SJA MUN III

2025. 09.27 - 2025.09.28

Disarmament and International Security Committee (DISEC)

Addressing the Threat of Cyber Warfare to International Security

Last updated on August 3rd 2025

Table of Contents

Letter from the Chairs

Dear most esteemed delegates, We are Taewoo Park, Seonmin Lee, and Hyunjun Jang, who will be serving as your chairs for the DISEC committee.

Hello delegates! I am Taewoo Tony Park, a junior at SJAJ, and I will be serving as the Head Chair of the DISEC Committee. It is such an honor for me to serve delegates of the DISEC committee. I started my MUN journey way back in 2022. We acknowledge that winning a prize is also a big part of MUN but we sincerely hope that delegations can learn about cooperation, debate, and the joys of MUN! I firmly believe that this conference will be an opportunity for you to grow both as a MUNer and as a person. During the conference, you will face a variety of obstacles. However, it is up to you to challenge and climb over these obstacles, one by one. Though these challenges may seem daunting, you should ultimately find the entire process rewarding and enjoyable.

Greetings delegates, I am Seonmin Olivia Lee, an 8th grader attending KISJ, and I'm honored to be serving as your deputy chair for the Disarmament and International Security Committee. This is approximately my second year doing MUN, and my second time chairing. Having been a novice just a few conferences ago, I can empathize with the frustration you may face. Despite the numerous nights you may spend writing your position papers, or disagreements and objections you may encounter, I sincerely hope this conference will become the cornerstone of your growth as a delegate as well as a person. I look forward to the productive environment, ferocious debate, and the joys of MUN. Please feel free to contact us via email. Meet you there!

Hello delegates, my name is Eric Jang and I am a 9th grader attending Saint Johnsbury Academy Jeju. I am truly honored to serve as your associate chair for the DISEC committee. This is my 4th year of MUN and this is my second time chairing offline. Through MUN, I have been taught to negotiate, use logic, debate, and compromise, a few of life's most important skills. This helped me develop as a debater, a scholar, and a person. Through this conference, I hope you can take away the important lessons listed above. I wish all delegates luck and encourage you not to fear shaping your creativity into words, and finding out ways to resolve various problems in the world. I will aid you delegates in all ways I am not limited to, but also maintain impartiality. I hope this committee can find a feasible solution through the fruitful debate we will have. I wish all delegates the best of luck.

As the chairs, we are not only here to facilitate the conference, but also make SJAMUNIII a truly enjoyable experience. If you have any questions and concerns, or need assistance preparing for the conference, please don't hesitate to reach out to us. See you in September!

Taewoo (Tony) Park | Head Chair | s22270850@sjajeju.kr
Seonmin (Olivia) Lee | Deputy Chair | seonminolivia@gmail.com
Hyunjun (Eric) Jang | Associate Chair | s20297234@sjajeju.kr

Committee Introduction

The Disarmament and International Security Committee (DISEC) is an international governmental entity also known as the United Nations General Assembly's First Committee, being the first of the six major committees part of the United Nations General Assembly. It was founded in 1952 as the First Committee and then changed its title to DISEC in 1993. For many years, DISEC has been the basis of discussion between member states, enabling peace to be established in the international community. It has also been essential to finding feasible and mutually beneficial solutions for international conflicts and controversies.

Aligned with Sustainable Development Goal (SDG) 16, which calls for peace and justice, DISEC addresses ethical, socio-economic, and humanitarian concerns. It also combats issues around the globe regarding topics relating to disarmament, territorial disputes, and threats to peace. The committee is composed of 193 member states, all working towards a more peaceful society. Furthermore, there have been 79 sessions as of 2024, meeting annually during the General Assembly session in New York.

Each year, DISEC is continually working towards world peace, combating a multitude of global issues, ranging from denuclearization, maritime piracy, terrorism, emerging technologies, to current wars. Through controversial debate and prolific discussion, feasible and mutually beneficial solutions have been devised to effectively combat these international issues. The frameworks and resolutions created and agreed upon during these conferences serve as the fundamental pillars in maintaining peace and instigating further actions to be taken by both state and non-state actors. Ultimately, DISEC stands as a fundamental pillar in ensuring peace and security in the international community.

In 2017 and 2022, along with DISEC, UN Office of Counter-terrorism(UNOCT) and UN Counter Terrorism Centre(UNCCT) hosted the Group of Government Experts(GGE) to address the global threat of cyber warfare. DISEC in 2022 drafted a resolution about cyber warfare, the use of information, and communication technology; however, clear regulation was not made.

DISEC plays a crucial role in enhancing the goals of the United Nations and reaching towards a more peaceful and secure world. In summary, DISEC serves as a key forum within the United Nations system for member states to discuss international security, disarmament, and arms control. Through cooperation, negotiation, and consensus-building, the committee aims to find effective solutions to global crises and contribute to international security.

Agenda Introduction

The first ever state-sponsored, coordinated cyber-attack occurred in 2007, where government and parliamentary portals, ministries, major banks, and minor businesses were all damaged by a Distributed Denial of Service (DDoS) attack executed over a 3-week period. Numerous other acts of cyber-warfare were detected, the attacks infringing countries' privacy and integrity in all aspects, endangering both the private sector as well as the government.

Recently, with technology and databases reaching an exponentially high level of significance in government mechanisms as well as citizens' daily lives, cyber security has become one of the ultimate priorities of a nation. The annual cost of cybercrime in 2024 was $922,0,000,000,000 USD, which is more than 10 times the cost of cybersecurity in 2018: $860,000,000,000 USD. In the 21st century, information storage, domestic communication, the management of internal processes, and the provision of public services are all becoming digitized. Specifically, governments store citizens' personal information, the government's classified information, as well as financial information that includes government accounts, budgets, and contracts. Due to this, governments are becoming more and more reliant on these technologies –for instance 60% of global GDP has been digitized by 2022– and thus, countries are highly vulnerable to cyber attacks, now more than ever. Simultaneously, malicious technology and methods in attacking cyberspace have drastically developed, leading to an unprecedented increase in cyber-crimes. Recently, these cyber technologies have been illegally utilized and exploited by particular governments, to seek its benefits in accessing private information, appropriating money, etc. These malicious acts are referred to as cyber warfare, and have become a threat to international security, intensifying tensions between nations.

