



United Nations Security Council

February 2024

Head Chair: Tatiana Chen

Co-Chair: Laís Taranto





LETTER FROM THE DAIS

Dear Delegates of the Security Council,

We would like to welcome you all to the United Nations Security Council (UNSC) and express our contentment with the opportunity to chair this grand committee. Moreover, we hope to use this second edition of MinasMUN to its full potential and learn the absolute most from it.

The UNSC being one of the most critical and accountable committees in the UN, it is critical that delegates make use of documents such as the UN Charter to work towards collective international peace. Furthermore, the topics of discussion are particularly relevant for the Security Council as it models after topics that the committee is currently discussing in real life.

As usual, feel free to reach out if you have any questions or concerns whatsoever. We look forward to assisting and guiding you through UN procedures.

Tatiana Chen

tatianachen12@gmail.com

Laís Taranto

laisotaranto@gmail.com

COMMITTEE DESCRIPTION



The United Nations Security Council (UNSC) is one of the six main organs of the United Nations responsible for international peace and security. Established in 1946, the Security Council officially has fifteen members, five being permanent (China, France, Russia, the United States of America, and the United Kingdom). The council, located in the New York Headquarters, is the only committee that can obligate member states to follow resolutions, unlike the other committees that are advisory. Therefore, its resolutions can be thought of as firm enforcements to the UN Member States since they ultimately lead governments to adopt legislation in line with the council's final decisions. Furthermore, besides its five permanent members with veto power due to their participation in the founding of the UN, the UN General Assembly elects ten non-permanent members for terms— typically two years.

Topic A: Addressing the Israel and Palestine Conflict




BACKGROUND INFORMATION

Introduction

On October 7, 2023, the armed militant group *Hamas* stormed the border of Gaza, Palestine, into The State of Israel, killing 1,200 people and abducting 250 Israelis and immigrant workers as hostages. While this initiated the ongoing Israel-Hamas war, the story behind the turbulent attack begins in the history of the establishment of a Jewish state. When the Ottoman Empire collapsed at the end of World War I, the League of Nations granted Britain administration of Palestine which demonstrated full support in establishing an official Jewish state alongside the Allies of WW1: USA, France, Italy, Japan, etc. Although Palestine had already been a religiously diverse location due to its religious significance to both Jews and Arabs, the drastic increase of Jewish influx into the region during WWI sparked a violent conflict. On May 14, 1948, the head of the Jewish Agency officially declared Israel an official state recognized by key world powers soon after, ceasing the British Mandate.

1. Arab-Israeli Wars

From 1948-49, many neighboring Arab countries to Israel were outraged by the establishment of a Jewish state on Palestinian land and spurred into the first Arab-Israeli War, later followed by five other wars between Israeli military powers and multiple Arab forces. With a series of back-and-forth attacks displacing thousands of Israelis and Arabs, known as the War for Independence in Israel but the Nakba (Catastrophe) in the Arab world. The Six-Day War, which took place in 1967, was a brief but impactful conflict between Israel and several Arab states, including Egypt, Jordan, and Syria. Sparked by regional tensions and disputes over borders, the war resulted in a decisive Israeli victory, leading to significant territorial changes, including Israel's occupation of the Sinai Peninsula, the West Bank, East Jerusalem, and the Golan Heights. The Yom Kippur War, from October 6 to October 25, 1973, was a conflict between Israel, Egypt, and Syria. Launched on the holiest day in Judaism, Yom Kippur, the surprise attack initially posed



a significant threat to Israel, but through intense battles and international mediation, Israel managed to regain the initiative, leading to a ceasefire and territorial changes.

