – A network component that filters incoming and outgoing traffic on a website.

Project Google Zero – A Google project aimed at finding new vulnerabilities in software.

Krack – Attacks against the WPA2 protocol that allow an attacker to force the reuse of an encryption key. This allows the attacker to collect a large number of packets, and therefore decrypt the network traffic more easily, without knowing the key.

Malware – A program used for a purpose that is inconsistent with the user's expectations and violates the security policy. Malware often uses vulnerabilities to enter a system.

Phishing – A social engineering technique, in which an attacker convinces a victim to act without understanding the consequences. The technique often relies on emails with fraudulent content (e.g. CEO fraud scams).

Ransomware – Malicious software (malware) aimed at extorting money from a victim, often by encrypting the data on their computer's hard disk and demanding payment in exchange for the decryption key (often these keys are useless, and purchasing them is therefore useless).

Trojan Horse – A backdoor installed on a system without the users' and administrators' knowledge, which allows a hacker to regularly and easily connect to the system without being seen.

Virus – Malicious software capable of entering a system and spreading to infect other systems.

Some Countries and Their Policies Against Cyber Attacks

a. France

France is an important international and European actor. It is a member of NATO, the European Union and a permanent member of the United Nations Security Council. It also works closely on cybersecurity issues with bilateral partners such as the United Kingdom and Germany. France wants to position itself as an international power in cybersecurity. This is despite the fact that offensive cyber capabilities are rarely mentioned in cyberdefense strategies and national cybersecurity is mainly lead by the civilian entities and focused primarily on resilience.

i. Key policy principles

Cybersecurity The French Cybersecurity Strategy has a broader perspective than purely cybersecurity issues by being named as the National Digital Security Strategy. It encompasses technical issues and cybercrime but also propaganda and "influence campaigns" led through cyberspace against France's population. The French National Cybersecurity Agency (ANSSI) is the lead agency for the civilian side of cybersecurity. **Cyberdefense**The French Cyber Defense Strategy focuses mainly on defensive measures by improving robustness and resilience. The Ministry of Defense (MoD) is the lead entity and is also responsible for the cybersecurity of its own information systems and networks.

ii. Level of partnership and resources

France cooperates on cybersecurity issues with its allies within NATO and the EU, but also wants to cooperate more closely with the UK and Germany on issues of cybersecurity. The strategies do not describe any public-private partnership, but the ANSSI is the main actor to set cybersecurity standards and to make sure that operators of critical infrastructures meet these standards.

b. Germany

Germany is an important international economic actor and is developing an international presence in both cybersecurity and cyberdefense, primarily from a soft power perspective. This is being developed within the framework of its leadership position in the EU as well as its cooperation with partnerships such as NATO. In terms of specific cybersecurity and cyberdefense frameworks, Germany is undergoing a period of centralization, with the policy development and leadership role being taken up by the Federal Ministry of the Interior (BMI) in cybersecurity, and the Ministry of Defense leading in cyberdefense. Germany is making statements about developing offensive cyber-capabilities under the aegis of its Ministry of Defense, but the lack of open-source data on these capabilities and the fact that overall strategic leadership sits with a civilian entity means that cybersecurity and cyberdefense remain predominantly civilian, socio-economic policy areas.

i. **Key policy principles**

Cybersecurity, Germany is adopting a holistic approach to cybersecurity.

Although the BMI leads from a policy-development perspective, operational responsibility is delegated to a dedicated set of agencies and offices from the intelligence community, law enforcement and public- private liaison. Bringing these bodies under the aegis of the BMI is intended to address issues of fragmentation by centralizing oversight and overall responsibility**.**
Cyberdefense Germany defines cyberspace as the "cyber and information space". While this definition is broad and potentially vague, it allows Germany to develop responses to a variety of current international cyber-threats. These include "traditional" cyberthreats such as damage or destruction to critical physical and information infrastructures, but also hybrid warfare, advanced persistent
threats, state and non-state cyber-terrorism and media and popular online manipulation. Germany's cyberdefense posture also involves the development of offensive cyber capabilities as well as publicly stating the readiness to deploy these capabilities should the need arise.

ii. **Level of partnership and resources**

Germany co-operates with core allies such as NATO and the EU in order to increase cybersecurity internationally. It is actively engaged in developing EU cybersecurity through promoting core legislation and cooperation mechanisms as well as advocating for the development of security standards and rules for vital sectors and key digital service providers. In cyberdefense Germany is an active member of the NATO Cooperative Cyberdefense Center of Excellence in Tallinn.