The most predominant concern so far is that, with the agenda being a newly arising issue, the international community lacks a consensus regarding the jurisprudential aspect of these attacks. The difficulty of attributing attacks to specific actors is a persisting challenge. Cyber attacks mostly happen anonymously, making it difficult for nations to determine the source of the attack. Adding on to that, nations have different views on what constitutes an act of warfare in cyberspace. This lack of agreement can lead to inconsistent responses and increased risks of escalation.

The threat of cyber warfare to international society is a complex and newly arising issue that demands urgent attention from all member nations. As technology evolves, so do the methods and motivations of cyber attacks. Understanding the implications of these threats is essential for nations to protect international security.

Key Terms

Cyber Attack

Any attempt to damage, disrupt, or gain unauthorized access to a computer system or network. Different types of Cyber attacks exist, such as a DDoS attack. It is crucial to understand the types and impact of cyber attacks to address the agenda.

Cybersecurity

Cybersecurity includes the technologies, processes, and policies designed to protect networks, devices, programs, servers, and data from digital attacks, damage, or unauthorized access. Nowadays, cybersecurity is essential for national security, and it will be crucial for member nations to share technology for cybersecurity.

Cyber Warfare

Cyber warfare is the use of computer network attacks by a nation or organization to disrupt, damage, or destroy another nation's computer system or infrastructure. DISEC's role is to develop international frameworks to define, prevent, and respond to cyber warfare incidents.

Distributed Denial of Service (DDoS) Attack

A DDoS attack involves taking over a system or network with excessive traffic from multiple sources, causing it to become slower or completely blocked. The 2007 cyber attack on Estonia, a prime example of a nation-level DDoS attack, marked the beginning of cyber warfare as a tool of international conflict.

Non-Intervention Principle

This principle prohibits member nations from interfering in the international affairs of other sovereign nations. Cyber warfare can violate this principle, so it needs to be addressed in the resolution.

Ransomware

Ransomware is one type of malware, which prevents you from accessing a file or a device usually by encrypting your files. A criminal group will then demand ransom in order for you to regain access to that file. It is a method widely used by criminals nowadays, mainly used to target a wide range from civilian users to companies.

State-Sponsored Cybercrime

This refers to cyber activities led by or supported by the state to achieve strategic objectives including destabilizing infrastructure or stealing valuable information. These activities

are distinct from other forms of cybercrime due to their scale, sophistication, and the level of resources backing them.

Terrorism

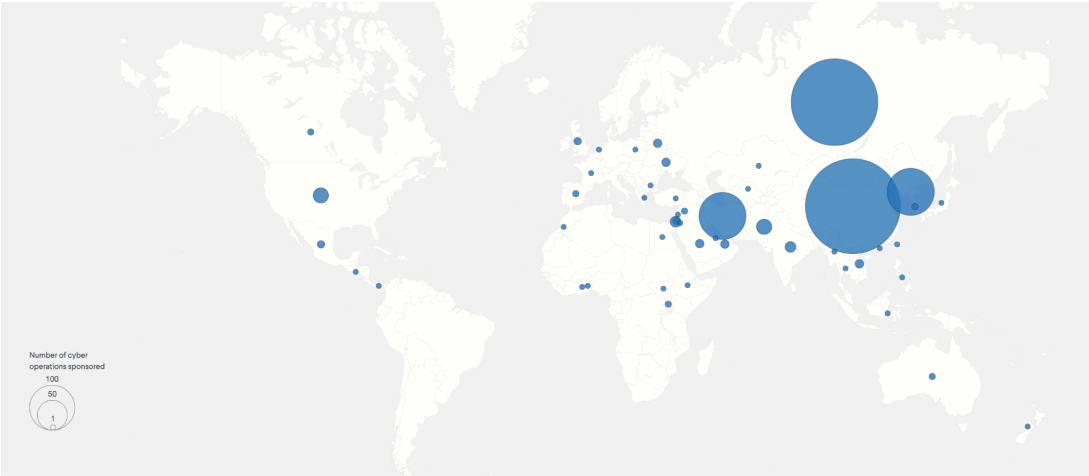
Terrorism involves the use of violence, threats, or intimidation against civilians. As cyber warfare starts to escalate, DISEC should consider the growing intersection between warfare and terrorism. Cyber tools can empower terrorist groups to cause large-scale disruption with minimal resources.

Historical Background

With the advent of the first general-purpose electronic computer in 1946, cybersecurity has become a progressively significant concern. The first recorded act of cyber malware utilization dates back to 1971, and throughout the rest of the 20th century, there have repeatedly been minor and somewhat major cases of cyber-attacks. However, the utmost severity and urgency of the jeopardization of cyber-security wasn't fully recognized until the 21st century, where major sophisticated attacks were first performed.

As briefly mentioned before, the first attack qualifying to be 'sophisticated' was the allegedly state sponsored 2007 cyber-attack on Estonia, in which the attackers, who identified to be located in Russia, installed a malicious network resulting in a denial of access for legitimate users. There were several notable aspects of this attack: 1) the attacks started and ceased simultaneously conveying that it was presumably a synchronized and thoroughly planned attack, 2) the attacks were traced back to individual hackers ensuring that any state sponsor would remain ambiguous, and 3) it was found that attackers could have inflicted more damage than done so, indicating the likelihood that the attack had a predominant psychological dimension in testing cyber-related capabilities and engendering confusion. The first factor acknowledges how major scale attacks have grown increasingly common and often-times state sponsored. This signals the beginning of the utilization of cybercrime in warfare, also known as cyber-warfare, in which a nation benefits from the access to private information and financial profit through illicit and malicious cyber-activity. Though for the 2007 attack, it was identified that the Russian government was highly likely to be involved, the second factor recognizes the immense level of difficulty in identifying the source of the attack, as further technology and tactics develop in disguising attack sources. This is especially due to governments denying association with cyber-attacks. The final aspect points towards the fact that multiple cyber-attacks would follow this particular attempt of cyber-warfare, presuming that it was intended to test capabilities rather than solely focussing on physical benefit.