2. Israeli State Expansion

The territory that Israel was given, split equal with The State of Palestine, has slowly expanded over time through settlements in the West Bank and in the East of Jerusalem. These settlements, constructed on Palestinian land occupied since the Six-Day War, receive support and funding from the Israeli government. Characterized by suburban-style housing, schools, and malls hinder the creation of a contiguous Palestinian state. This growth has undermined the viability of a two-state solution as despite its illegality according to Article 49 of the Fourth Geneva Convention, the settlements continue to grow and contribute to Israeli-Palestinian conflicts which complicate its efforts to achieve a lasting peace agreement. The Israeli government has funded the settlements to function as a buffer in Palestinian movement and imposed checkpoints in the occupied land, affecting Palestinian movement while settler violence has displaced over 1,000 Palestinians in the past two years.

3. October 7th Attack

Named one of the deadliest days of the Jews since the Holocaust, militant group *Hamas* caused global ramifications with fatalities and hostages on October 7th. Firing thousands of rockets, the gunmen killed 1,200 people which included children and elderly in a raided music festival. Hamas is known to have captured over 100 hostages, keeping them in the Gaza Strip, and has been releasing them in portions with deals between Israel and the militant group. These deals were mediated by Qatar who became a crucial piece in the return of Palestinian women and teens in Israeli prisons. However, despite these non-violent exchanges taking place, the Israeli Defense Force has notably been firing at Gaza, allegedly aiming at locations suspected to contain members of Hamas. 9,000 soldiers of the group have been killed according to the Israel Defense

Forces, however far more than 26,000 civilians have died as a result of the mass bombings throughout the strip of Palestinian land.

4. Harakat al-Muqawama al-Islamiya (Hamas)

Harakat al-Muqawama al-Islamiya is an Islamist movement and a political party of Palestine. The militant group came into power through an election that occurred in 2006, campaigning as an armed resistance to Israeli oppression. While many countries have officially named Hamas a terrorist organization, many other countries condemn their actions while demonstrating sympathy for the motives behind the terror on October 7th. Hamas was founded by Sheikh Ahmed Yassin, a Palestinian cleric who established the organization in the 1960s and preached charitable work in the West Bank and Gaza, two occupied territories after the Six-Day War. In 1988, Hamas published a charter that officially declared their calling for an Islamic society above Israel. The organization has a seemingly wide web with other Islamic states having a history of operating in Syria, Turkey, Qatar, and Egypt, alongside their funding coming from Islamic charities and private donors in the Persian Gulf.

5. Humanitarian Aid and the Rafah Crossing

Israel exerts control over Palestine's resources and the Rafah Crossing through various means: blockade on the flow of goods and materials into the territory from outside along with the complete control over the state's airspace and maritime borders, limiting the movement of people and goods in and out of Gaza. Israel has a significant military presence along the border of Gaza and Rafah, Egypt enforcing strict security measures. The Rafah crossing is the primary gateway to Egypt and is heavily influenced by the agreements between Israel and Egypt. Recently, humanitarian aid from the international community has been blocked at the Rafah Border for two main reasons: attempting to maintain the Palestinian land by resisting the emigration of residents along with Israel keeping a firm grip on Hamas members.



6. Israel Defense Forces

The State of Israel's armed forces, known as the Israel Defense Forces (IDF), are in charge of maintaining the security and defense of the nation. Because the IDF is a conscription-based military, all eligible Israeli citizens must enlist, with mandatory duty beginning at age 18. The IDF, which consists of: ground forces, air forces, and naval forces, is renowned for its cutting-edge military prowess. The national military also has specialized combat units, elite forces, and intelligence divisions. Recent efforts to raise the number of combat soldiers in the IDF amid continuous geopolitical tensions serve as an example of the vital role the force plays in defending Israel's borders and responding to security concerns.

RELEVANT WORKS

Balfour Declaration of 1917

The Balfour Declaration of 1917 is a statement issued by the British government expressing support for establishing a "national home for the Jewish people" in Palestine. It conveyed in a letter from British Foreign Secretary Arthur Balfour to Lord Rothschild, a prominent figure in the British Jewish community. The declaration played a significant role in paving the way for establishing the State of Israel. However, it also generated controversy, contributing to tensions between Jewish and Arab communities in the region.