iii. **White Paper on German Security Policy and the Future of the**

Bundeswehr 2016

The most recent document which sets out German national security policy is the White Paper on German Security Policy and the Future of the Bundeswehr 2016. This White Paper lists a number of cyber and information domain risks directly below transnational terrorism as one of the main threats to German security. This is a marked contrast to the previous White Paper of 2006 which only mentioned cyberspace once as a potential target for and source of criminal activities, terrorism, and military attacks. Cybersecurity issues have therefore gone up the prioritization ladder in the ten years to 2016, to the extent that they are considered a major threat to national security.

c. The United Kingdom

The UK is an important international actor in cybersecurity and cyberdefense. It works closely with US, NATO and European allies and is able to project both hard and soft power. The UK has placed cyber risks as a high national security priority, including the protection of digital infrastructures. That being the case, the UK Cabinet Office – a civilian organ of the UK government – is the lead authority in UK cybersecurity policy.

i. **Key policy principles**

Cybersecurity Cybersecurity for the UK means ensuring that the economic and social opportunities afforded by cyberspace are available to all with a minimum risk to corporate, personal/citizen and national interests. Cybersecurity policy encompasses civilian, criminal justice and military/defense considerations. This solidifies the UK's civilian-led cyber policy while still addressing latent cyber risks and ensuring the UK retains its position as a leading digital nation. **Cyberdefense** The UK does not have a dedicated or separate cyberdefense policy. Cyberdefense issues are addressed in the UK's cybersecurity strategy, with input from the National Security Strategy. As such the core cyberdefense principles are the protection of UK interests at home and abroad, but within a civilian cybersecurity-led policy framework. That being said, the UK has established a National Offensive Cyber Program to develop offensive capabilities. Because this Program establishes such capabilities within a deterrence framework, the UK's posture in cyberdefense can still be considered defensive rather than offensive.

ii. **Level of partnership and resources**

The UK co-operates with core international allies such as NATO, the EU and the US and is a member of the Five Eyes intelligence-sharing partnership with the US, Canada, Australia and New Zealand. The UK actively promotes private sector partnership and involvement in cybersecurity (and by extension cyberdefense) provision, to the extent that it recognizes in policy that a significant portion of the UK's cybersecurity and defense tools and measures will be owned and operated by the private sector. There is, however, little specific detail provided regarding oversight or action.

9. Timeline of events

January 2018. The Unique Identification Authority of India and its Aadhaar system are hacked by unknown actors, resulting in the personal data of more than 1 billion people being available for purchase.

January 2018. A Japan-based cryptocurrency exchange reveals that it lost $530 million worth of the cryptocurrency NEM in a hack, in what amounts to possibly the largest cryptocurrency heist of all time.

January 2018. China denied that the computer network it supplied to the African Union allowed it access the AU's confidential information and transfer it to China, or that it had bugged offices in the AU headquarters that it had built.

February 2018. A cyberattack on the Pyeongchang Olympic Games attributed to Russia took the official Olympic website offline for 12 hours and disrupted wifi and televisions at the Pyeongchang Olympic stadium.

February 2018. The US and UK formally blame Russia for the June 2017 NotPetya ransomware attack that caused billions of dollars in damages across the world.

February 2018. German news reported that a Russian hacking group had breached the online networks of Germany's foreign and interior ministries, exfiltrating at least 17 gigabytes of data in an intrusion that went undetected for a year.

March 2018. A UN report details attempts by North Korean hackers to compromise email accounts of the members of a UN panel enforcing trade sanctions against North Korea.

March 2018. Cybersecurity researchers announce evidence that the same North Korean hacking group linked to the SWIFT financial network attacks has been targeting several major Turkish banks and government finance agencies.

April 2018. Israeli cyber researchers revealed that Hamas had planted spyware in mobile phones owned by members of Fatah, a rival Palestinian faction

May 2018. Researchers reveal that a hacking group connected to Russian intelligence services had been conducting reconnaissance on the business and ICS networks of electric utilities in the US and UK since May 2017.

May 2018. Within 24 hours of President Trump's announcement that the US would withdraw from the Iran nuclear agreement, security firms reported increases in Iranian hacking activity, including the sending of emails containing malware to diplomats in the Foreign Affairs ministries of US allies, as well as global telecommunication companies.

May 2018. Turkish government hackers were discovered to be using surveillance software FinFisher to infect Turkish dissidents and protesters.

June 2018. Chinese hackers were found to be engaged in a cyber espionage campaign to collect data from satellite, telecom, and defense organizations in the U.S. and Southeast Asia.

June 2018. Ukraine police claim that Russian hackers have been systematically targeting Ukrainian banks, energy companies, and other organizations to establish backdoors in preparation for a wide-scale strike against the country.