Yet another preeminent event was the 2015 NotPetya attack on Ukraine, yet another attack made by hackers in Russia. The attack is often referred to as the largest cyber-attack, resulting in $10 billion of damage. A notable factor in this particular attack was the fact that it was allegedly brought upon by Russia. Though whether it was state sponsored or not could not be determined, it is considered a component in the ongoing russo-ukrainian conflict after the dismantling of the Soviet Union. This is again presumably an act of cyber-warfare, yet due to the fact that the attack source is merely alleged, no international legal action could be taken into place, with Russia denying the attacks. An aspect to take into mind is the currently ongoing Russo-Ukrainian war, and the cyber-warfare that may take place to breach government systems and illicitly access data or make financial gain.



Graph 1: Cyber-Operations Per Country *(2005-2025 . Council on Foreign Relations)*

Since 2005, thirty-four countries are suspected of sponsoring cyber operations. China, Russia, Iran, and North Korea sponsored 77 percent of all suspected operations.

Furthermore, as cross-border –and oftentimes state sponsored– attacks began devastating both national governments and the private sector, cybersecurity has grasped the interest of the international community. There have purportedly been repetitive cases of state sponsored cyber-warfare by countries such as but not limited to: China, Russia, Iran, and North Korea. Yet, due to the ambiguity of nations as well as state sovereignty concerns, there has been constant dispute between the nations.

To mitigate the damage done by these attacks and establish specific criminalization standards as well as mechanisms, the international community was brought together in 2001, where the Budapest Convention on Cyber-security was signed and later entered into force in 2004. This convention, created under the Council of Europe, aimed to harmonize international cyber-security laws and standards, including standards relating to the persisting dilemma regarding state sovereignty in criminalization. It enables legal investigation on global-scale crimes and has several basic legal frameworks that work towards preventing cybercrime. To this day, it is one of the only long-lasting conventions on cybercrime. Yet, the convention has its drawbacks. Though it is currently ratified by 76 states, it has not yet been ratified by significant contributors that may be heavily related to international cybercrime, such as China, Russia, or the DPRK. This raises concerns regarding the level of compliance. Additionally, taking into consideration that the convention was created as long as 24 years ago, it lacks modern methods and hence, cannot be considered up to date.

Though there has been much improvement in cyber-security over the years, it is wholly comprehensible that there are many more standards to be set, incentives to be guaranteed, and legal jurisprudence to be created. Cyber warfare persists to be an utmost menace to international security.

Current State of Affairs

Cyber warfare has become one of the most pressing security concerns of the 21st century, with states increasingly relying on cyberattacks as malicious tools of geopolitical influence, sabotage, and illicit intelligence gathering. The ongoing Russo-Ukrainian War is a stark example. Russia has launched waves of cyberattacks against Ukrainian infrastructure, government networks, and private companies, often coinciding with kinetic military operations. These attacks have disrupted communications, damaged energy grids, and destabilized Ukrainian Society.

Similarly, tensions between the US and China have arisen with heated frequent accusations of state-sponsored cyber espionage. The US has attributed large-scale breaches, such as the 2014 Office of Personnel Management hack, to Chinese actors allegedly operating under state direction. China, in turn, has denied involvement and accused the US of its own cyber operations.

A central concern in the current landscape is criminalization and responsibility. Because the attribution of cyberattacks is technically complex and often circumstantial, with limited access to information, taking into mind that the investigation is often one-sided. Nations accused of sponsoring attacks, such as China, Russia, or North Korea, are technically merely allegedly responsible. This means no binding international legal mechanism exists to prove responsibility to a degree sufficient for enforcement of sanctions under international law.

This ambiguity cannot be cleared due to implications regarding state sovereignty, as countries find themselves under digital attack without a clear legal path to seek neither justice nor deterrence. The lack of accountability mechanisms engenders an environment where states can escape allegations, since they face no guaranteed repercussions. Because of this, there is little incentive to halt offensive cyber operations. This cycle of blame and denial intensifies cyber conflicts, encouraging more frequent and more sophisticated attacks as states seek strategic advantage without fear of legal or diplomatic consequences.

Stances of Parties

Afghanistan

Afghanistan recognizes the threats of cyber warfare in the status quo. The country's National Cyber Security Strategy, adopted in 2014, explicitly addresses the need to protect government, business, and citizen data from cyber threats, and highlights the importance of international cooperation to combat cybercrime and cyber warfare. In May 2025, the hacker group Afghan Dragons launched a major cyberattack that disrupted online services of at least 20 Taliban-led ministries and several affiliated agencies. The attack was a protest against the Taliban's policies. Earlier in 2025, another group called the TabiLeaks infiltrated the Taliban's government networks, exfiltrating and publishing over 50 Gigabytes of sensitive information. However, although the Taliban in power is seen with a negative view throughout the international community, Afghanistan has recently become a large victim.

Australia

Australia views cybercrimes as an enormous rising threat to the international community, with state-sponsored cyber warfare, cybercrime, and threats to critical infrastructure at the forefront of its national security concerns. The government has taken a proactive approach, recognizing that the digital domain is now a primary battleground for both state and non-state actors.

Australia has seen a sharp increase in ransomware cases in 2025, with a 126% rise in reported incidents in the first 6 months of 2025 alone. Healthcare, finance, and manufacturing industries have been heavily targeted. Therefore, Australia aims to be a world leader in cybersecurity by 2030. The 2023-2030 cyber security is built around six "cyber-shields designed to protect citizens, businesses, and critical infrastructure.