October 30, 2023 UNSC Meeting on the Situation in the Middle East + Article 33 of the Geneva Convention (IV) on Civilians, 1949

The Security Council meeting on the Middle East highlighted urgent calls for a ceasefire, particularly due to Israel's intensified offensive in the Gaza Strip following the October 7th attacks by Hamas. Speakers emphasized that civilians in Gaza should not be subject to collective punishment, condemning the shocking bombardment by the IDF. UN officials described the unprecedented destruction, forced displacement, and dire humanitarian conditions, including widespread casualties among children. The situation raised concerns about violations of Article 33 of the Geneva Convention, which prohibits collective punishment. Along with calls for a ceasefire, the Council faced challenges, with members defending Israel's right to self-defense and others criticizing the perceived inaction and one-sided resolutions— which resulted in various vetoes by the P5 nations.

Iron Dome

The Iron Dome is an Israeli missile defense system designed to intercept and destroy short-range rockets and artillery. It safeguards Israeli civilians and infrastructure by using advanced radar and interceptor missiles to neutralize incoming threats. The system has received international



support, notably from the United States, highlighting the strategic cooperation between the nations for regional security.

KEY TERMS

Anti-Semitism

Anti-Semitism is a form of prejudice or discrimination against those of Jewish descent both ethnically and religiously, often rooted in historical stereotypes and misconceptions. It manifests in various ways such as: verbal attacks, vandalism, and even violence towards individuals or institutions that are associated with Judaism. Throughout history, anti-Semitism has led to a long history of violence most notably genocide during the Holocaust (WWII).


Zionism

Zionism is the political and ideological movement that advocates for the establishment and support of a Jewish homeland. Rooted in the belief of Jewish self-determination and national identity, Zionism emerged in the 19th century as a response to growing anti-Semitism and a solution that was favored by those who supported the Jewish *and* those who were against them. However, it remains a topic of debate due to its implications for Palestinian rights, territorial disputes, and past reemerging plans.

Genocide

Genocide refers to the systematic and deliberate extermination of a particular group based on ethnicity, nationality, religion, and etc. It involves acts such as mass killings, torture, displacement, and destruction of defining characteristics such as cultural heritage with the intent to eliminate the targeted group in its whole. A widely debated topic within the Israel-Palestine conflict is the use of the word “genocide” to describe the oppression of Palestinian people.

Self-Defense



Self-defense is the lawful use of force to protect oneself, one's property, or other rights from harm or imminent danger. It is a fundamental right recognized by both national and international law, allowing individuals or nations to defend against aggression or attack. The principle of self-defense extends to actions taken to prevent harm or injury when no other reasonable alternative is available. However, the use of force is widely agreed to must be proportionate to the threat faced, and efforts should be made to avoid causing unnecessary harm.

MAJOR DELEGATIONS

State of Palestine

The State of Palestine currently faces significant challenges both domestically and internationally, under the entire globe's spotlight with the recent drastic escalations to the ongoing conflict with Israel. The expansion of Israeli settlements in Palestine undermines the viability of a two-state solution, complicating efforts for a lasting peace agreement. The recent attack by Hamas on Israeli civilians has sparked global ramifications and heightened tensions internationally. Meanwhile, Israel's control over resources and movement in Palestine, particularly through measures like the blockade on the Rafah Crossing, further exacerbates humanitarian concerns and geopolitical tensions. There have been countless demonstrations of support and opposition, ranging from intergovernmental organizations to street marches in the United States and the United Kingdom. It is of great importance to acknowledge that Palestine does not have international recognition as a formal state and is solely an observer in the United Nations.