July 2018. Security researchers report that Chinese hackers had been actively spying on political actors on both sides of the upcoming Cambodian elections. Targets include the country's National Election Commission, several government ministries, the Cambodian Senate, at least one Member of Parliament, and multiple media outlets and human rights activists.

July 2018. Russian hackers were found to have targeted the Italian navy with malware designed to insert a backdoor into infected networks.

July 2018. Security researchers report that an Iranian hacking group had been targeting the industrial control systems of electric utility companies in the U.S., Europe, East Asia, and the Middle East.

August 2018. Microsoft announces that Russian hackers had targeted U.S. Senators and conservative think tanks are critical of Russia.

August 2018. Facebook identified multiple new disinformation campaigns on its platform

sponsored by groups in Russia and Iran. The campaigns targeted users in the U.S., Latin America, Britain, and the Middle East, and involved 652 fake accounts, pages, and groups.

August 2018. North Korean hackers stole $13.5 million from India's Cosmos Bank after breaking into the bank's system and authorizing thousands of unauthorized ATM withdrawals, as well as several illegal money transfers through the SWIFT financial network.

September 2018. Security researchers find that Iranian hackers have been surveilling Iranian citizens since 2016 as part of a mobile spyware campaign directed at ISIS supporters and members of the Kurdish ethnic group.

September 2018. Security researchers found that a Russian hacking group had used malware to target the firmware of computers at government institutions in the Balkans and in Central and Eastern Europe.

October 2018. The Security Service of Ukraine announced that a Russian group had carried out an attempted hack on the information and telecommunication systems of Ukrainian government groups

October 2018. News reports reveal that the Israel Defense Force requested that cybersecurity companies develop proposals for monitoring the personal correspondence of social media users.

October 2018. Media reports state that U.S. agencies warned President Trump that China and Russia eavesdropped on calls made from an unsecured phone.

October 2018. The head of Iran's civil defense agency announced that the country had recently neutralized a new, more sophisticated version of Stuxnet

November 2018. The Pakistani Air Force was revealed to have been targeted by nation-state hackers with access to zero-day exploits

November 2018. Researchers discover that a Chinese cyberespionage group targeted a UK engineering company using techniques associated with Russia- linked groups in an attempt to avoid attribution

November 2018. Security researchers report that Russian hackers impersonating U.S. State Department officials attempted to gain access to the computer systems of military and law enforcement agencies, defense contractors, and media companies

November 2018. Chinese state media reports that the country had been the victim of multiple attacks by foreign hackers in 2018, including the theft of confidential emails, utility design plans, lists of army units, and more

November 2018. German security officials announced that a Russia-linked group had targeted the email accounts of several members of the German parliament, as well as the German military and several embassies

December 2018. Italian oil company Saipem was targeted by hackers utilizing a modified version of the Shamoon virus, taking down hundreds of the company's servers and personal computers in the UAE, Saudi Arabia, Scotland, and India

December 2018. Researchers report that a state-sponsored Middle Eastern hacking group had targeted telecommunications companies, government embassies, and a Russian oil company located across Pakistan, Russia, Saudi Arabia, Turkey, and North America

December 2018. U.S. Navy officials report that Chinese hackers had repeatedly stolen information from Navy contractors including ship maintenance data and missile plans.

December 2018. Chinese hackers were found to have compromised the EU's communications systems, maintaining access to sensitive diplomatic cables for several years
December 2018. North Korean hackers targeted the Chilean interbank network after tricking an employee into installing malware over the course of a fake job interview.

11. **Bibliography**

https://www.cyberdefensemagazine.com/cyber-attacks-the-biggest-threat-for-future-weapons/

https://www.diplomacy.edu/blog/cyber-armament-growing-trend-part-i

https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity

https://www.transunion.com/blog/identity-protection/why-is-cyber-security-important

tps://www.hackmageddon.com/category/security/cyber-attacks-statistics/

https://www.kramerlevin.com/en/perspectives-search/the-evolution-of-cybersecurity.html

https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

https://us.norton.com/internetsecurity-privacy-data-breaches-what-you-need-to-know.html

https://blogrecherche.wp.imt.fr/en/2018/03/20/24-words-understanding-cybersecurity/

https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

https://www.cnbc.com/2018/11/12/cyber-attacks-and-weak-government-among-biggest-risks-to-firms-wef.html

https://www.diplomaticourier.com/posts/implications-cyber-attacks-governments

https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

https://insight.kellogg.northwestern.edu/article/how-governments-can-better-defend-themselves-against-cyberattacks

https://foreignpolicy.com/tag/cyberattacks/

https://www.amrita.edu/center/Cyber%20Security/projects/all