Belarus

Belarus officially recognizes cybersecurity as a major component of national and international security, emphasizing the need to counter threats such as terrorism and the misuse of emerging technologies such as AI. The country's 2019 Doctrine of Information Security promotes the concept of information sovereignty and advocates for the respect for the digital sovereignty of states. Belarus endorses international agreements to ensure information security, similar to military confidence-building measures.

Canada

Canada views cyber warfare as a significant threat to international security and has articulated a clear stance that emphasizes the application of international law, multilateral cooperation, and proactive defense. Canada strongly supports the application of existing international law, including the UN charter to cyberspace. Canada promotes a rule based international order in cyberspace, promoting responsible state behavior and the development of global norms.

China

China, although a publicly accused state sponsor of cybercrime, does acknowledge the threats of cybercrime to the international community. China emphasizes the need for the development of international norms to protect mainly its civilians. It has actively advocated for multilateralism and international rules for the protection of global industries and trade, since China is a major producer in the global supply chain.

However, as corresponding to the accusations against China, the Chinese government strongly seeks to defend its cyberspace sovereignty, protect critical information and infrastructure, and prevent foreign adversaries from using cyber operations to undermine political and social stability. China believes that existing international laws can be revised or clarified to apply to cyberspace but stresses the need for openness and flexibility in developing these frameworks.

DPRK

The Democratic People's Republic of Korea does not publicly articulate a formal diplomatic stance on the threat of cyber warfare to international security. The country has been attributed for cyber-warfare by numerous nations, especially the ROK and the USA. Yet, the nation continues to emphasize the unreliability of the accusations made against the nation, often denying the charges of cyberwarfare pressed against the state. The DPRK stresses the fact that these accusations are simply presumed and are highly inaccurate, in particular, refuting the comments made about Bureau 121's – a North Korean military unit/agency– responsibility for South Korean data breaches.

The DPRK strongly believes that these extreme allegations hurt and destroy a nation's image in the international community and prioritizes a nation's state sovereignty. Furthermore, the nation continues to have a reserved stance towards international legal measures relating to cyber-activity, especially in the case of investigation and formal legal charges against nations. Therefore, the nation prefers national domestic action against cybercrimes rather than an international approach in executing formal repercussions against accused nations.

France

France considers cyber warfare a significantly large evolving threat to international security. The French have experienced a sharp and sustained increase in cybercrime over the past several years. In 2024, the annual cost of cybercrime in France reached an estimated $129 billion, a number that grew rapidly from $41 billion in 2016. The cyber attacks were mainly associated with healthcare and companies.

Even the government suffered from multiple cyber attacks. In 2024 and 2025, France publicly accused Russia's GRU military agency of orchestrating a series of cyberattacks against French government ministries and organizations that planned the 2024 Paris Olympics.

Against these cyber threats, France advocates for the UNSC to remain vigilant and integrate the cyber dimension into their work. They have established a strategic framework from the late 2010's. In 2009, France established the ANSSI to coordinate national cyber defense, and

in 2011, after the government was targeted, the French explicitly declared that it would strive to become a leader in global cyber powers.

Germany

Germany actively advocates for a robust international response grounded in law, cooperation, and multilateralism. Some key aspects of Germany's stance include: recognizing the threat, applying and adapting international laws to cyberspace, utilizing multilateral organizations, approaching in a comprehensive and cooperative manner, and building trust. In summary, Germany views cyber warfare as a major threat to international security and champions a rules-based, multilateral response anchored in international law, collective defense, and active norm-building.

Recently, the pro-Russian and the anti-Israeli hacker groups have targeted public and federal institutions of Germany. As a large country and an economic leader in the Western world, critical infrastructure and government services have been repeatedly targeted. In response to these, Germany has presented a National Cyber Security Strategy and has multi-layered actions. It has advanced technical defenses that actively utilize AI-powered threat detection. It also uses public-private collaboration with campaigns and education for employees and the public.

Iran

Iran, a country currently active in conflict, views cyber warfare as a threat to its own security, but has also been accused of sponsoring its own attacks –though the allegations have been mostly denied. Officially, Iran emphasizes the need to defend its critical infrastructure and sensitive data against foreign cyberattacks, particularly in response to events like the Stuxnet attack.

To reiterate, Iran is widely recognized as a state sponsor of cyber warfare, as multiple US government agencies, including the FBI and the CISA, confirmed that Iran has contributed to malicious cyber activities. Yet Iran believes these allegations are hurtful towards international relations and is faltering peace rather than promoting justice, particularly because of the lack of evidence to back these attributions.

Iraq

Iraq views cyber warfare as a serious and growing threat to both its national and international security. The country recognizes that cyber threats pose invisible challenges to its strategic sectors. The government has been concerned that Iraq's digital infrastructure is still vulnerable and susceptible to cyberattacks. Internationally, Iraq supports legal frameworks against cyber threats. The government has made partnerships with entities such as NATO to build cyber defense capabilities and has called for the construction of comprehensive legal and regulatory structures.

Although there weren't any incidents, Iraq feels threatened by Iranian cyber strategies, often involving targeting regional adversaries. Additionally, Iranian cyber groups are currently active around the Middle East with local proxies. This indicates that Iraq, which has a complicated

relationship with Iran and has a history of hosting Iran-backed groups, could be a stage for indirect operations, such as Belarus.

India

India has a similar attitude towards cyber warfare as other active nations, which is recognizing cyber threats and advocating for global cooperation. India actively supports international collaboration for security, especially through international forums. India has participated in major UN processes such as the GGE or the OEWG, working towards a rule-based international order in cyberspace.

However, due to India's complicated relationship with Pakistan and the dispute for the region Kashmir, to India, Pakistan is considered a significant cyber threat to India. Multiple recent events and reports confirm that Pakistan-linked groups and state-sponsored actors have targeted the Indian government, military, and critical cyber infrastructure. In May 2025, Pakistani cyber teams reportedly launched large-scale attacks against Indian communications and the government, solidifying India's concern. India quickly mobilized national and state-level cyber response teams, notably the CERT-In, to mitigate damage. It has taken proactive measures to defend critical infrastructure.