State of Israel

Israel is a nation born out of the aftermath of WWII and the Holocaust, leaving them to face complex challenges domestically and internationally regarding their right to self-determination and self-defense. In the United Nations, Israel faces criticism regarding its policies in Palestinian territories but actively participates in peacekeeping missions and various agencies. Efforts to counter resolutions are perceived as biased and often supported by allies: particularly the United States, highlighting their significant role in international affairs and military power. With lines between Zionism and anti-Semitism blurring in the conflict, Israel has been demonstrating its everlasting efforts to maintain a strong influence on its neighboring Arab countries and Western powers such as the US and UK. Despite Israel's current reputation, the state remains a crucial piece to the UN with strategic partnerships and development projects in partnership with other nations.



United States of America


The United States has maintained assertive and unwavering support for Israel since its inception, especially during the Cold War. President Joe Biden, like his predecessors, has pledged unwavering commitment to Israel in its conflict with Hamas. The relationship has faced criticism from progressive Democrats, and public sentiment in the U.S. has appeared to be shifting, showing a decline in sympathy for Israel. Despite challenges, the U.S. continues to provide substantial military aid to Israel, contributing to its survival and facilitating diplomatic successes in the region.

The United Kingdom

The United Kingdom holds a lot of historical significance in the Israel-Palestine conflict as the former colonial power in the region until 1948. The Balfour Declaration of 1917, issued by the UK, expressed support for a “national home for the Jewish people” in Palestine. Over the years, the UK has played a diplomatic role, participating in peace talks and advocating for a two-state solution. However, British Prime Minister Rishi Sunak has expressed eternal solidarity for Israel following the ongoing conflict with Hamas while visiting Israel and personally speaking with Benjamin Netanyahu. The two states also have very close military and commercial ties with collaborations in military training and arms sales.

Islamic Republic of Iran

While Iran has endlessly demonstrated support for Hamas politically, financially, and with military training, it officially denies arming the group despite the fingers pointing at their partnership in the October 7 attacks. Iran considers Israel an adversary, often expressing anti-Israel sentiments, but it hasn't directly engaged in a war with Israel. The recent conflict in



Gaza has raised tensions between the two states, and while Iran supports Hamas, it is unlikely to initiate a full-scale war with Israel.

Kingdom of Saudi Arabia

In strong support of Palestine currently, Saudi Arabia has had a longstanding support for the state throughout all of its history. The wealthy country has challenged its talks with Israel after Crown Prince Mohammad bin Salman called for a halt in arms exports to Israel. Despite historical diplomatic efforts, Saudi Arabia is currently prioritizing humanitarian aspects, such as calling for an arms embargo on Israel, reflecting public outrage over Gaza. The Saudis actively participate in diplomatic efforts, advocating a two-state solution and leading calls to end Israel's military operations. While challenges persist, the country remains a potential future broker in the Israel-Palestine negotiations, recognized by the US administration.

Republic of South Africa

South Africa has accused Israel of committing genocide against Palestinians and brought the case to the International Court of Justice (ICJ). The country alleges that Israel's actions aim to destroy a substantial part of the Palestinian group. The ICJ issued "emergency measures," instructing Israel to prevent genocidal acts and enable humanitarian assistance to Gaza. Despite Israel's rejection, the court ruled to proceed with the case, with a final verdict expected in several years. South Africa's historical solidarity with Palestinians and its obligation under the Genocide Convention motivated its legal action against Israel.



GUIDING QUESTIONS

Do Israeli settlements impact the chance for peace?

To what extent is self-defense allowed?

How effective is the Iron Dome in protecting Israel, and should countries support its use for regional security?

How should the international community distribute humanitarian and military aid to Israel?

How does the international community protect the citizens of Gaza with Hamas being the elected leader?

Topic B: Tacking the Reoccurring Issue of State-Sponsored Cyber Attacks



BACKGROUND INFORMATION

Introduction

In the 21st century, technological advances have become major players in all areas of the world. Technology has been developing at an unprecedented pace, bringing development, but also increasing tension. The concern over the misuse of technology has been growing, and so has the number of state-sponsored cyber-attacks around the globe. Many states have stressed the importance of cooperation when tackling this concern, as foreign hackers become an increasing threat to government institutions, including those responsible for countries' economies, healthcare, and security. Cybercrime is now directed not only to individuals but to businesses and governments as well, reinforcing the need for cooperation and coordination between states.


Relevant Works

Council of Europe's Budapest Convention

Signed in November 2001, the convention has been active for over 20 years, with nearly 70 state parties. Its goal is to define the boundaries of cybercrime and assist law enforcement agencies' cooperation. Countries such as Russia and India have, however, refused to enter the agreement, as Russia states that the Budapest Convention is not globally relevant, and both Russia and India have affirmed it violates their national sovereignty.

Ad Hoc Committee

In December 2019, the UN passed a resolution establishing an open-ended Ad Hoc Committee (AHC) to elaborate a "Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes". Negotiations started in early 2022 and will conclude at the beginning of February 2024. During the last two years, delegates debated a zero draft of the United Nations Treaty on Countering the Use of Information



and Communications Technologies for Criminal Purposes, also known as the “cybercrime treaty”. Arriving at a consensus on cyberwar has proven to be hard, and the differences between countries prevented any major steps from being taken.

The UN Office of Counter-Terrorism (UNOCT)

UNOCT launched several initiatives in the field of cybersecurity and new technologies. In 2020 it adopted the Cybersecurity and New Technologies program, which aims to assist Member States and private organizations in preventing cyber-attacks. In 2022, UNOCT, together with INTERPOL, launched the CT TECH initiative, which works to strengthen the abilities of law enforcement and criminal justice authorities in countering the use of technology for terrorist purposes. It also works to aid Member States in developing technologies to fight against cyber terrorism.

UN Open-Ended Working Group (OEWG)

In December 2020, the General Assembly adopted resolution 75/240, which established an Open-ended Working Group on “security of and in the use of information and communications technologies”. The UN Open-Ended Working Group (OEWG) was able to adopt a consensus report in March 2021 on the “developments in the field of information and telecommunications in the context of international security”.

Cybersecurity

Introduction

The first acknowledgment of the necessity for regulating cyber war was in May 1999, when the Pentagon general counsel office published “An Assessment of International Legal Issues in Information Operations”, setting guidelines for waging cyber warfare. As time passes, the importance of regulations such as this one has only increased.

Between 2017 and 2020, there was a 100% rise in significant nation-state incidents relating to cyber attacks. The Cyber Operations Tracker released data that shows that 77 percent of all suspected operations worldwide (since 2005) were sponsored by China, Russia, Iran, or North Korea. Furthermore, in 2022, Russia and China were the biggest sponsors of cyber attacks, with Ukraine being the most targeted country. Russia’s attacks are often related to interference in elections, challenging Western institutions. China is often accused of stealing intellectual assets, while North Korea is usually involved in attacks relating to financial institutions.

Major State-Sponsored Attacks

The Stuxnet - 2010, Iran

The Stuxnet is widely considered the world’s first known cyberweapon. Deployed first in Iran, in 2010, the virus severely damaged centrifuge machines in the Natanz Nuclear Facility, located in Ahmedabad. The disruption of the Iranian nuclear program, in addition to the very well-designed and complicated computer worm, led analysts to credit it to a nation-state sponsor. The high-level sabotage operation is widely accepted as the work of the intelligence agencies of the United States and Israel, despite neither government having officially taken responsibility for it.

Paris G20 Summit - 2011, France

The Paris G20 Summit cyber attack consisted of malware attachments sent to the French Ministry of Finance officials. Its goal was to gain access to the classified G20 documents, the conference being attended by some of the most powerful countries in the world. More than 150 of the ministry's computers were infiltrated, and some of the information accessed was redirected to Chinese websites. The attack was on such a large scale, indicating that it was state-sponsored, probably of an Asian country. Despite all the speculation, no countries were confirmed to be involved in it.