Israel

Israel also views cyber warfare as a significant and growing threat to international security and has solidified its position as a global leader in both cyber defense and offense, considering the geopolitical tensions in the environment of the Middle East. The IDF plays a central role in defending Israel's cybersecurity as can be seen in the name. Israel actively engages in international partnerships, especially with the Western world to share intelligence and develop global cybersecurity standards.

Hamas has recently developed new cyber capabilities that are now targeting Israeli digital infrastructure and intelligence. The Hamas-affiliated hackers recently claimed victory after gaining access to Israeli governmental systems. Although Hamas's capabilities are far less advanced than other state-sponsors, Hezbollah also engages in cyber attacks as well. It possesses cyber units and has been involved in numerous operations against Israel. Due to all of these geopolitical factors, Israel has no choice but to solidify its stance against cyber warfare and defend its own critical cyber infrastructure, but also develop offense.

Italy

Italy, being one of the most protected countries from cybercrime, is considered a tier 1, 'role-modeling' country, scoring a 100, in terms of the level of commitment to cyber-security according to the 2024 ITU Global Cybersecurity Index. Yet, cybercrime is still a persisting concern for the country with criminals breaching its systems and causing notorious damages. The Italian Cybersecurity Association (CLUSIT) has connoted upon the severity of the situation, with the Postal and Communications Police (CNAIPIC) having to interfere with 13,000 attacks –some state sponsored and others by individual entities– in the year 2022, which is more than double the level of attacks in the previous year.

In response, the Italian government has strengthened national security, establishing the National Cybersecurity Agency (ACN) in an effort to coordinate responses to major cyber-attacks, especially those relating to government data breaches. Furthermore, by initiating the National Cybersecurity Strategy in 2022, until 2026, the nation aims to enhance resilience in developing cyber infrastructures and improving its capacity to respond to cyber-attacks.

Japan

Japan, being a leading nation in cybersecurity ranks in tier 1 of the 2024 ITU Global Cybersecurity Index, with a score of 97.58, although the nation slightly lacks in cooperation measures, the country demonstrates a nearly full commitment to ensuring its resilience against forms of cybercrime. Yet, multiple attacks allegedly sponsored by the DPRK as well as China have breached Japan's cybersecurity mechanisms. In the fall of 2024, Japan, along with the US, has attributed military cyber attacks against Japan's compromised classified defense networks to China, which involve plans, shortcomings, and capabilities of the country's military infrastructures.

In response, the nation has created multiple legislative frameworks, including the 'Active Cyber Defense Law', to be operational in 2027, a law that enables the nation to execute preemptive measures against possible cyber threats. Though these strategies require much improvement, the establishment of the law signals that more proactive action is being taken.

Lithuania

Lithuania is considered an 'Advancing' nation in cybersecurity efforts by the 2024 ITU Global Cybersecurity Index, scoring 92.88. The nation, situated in Northeastern Europe, has also been targeted in global cybercrimes, with a general rise of 63 percent more cyber incidents in 2024 than in 2023, according to the 2024 National Cybersecurity Status Report. Among the numerous attacks against the country that year, 3 were deemed major, and linked to state-backed foreign cyber groups. Allegedly, these groups were aiming to pursue long-term goals through the malicious act, such as espionage.

In response, the National Cyber Security Center –a government body within Lithuania responsible for developing cyber resilience by assessing and enhancing national capabilities and domestic legal frameworks– has carried out efforts to ensure proper implementation of legal frameworks and infrastructure. The center prioritizes the intensification of administrative sanctions for non-compliance in establishing a clear law of cybersecurity and effectively implementing it throughout the state.

Philippines

The Philippines scores a 93.49 in the 2024 ITU Global Cybersecurity index, thus recognized as an 'Advancing' nation. Statistically, the state relatively lacks in capacity/infrastructure development, presumably due to the country being considered a 'developing economy' or 'LEDC' by the United Nations. The nation lacks the financial capacity to ensure the implementation of comprehensive infrastructure and mechanisms for resilience against cyber attacks in technical means. In 2024, researchers at the US cybersecurity firm suggested a 325% increase of cyber crimes targeting the Philippines compared to 2023. Allegedly,

the majority of state-sponsored cyber warfare is attributed to the Chinese government. Experts claim that the recent unprecedented acceleration of cybercrimes may connect the tensions between the nations relating to the South China Sea Dispute.

In response, the Philippine government has drastically improved cybersecurity measures, climbing from 61st to 53rd in the United Nations Global Cybersecurity Index in September of 2024. Furthermore, the National Cybersecurity Plan (NCSP) 2023-2028 incorporates the government's strategic goals to enhance cyber resilience. As of 2025, the government is prioritizing international cooperation and is willing to facilitate discussions between countries to reach a unanimous solution.

Republic of Korea (ROK)

The Republic of Korea, with preeminent up-to-date progress on cyber security measures, is considered a 'Role-Modelling' nation by the 2024 ITU Cybersecurity Index, being one of the most developed in cyber-security infrastructure-wise along with the USA. Yet, according to the ROK's Ministry of Foreign Affairs, the DPRK is an evident threat to the nation's cybersecurity. The government claims that after tighter sanctions imposed upon the DPRK in 2016, the nation has increased the usage of cyber-warfare, as a means of earning foreign currency and financing for its nuclear development program.

In hopes of mitigating the damage done and preventing cyber attacks, the ROK prioritizes cooperation with the international community, as well as increasing awareness both in domestic and international terms. Since a majority of the attacks are toward the public, the nation aims to enhance resilience by coordinated reporting of DPRK's illicit cyber-activity and response. Yet, in order to prevent further cyber activities from the DPRK, the ROK connotes the need for international discussion and for a consensus on the issue to be unanimously agreed and complied upon.