Armageddon - Ukraine, 2013

According to the Security Service of Ukraine, in 2013, hackers sponsored by the Russian government conducted over five thousand attacks on Ukrainian state entities and critical infrastructure through the "Armageddon" group. The multiple attacks destabilized the country's computer networks and communications.

Yahoo Attack - 2013, US

The web platform Yahoo was the target of multiple attackers in 2013 and 2014. In 2013, the hackers gained access to information about all three billion user accounts registered at the time; in 2014, 500 million profiles were impacted. Users had their names, email addresses, telephone numbers, birth dates, and encrypted passwords compromised. Yahoo only became aware of the 2014 hack in 2016, when they published a statement that blamed a "state-sponsored actor" for the breach, without revealing which nation was involved. In 2017, the U.S. Department of Justice indicted four individuals for the cyberattacks, two of whom were officers of the Russian Federal Security Service (FSB) and seem to have "protected, directed, facilitated and paid" two hackers to deliberately access user information.

Parliament hack - 2015, Germany

In 2015, the German government experienced a large cyberattack on the federal computer networks. The attackers infiltrated the Foreign Ministry and the Defence Ministry. The group responsible, APT28, has been linked to Russian military intelligence, and the German domestic intelligence services, Bundesamt für Verfassungsschutz (BfV), believe Russia was behind the attack. The attack led to the UK enforcing new sanctions against Russia for malicious cyber activity.

The OPM hack - 2015, US

In April 2015, the Office of Personnel Management, responsible for human resource management, was hacked. The hackers gathered an enormous amount of civilian information, including millions of people's fingerprints, and the personal information of four million federal employees (past and present). US law enforcement has established that a foreign entity was the perpetrator, and further analysis shows tools associated with Chinese hackers. Despite numerous denials from the government, including from the Chinese diplomat Hong Lei who called the accusations irresponsible and unscientific, it is commonly accepted that the breach was a result of state-sponsored attackers working for the Chinese government

Operation Glowing Symphony - 2016, ISIS (Islamic State of Iraq and Syria)

The Pentagon operation that took place in 2016 sabotaged Islamic State's online propaganda. The operation was able to discover passwords belonging to various Islamic State administrator accounts and used them to destroy media content. Operation Glowing Symphony became known as one of the largest offensive cyber operations in U.S. military history and was successful in disrupting ISIS' media operations.

WannaCry Attack - 2017, UK

In 2017, the UK's National Health Service crashed after being attacked by malicious software. The NHS staff lost all access to their computer systems and were obligated to use pen and paper, causing a major disruption to the UK health system. Both the British government and the US Department of Justice claimed that North Korea was directly behind the attack, through a state-sponsored group. North Korea denied the accusations, but that didn't stop Minister of Security, Ben Wallace, from declaring that "North Korea was the state (...) involved [in] this worldwide attack."

NotPetya - 2017, Ukraine

The Russian invasion of Ukraine has been closely connected with cyber warfare. In 2015, following Russia's annexation of Crimea, a hacker group linked to Russia took down the power grid and left 230,000 Western Ukrainians without power for up to six hours. The most serious incident, however, came in 2017. Now infamously known as NotPetya, the cyberattack sought to destabilize Ukrainian computer systems but ended up spreading worldwide; it led to 10 billion dollars worth of damage for countless companies, in sectors such as shipping and food production. NotPetya was coined as the "most destructive and costly cyber-attack in history" by the White House and Ukraine was quick to point the finger at Russia, which the Kremlin's government quickly denied. Nonetheless, an investigation conducted by the UK's National Cyber Security Centre in 2018 found that the Russian military was almost "certainly responsible". Since then, many smaller-scale instances have continued to happen, especially in the context of Russia's invasion of Ukraine. Hacking continues to be employed as a strategy for war destabilization.