Russia

The Russian federation is regarded as a Tier 2 country in terms of cybersecurity by the 2024 ITU Cybersecurity Index, with 92.13 points. Yet, the nation is one of the most severely accused for state-sponsored cybercrime, especially for targeting Ukraine amid the tension between the two nations.

Facing these accusations and numerous suggestions in international sanctions through the United Nations Security Council, the nation has continued to emphasize the significance of the nation's right to state sovereignty, and adamantly refuted the alleged accusations. Due to the fact that thorough investigation on the source of cyber-crime is not guaranteed with concerns of state sovereignty, Russia constantly claims that the nation's presumable responsibility for the cyber attacks is not factually proven.

Singapore

Singapore, with 99.86 points is considered a 'Role Modelling' nation in cybersecurity by the 2024 ITU Cybersecurity Index. Yet, the nation faces constant threats of cyber crime.

The Cybersecurity Agency of Singapore (CSA), founded in 2015, aims to enhance the nation's resilience against international cybercrimes, and hence, has goals encompassing various aspects of cybersecurity, such as but not limited to: protecting cyberspace, enhancing cybersecurity awareness among the public, and implementing cyber infrastructure to augment its cyber capacity. The Agency analyzes risks and executes appropriate measures in relation to the threats. Furthermore, the Ministry of Foreign Affairs of Singapore recognizes the importance of international discussion, and thus, aims to "play an active role in cybersecurity discussions at the UN".

Sweden

Sweden is regarded as a 'Role Modelling' nation by the 2024 ITU Cybersecurity Index, with a total of 99.31 points. Yet, according to the International Trade Administration, in 2019, the number of ransomware attacks have increased to an unprecedented level of 144% in Sweden. Thus, the nation continues to put effort in expanding its cyber-combating capabilities.

The nation is characterized by its focus on enhancing cybersecurity technologies and mechanisms to combat cyber crime in technical means. The nation's security policies underscore the significance of developing technologies, and connotes emerging technologies such as artificial intelligence, quantum technology, advanced semiconductors, and 6G communication networks will be a key driver in cybersecurity. The nation hence believes that being up to date with these technologies is crucial, especially artificial intelligence, as it is already widely utilized in cybercrime. The nation also emphasizes the importance of international communication in enhancing cybersecurity in a global magnitude.

Switzerland

Switzerland, scoring 91.26 points, is considered an 'Advancing Nation' in cyber security according to the 2024 ITU Global Cybersecurity Index. Yet, according to the Swiss Federal Intelligence Service, in 2019, "... a record number of state-sponsored cyber attacks on Swiss interests, most of which were of Russian, North Korean, Chinese and Iranian origin." have been detected.

In response to the detrimental attacks on the critical cyber-infrastructures of Switzerland, the National Cybersecurity Center has decided upon an amendment to the Information Security Act (ISA) of 29 September 2023 to be implemented in April of 2025. The legal framework mandates that detected activity of cybercrime dismantling necessary infrastructure such as energy and water suppliers, must be immediately reported within 24 hours of discovery, hence ensuring enhanced coordination in combating cybercrimes and augmented cyber resilience. Furthermore, the Swiss government advocates for a unanimous international standard upon cyber-security to be set, through multilateral discussion under the UN or any other international entity.

Türkiye

Türkiye, with a full score, is regarded as a 'Role Modeling' nation in cybersecurity by the 2024 ITU Global Cybersecurity Index. However, Advanced Persistent Threat (APT) entities pose

as menaces to the nation's cyber-related systems, specifically –allegedly– Iranian hackers and pro-Russian groups. These state sponsored actors have breached Türkiye's critical government funded infrastructure, aerospace sectors, and government systems, by employing complicated and sophisticated cyber espionage techniques. Hence, geopolitical tensions among the countries have arisen.

In an effort to mitigate the aftermath of these attacks and strengthen resilience, the nation's government has amended the past 'Personal Data Protection Law', to further align with the European Union's framework on cybersecurity. These updates have also ensured that the law encompasses mechanisms to simplify compliance among businesses to fortify cyber defenses, and means of improving data transfer and cyber security standards throughout the nation.

Ukraine

Ukraine ranks in tier 3 in the 2024 ITU Global Cybersecurity Index, scoring 83.93. The country relatively lacks measures related to capacity development and organization, and it is recognizable that there is much improvement to be made. Ever since the infamous Not Petya attack against the nation, Ukraine has faced numerous attacks allegedly from Russia, due to the historically severe tensions between the two nations, with the number of cyber attacks escalating after the beginning of the recent fully fledged Russo-Ukrainian conflict that began in 2022. Most notably, as tensions arose in 2016, Ukraine publicly accused the Russian government of utilizing cyber warfare against the nation's government website, thus imposing major sanctions on Russian internet businesses.

In an effort to prevent cyber attacks and mitigate damage, the Ukrainian government has initiated multiple projects through the National Security and Defense Council of Ukraine, in that Ukraine requires development in deterrence, cyber resilience, and interaction. The council has connoted the importance of strengthening the capacity of national cyber security systems, particularly by enhancing cyber infrastructures. Furthermore, communication and coordination in managing wide-scale cyber attacks has been addressed by the nation strengthening international relations and collaborating with the European Union, the United States, and other NATO member states.

United Kingdom (UK)

The UK is ranked tier 1 in the 2024 ITU Global Cybersecurity Index with 100 points. Hence, it is one of the most financially and technically advanced countries regarding cyber security. Yet, in the year 2024, the United Kingdom's National Cyber Security Center found a three-fold increase in cyber attacks categorized as the "most significant", compared to 2023. The NCSC also provided aid and support for 430 attacks, 89 categorizing as "nationally significant", and proclaimed the countries of China, Russia, Iran, and North Korea as "real and enduring threats". The same year, 190 megabytes of data were exposed, revealing a Chinese company's alleged espionage attempts on the UK's government.

In the past, the UK has carried out multiple international initiatives, endeavoring to create resilience against cybercrime. The UK has provided £7.3 million of cyber support towards Ukraine since the start of the war due to the mass number of cyber breaches from the Russian Federation.