SolarWinds Hack - 2020, US

Considered to be one of the biggest cybersecurity breaches of the 21st century, the SolarWinds hack is infamous for infiltrating multiple organizations at once. The hack attacked the IT monitoring system known as SolarWinds, gaining access also to the systems and the data of 30,000 of the company's customers. The US's Federal investigators, together with cybersecurity agents, concluded the operation to be sponsored by Russia's Foreign Intelligence Service. The Russian government denied any involvement in the attack.

KEY TERMS

Cyberwar

“War conducted in and from computers and the networks connecting them, waged by states or their proxies against other states. Cyberwar is usually waged against government and military networks in order to disrupt, destroy, or deny their use.”

ICT: Information and communication technologies

“Information and communication technologies (ICT) is defined as a diverse set of technological tools and resources used to transmit, store, create, share or exchange information.”

APT: Advanced Persistent Threats

“An advanced persistent threat (APT) is a broad term used to describe an attack campaign in which an intruder, or team of intruders, establishes an illicit, long-term presence on a network in order to mine highly sensitive data.”

Malware: malicious software

“Malware, short for malicious software, refers to any intrusive software developed by cybercriminals (often called hackers) to steal data and damage or destroy computers and computer systems. Examples of common malware include viruses, worms, Trojan viruses, spyware, adware, and ransomware. Recent malware attacks have exfiltrated data in mass amounts.”

MAJOR DELEGATIONS


People's Republic of China

China has been accused of multiple cyber attacks during the past decades, with the United States being the main alleged target. The U.S. Cybersecurity and Infrastructure Security Agency has voiced its concern about the sophistication and abundance of the country's cyber technology, in addition to its worries regarding the general "state-sponsored cyber threat to the United States" that the PRC imposes. The 2023 Annual Threat Assessment Of The U.S. Intelligence Community stated that "China probably currently represents the broadest, most active, and persistent cyber espionage threat".

The country has repeatedly established its support for the concept of information sovereignty, which grants all countries the right to control their information and communication technology (ICTs) within their territories as they deem necessary. China is well-known for its strict protectionism, best exemplified by the Great Firewall of China, which often blocks content deemed as too Western and harmful to the country's population.

Russian Federation

Russia's participation in global cyber warfare, which has always been a cause for worry (particularly after the NotPetya incident, which shifted global perspectives on cybersecurity), has become increasingly controversial with the Russo-Ukrainian War. With highly developed ICT, the country has launched an unprecedented number of disruptive attacks against Ukraine from Russian-aligned cybercrime groups. The Microsoft Digital Defense Report analyzed international cybersecurity incidents from July 2022 through June 2023 and concluded that the most targeted country during that period was Ukraine. Other reports on Cyber-Attacks in Ukraine found that, in only the first semester of 2023, over 760 attacks were recorded, showing the continuation of this trend. There is, nonetheless, little hope for direct confirmation regarding Russia's involvement in



many of these attacks, since information leaving the country regarding military operations is scarce. Most Western countries seem to agree that the attacks on Ukraine are at least motivated or funded by the Russian Federation.

United States of America


As one of the most economically developed countries in the world, the United States employs diverse types of technology extensively, which makes it more vulnerable to cyber attacks, but also allows for its involvement in cyber warfare. The country has been investing in advanced technology for both defensive and offensive purposes, which is especially relevant when considering the US' substantial investment in military forces.

Despite having condemned the use of ICTs for cyberattacks and highlighted the danger of their misuse, the United States Department of Defense has also acknowledged their usefulness as an attack mechanism in situations of conflict. A report by the International Institute for Strategic Studies conducted in 2021---which takes into account nations' cyber attack, defense, and intelligence capabilities---placed the United States as the world's leading cyber superpower. As the country's investment in the technological field increases, so does its potential for use of this particular type of warfare.

Islamic Republic of Iran

The United States' Office of the Director of National Intelligence's 2023 Annual Threat Assessment states that "Iran's growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of U.S. and allied networks and data." The report also elaborates on Iran's opportunistic approach to cyber-attacks and affirms that Iran will continue to be a major threat to the stability and peace of the U.S. and the Middle East.

In recent years Iran has deployed numerous resources to improve their technological capabilities, and the country's associations with sophisticated espionage have increased as a result. In



addition to the many suspected assaults carried out by Iranian forces, the country has received its fair share of cyberattacks, including the infamous Stuxnet attack of 2010.

Democratic People's Republic of Korea

Despite being one of Asia's poorest countries, North Korea's cyber program has also been under rapid development as the country fights to remain relevant in the modern global scenario, and it is only expected to continue growing. The country's military forces contain many offensive and intelligence-gathering cyber weapons, and the country is considered to train and shelter some of the most skilled hackers in the world. South Korea has been the target of most of the country's attacks, followed by the United States. The government is often tied to activities of the Lazarus Group, which is commonly considered to be a state-sponsored organization. Much like Russia, there is a lack of concrete data regarding North Korean activities because the sharing of information is strictly restricted.



GUIDING QUESTIONS

Where should states draw the line between sovereignty and international collaboration?

How can information and communication technologies (ICTs) be regulated without harming national sovereignty and security?

How can states guarantee ethical uses of cyber technology?

What are ways to guarantee the proper use of ICTs in the future and international cyber security as technology rapidly advances?

WORKS CONSULTED

- <https://interactive.aljazeera.com/aje/2017/50-years-illegal-settlements/index.html>
- <https://www.britannica.com/place/Israel/Climate>
- <https://uca.edu/politicalscience/home/research-projects/dadm-project/middle-eastnorth-africapersian-gulf-region/british-palestine-1917-1948/>
- <https://www.aljazeera.com/news/2023/11/6/who-are-israeli-settlers-and-why-do-they-live-on-palestinian-lands>
- <https://www.bbc.com/news/world-middle-east-67039975>
- <https://www.washingtonpost.com/world/2023/11/30/hamas-hostages-list-names-tracker-israel-gaza/>
- <https://apnews.com/article/israel-palestinians-hamas-tunnels-warfare-15453b5729e38aeb55af5b419835a5eb>
- <https://www.cfr.org/backgrounder/what-hamas>
- <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a>
- <https://www.newyorker.com/magazine/2021/04/26/the-incredible-rise-of-north-koreas-hacking-army>
- [https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI\(2023\)702594_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf)
- <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf>
- <https://www.bbc.com/news/technology-45440533>
- <https://www.nytimes.com/2017/10/27/world/europe/uk-ransomware-hack-north-korea.html>
- <https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis>
- [https://cyberlaw.ccdcoe.org/wiki/Operation_Glowing_Symphony_\(2016\)](https://cyberlaw.ccdcoe.org/wiki/Operation_Glowing_Symphony_(2016))

-
- <https://www.gov.uk/government/news/uk-enforces-new-sanctions-against-russia-for-cyber-attack-on-german-parliament>
 - <https://threatresearch.ext.hp.com/web-of-profit-nation-state-report/>
 - <https://www.un.org/en/chronicle/article/cyberconflicts-and-national-security>
 - <https://www.chathamhouse.org/2023/08/what-un-cybercrime-treaty-and-why-does-it-matter>
 - <https://www.un.org/counterterrorism/cybersecurity>
 - <https://carnegieendowment.org/2021/05/19/un-struggles-to-make-progress-on-securing-cyberspace-putin-84491>
 - <https://dialogo-americas.com/articles/the-threat-of-foreign-state-sponsored-cyberattacks-in-brazil/>
 - <https://www.bbc.com/news/business-12662596>
 - <https://www.france24.com/en/20110307-cyber-attack-french-finance-ministry-g20-presidency-target-barack-obama>
 - <https://cyberscoop.com/ukraine-russian-hackers-armageddon-videos-gamaredon/>
 - <https://www.theguardian.com/technology/2015/jun/04/us-government-massive-data-breach-employee-records-security-clearances>



EABH MUN,
February 23-25, 2024