The UK has also set up numerous formal cyber dialogues with more than 10 countries across the world as well as the EU. Also, the United Kingdom has announced a partnership with France and signed a joint statement with the US and 11 other countries on countering cyber dangers. Through these actions, the UK has yet again shown disposition in becoming a global leader in cyber affairs.

United States of America (USA)

With a near perfect score of 99.86, the United States of America ranks in tier 1 of the 2024 ITU Global Cybersecurity Index. Being one of the leading voices in the lasting discussion regarding international cyber security, the USA seeks to establish and enforce a strictly binding legal agreement to preempt further mass-scale international cyber security breaches from further debilitating countries' government systems. The USA has accused numerous nations, especially China, Russia, and the DPRK for facilitating cyber warfare against the nation. Recently, in 2021, the country inculpated China for an array of cyber crime activities, reproaching its Ministry of State Security, allegedly linked to a coordinated attack on Microsoft's widely used email server software earlier in the year. Indeed, China denied these allegations.

In response, the United States has established a multi-agency approach to cybersecurity, with agencies such as Cybersecurity and Infrastructure Security Agency (CISA), the Department of Homeland Security (DHS), and the National Security Agency (NSA) collaborating to implement cyber security strategies and infrastructures. In international relations, the nation has continued to advocate for appropriate punishment and compensation measures to be enforced, along with its allies in the North Atlantic Treaty Organization (NATO) and the European Union (EU).

Possible Solutions

Solution 1: International Collective Action

With cyber-security being a relatively recent issue, it is recognizable that the international community lacks unified coordinated measures and repercussions in the handling of overseas cybercrimes, particularly those that are state sponsored. Though more discussion is required in resolving the implications regarding nations' state-sovereignty, this collision of stances may be resolved through continuous efforts in prioritizing mutual benefits for all states involved. In the past, multiple conventions and legal frameworks have been suggested, such as the Budapest Convention. Yet, many have been met with pejorative responses, hence lacking compliance, especially from nations deeply associated with the issue. Under this premise, it is evident that nations must introduce legal jurisprudence as well as jurisdiction regarding cybercrime, while simultaneously incentivizing adamant countries to comply. These incentives may include financial and technical support, preferably relating to cybersecurity. Yet, it must be taken into mind that these incentives would need to be equally, or more economically and politically rewarding than the very act of cyber-warfare.

Furthermore, whilst respecting the sovereignty of all nations, international standards and legal jurisprudence could be set, relating to managing responsibility, minimizing ambiguity, and prosecution regarding international cybercrimes. This may be held under an international entity, specifically an international court, such as but not limited to: the International Criminal Police Organization (INTERPOL) or the International Court of Justice (ICJ). This may involve potential arrest warrants for those held responsible for mass scale cybercrime, which does not directly infringe a nation's sovereignty seeing that it would not involve force towards a nation within its borders, only when the criminal would be in the territory of other countries. On a major scale, if the attacks relate to the state's government itself, there may even be sanctions charged, though this would require the consent of nations, further discussion –possibly through continuous annual conferences, and approval through the UNSC – taking into mind the limitations of DISEC. In summary, the most significant factors concerning these legal approaches would be 1) transparency and mutual trust among nations, 2) mutual benefits for all parties with appropriate incentives that have a feasible method of execution, and 3) mechanisms to ensure compliance and specific legal measures in the case of non-compliance.

Finally, another more achievable approach may be to amend the already existing past Budapest Convention by adding protocols. As mentioned in the historical background, the convention is somewhat flawed and outdated, with little compliance mechanisms and ratification. These protocols may encompass methods to ensure that the convention is more mutually beneficial –to increase rates of ratification, clear and feasible compliance mechanisms, or more up-to-date information taking into mind the rapidly escalating temperament of the issue following the utilization of newly arising technologies such as artificial intelligence.

Solution 2: International Support for Domestic Action

The jarring inequality in cyber-development between nations can be viewed in the ITU Global Cybersecurity Index. Furthermore, it is also recognizable that less economically developed countries (LEDCs) mostly populate the bottom tiers and rankings. In response, these nations may be funded to expand their cyber infrastructures in order to engender an overall cyber-resilient environment. To ensure feasibility, the financial/technical funding would require a benefactor, which may be decided upon by assessing the financial and technical capacity of nations, specifically the level of development in cybersecurity infrastructures, potentially through existing assessments in capacity such as the ITU cybersecurity index.

Yet, another factor to consider is ensuring transparency in the funding due to the undeniable fact that the funding may be taken advantage of with an ulterior motive and used in a corrupt manner by some nations that do not prioritize cyber-security. Delegates must consider a means of guaranteeing transparency to acquire mutual trust among all parties, both giving and receiving the funding. This solution would be a more feasible and achievable solution, most likely the first step in achieving complete security and mutual trust/compliance.

Questions to Consider

1. How could the attempts of escaping international condemnation of the state sponsors of cybercrime be thwarted and compliance of agreements be guaranteed while simultaneously maintaining a reverent attitude towards nations' state sovereignty?
2. How might enhancing reliance on digital infrastructure affect the nature of crimes between corporations and countries?
3. How might the proliferation of asymmetrical cyber capabilities affect power dynamics between states? How could these inequalities be resolved through an international unified agreement?
4. To what extent could cyber warfare be considered an act of aggression under international law, specifically the United Nations Charter, and what are the implications for the right to self defense for affected parties?
5. How can transparency be ensured in any and all government responses regarding cyber-security, and how could mutual trust among all parties?

Bibliography

Canada's National Cyber Security Strategy: Securing Canada's Digital Future, 24 March 2025, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2025/index-en.aspx. Accessed 20 July 2025.

"About the Convention - Cybercrime." *The Council of Europe*, https://www.coe.int/en/web/cybercrime/the-budapest-convention. Accessed 20 July 2025.

al-Ali, Ali Ziad. "The Hidden Threats to Iraq's National Security." *Al-Bayan Center for Studies and Planning*, Al-Bayan Center for Studies and Planning, 7 10 2018, https://www.bayancenter.org/en/2018/07/1549/. Accessed 20 7 2025.

"Cyber Operations Tracker | CFR Interactives." *Council on Foreign Relations*, https://www.cfr.org/cyber-operations/. Accessed 20 July 2025.

Devanny, Joe. "Interpreting India's Cyber Statecraft." *Carnegie Endowment for International Peace*, 27 March 2025, https://carnegieendowment.org/research/2025/03/interpreting-indias-cyber-statecraft?lang=en. Accessed 20 July 2025.

Developments in the Field of Information and Telecommunications in the Context of International Security – UNODA. https://disarmament.unoda.org/ict-security/#:~:text=In%202022%2C%20a%20General%20Assembly%20resolution%20entitled,account%20the%20views%20submitted%20by%20States%20(A/78/76). Accessed 31 July 2025.

"DICT fortifies PH cybersafety with National Cybersecurity Plan '23-'28." *Philippine News Agency*, 14 February 2025, https://www.pna.gov.ph/articles/1244121?utm_source. Accessed 20 July 2025.

"France - Octopus Cybercrime Community." *The Council of Europe*, https://www.coe.int/en/web/octopus/-/france. Accessed 20 July 2025.

"Global Cybersecurity Index 2024." *ITU*, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf. Accessed 20 July 2025.

Government of Belarus. "CSTO countries to take additional measures to combat cyber threats." *Belarus by*, Government of Belarus, 22 11 2023, https://www.belarus.by/en/government/events/csto-countries-to-take-additional-measures-to-combat-cyber-threats_i_164574.html. Accessed 20 7 2025.

Government of Sweden. "Security Policy." *Government Offices of Sweden*, Government of Sweden, https://www.government.se/government-policy/sweden-in-a-digital-world/security-policy/. Accessed 20 7 2025.

"How the NotPetya attack is reshaping cyber insurance | Brookings." *Brookings Institution*, 1 December 2021, https://www.brookings.edu/articles/how-the-notpetya-attack-is-reshaping-cyber-insurance/. Accessed 20 July 2025.

International Trade Administration. "Sweden Country Commercial Guide." *International Trade Administration*, U.S. Department of Commerce, 18 12 2023, https://www.trade.gov/country-commercial-guides/sweden-cybersecurity. Accessed 20 7 2025.

"Italy - Cybersecurity." *International Trade Administration*, 23 January 2024, https://www.trade.gov/country-commercial-guides/italy-cybersecurity. Accessed 20 July 2025.

Kirichenko, David. "In the digital shadows, Belarusian cyber partisans unnerve Lukashenka." *NewEasternEurope*, New Eastern Europe, 8 5 2025, https://neweasterneurope.eu/2025/05/08/in-the-digital-shadows-belarusian-cyber-partisans-unnerve-lukashenka/. Accessed 20 7 2025.

McLeod, Riam Kim. "Iran's Cyber Strategy and the Israel-Iran Coflict." *SecAlliance*, SecAlliance, 13 6 2025, https://www.secalliance.com/blog/irans-cyber-strategy-and-the-israel-iran-conflict. Accessed 20 7 2025.

"National Cyber Security Strategy of Afghanistan (NCSA)." *ITU*, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Afghanistan_2014_National%20Cybersecurity%20Strategy%20of%20Afghanistan%20(November2014).pdf. Accessed 20 July 2025.

"National Cyber Strategy 2022 - Annual Progress Report 2022-2023." *GOV.UK*, https://assets.publishing.service.gov.uk/media/64e60e4b1ff6f3000d70ae7c/14.283_CO_National_Cyber_Strategy_Progress_Report_Web_v3.pdf. Accessed 20 July 2025.

Riaz, Sidra. "Cyber Warfare & Sovereignty: A Case Study of the Iran-Israel Cyber Conflict." *Paradigm Shift*, Paradigm Shift, 30 5 2025, https://www.paradigmshift.com.pk/iran-israel-cyber-conflict/. Accessed 20 7 2025.

Schmitt, Michael. "Germany's Positions on International Law in Cyberspace." *Just Security*, Just Security, 9 3 2021, https://www.justsecurity.org/75242/germanys-positions-on-international-law-in-cyberspace/. Accessed 20 7 2025.

Sharma, Abhishek. “North Korea's Cyber Strategy: An Initial Analysis.” *OBSERVER RESEARCH FOUNDATION*, 21 November 2024, https://www.orfonline.org/research/north-korea-s-cyber-strategy-an-initial-analysis. Accessed 20 July 2025.

“State Sponsors of Terrorism - United States Department of State.” *State Department*, https://www.state.gov/state-sponsors-of-terrorism. Accessed 20 July 2025.

“Strategy - 2023-2030 Australian Cyber Security Strategy.” *Department of Home Affairs*, 21 December 2023, https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy. Accessed 20 July 2025.

“Timeline: a history of cybersecurity.” *Global Defence Technology*, 13 August 2024, https://defence.nridigital.com/global_defence_technology_aug24/cybersecurity-timeline. Accessed 20 July 2025.

“2007 cyber attacks on Estonia.” *NATO Strategic Communications Centre of Excellence*, https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf. Accessed 20 July 2025.

“2007 cyber attacks on Estonia.” *NATO Strategic Communications Centre of Excellence*, https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf. Accessed 20 July 2025.

“UN General Assembly - First Committee - Disarmament and International Security.” *Welcome to the United Nations*, https://www.un.org/en/ga/first/. Accessed 20 July 2025.

Usman, M. “The Taliban's Cyber Caliphate.” *Modern Diplomacy*, 21 May 2025, https://moderndiplomacy.eu/2025/05/21/the-talibans-cyber-caliphate/. Accessed 20 July 2025.

“Who We Are.” *Cyber Security Agency of Singapore*, https://www.csa.gov.sg/about-csa/who-we-are/. Accessed 20 July 2025.