DPS MUN 2025

JODHPUR CHAPTER VIII

Carpe Diem
Carpe Noctem

BACKGROUND GUIDE DISEC

WARFARE 2.0: ADDRESSING EMERGING THREATS AND REDEFINING WAR CRIMES IN THE CONTEXT OF CYBER WARFARE AND DIGITAL CONFLICT

DPSMUN 2025

STUDY GUIDE

United Nations General Assembly
DISEC

DPSMUN 2025

Committee – UNGA DISEC

Agendum – Addressing Emerging Threats and Redefining War Crimes in the context of Cyber Warfare and Digital Conflict

LETTER FROM THE EXECUTIVE BOARD

Greetings Delegates,

As a part of the Executive Board, it is our responsibility to facilitate your educational experience at the simulation of the **UNITED NATIONS GENERAL ASSEMBLY - DISEC** at **DPSMUN 2025**. We would like to thank the organizers of **DPSMUN** for the constant encouragement that their platform provides. We are certain that attending this conference is an opportunity for all of us to come together, debate global issues and experience the art of diplomacy.

This background guide contains some basic elements on the topic that will guide your research. However, such mentions do not limit the scope of discussion in the committee at all. We expect from all delegates an active participation in the proceedings of this committee to have a fruitful discussion on a pertinent global problem. For that purpose, extensive and thorough research is expected of you over and beyond this study guide. Think of this study guide as merely an initiation to your research, defining the broad aspects.

We expect from all delegates an active participation in the proceedings of this committee to have a fruitful discussion on a pertinent global problem. For that purpose, extensive and thorough research is expected of you over and beyond this study guide. Think of this study guide as merely an initiation to your research, defining the broad aspects. This background guide will give you an overview of the topic at hand and the work of the Committee. It contains some basic elements on the topic that will guide your research. However, such mentions do not limit the scope of discussion in the committee at all. We are looking forward to fiery arguments, bizarre elucidations, and bursting sessions of diplomatic spectacle to amaze us.

With Warm Regards,

Parth Mangal (parthmangal.muns@gmail.com)

Khushi Agarwal (agarwalkhushi14aug@gmail.com)

(Executive Board)

THE NATURE OF PROOF/EVIDENCE IN COMMITTEE

EVIDENCE OR PROOF IS ACCEPTABLE FROM THE FOLLOWING SOURCES

→ **News Sources**:

State operated News Agencies – These reports can be used in the support of or against the State that owns the News Agency. These reports, if credible or substantial enough, can be used in support of or against any Country as such but in that situation, they can be denied by any other country in the council.

Some examples are –

1. Reuters *(Thomson Reuters Corporation)* (United Kingdom) https://www.reuters.com/
2. RIA Novosti (Russia) http://en.rian.ru/, IRNA (Iran) http://www.irna.ir/ENIndex.htm,
3. BBC (United Kingdom) http://www.bbc.co.uk/
4. Xinhua News Agency and CCTV (P.R. Of China) http://cctvnews.cntv.cn/

→ **Government Reports:**

These reports can be used in a similar way as the State Operated News Agencies reports and can, in all circumstances, be denied by another country. However, a nuance is that a report that is being denied bya certain country can still be accepted by the Executive Board as credible information. Examples are Government Websites like:

1. State Department of the United States of America: http://www.state.gov/index.htm,
2. Ministry of Defense of the Russian Federation: http://www.eng.mil.ru/en/index.htm,
3. Permanent Representatives to the United Nations Reports: http://www.un.org/en/members/(Click on any country to get the website of the Office of its Permanent Representative.
4. Multilateral Organizations like the NATO (http://www.nato.int/cps/en/natolive/index.htm)ASEAN (http://www.aseansec.org/), OPEC (http://www.opec.org/opec_web/en/), etc.

→ UN Reports:

(If Available)

All UN Reports are considered as credible information or evidence for the Executive Board of theGeneral Assembly.

1. UN Bodies: Like the SC (http://www.un.org/Docs/sc/), GA (http://www.un.org/en/ga/), HRC(http://www.ohchr.org/EN/HRBodies/HRC/Pages/HRCIndex.aspx) etc.
2. UN Affiliated bodies like the International Atomic Energy Agency (http://www.iaea.org/), WorldBank (http://www.worldbank.org/), International Monetary Fund (http://www.imf.org/external/index.htm), International Committee of the Red Cross (http://www.icrc.org/eng/index.jsp), etc. Treaty Based Bodies like the Antarctic Treaty System (http://www.ats.aq/e/ats.htm), theInternational Criminal Court (http://www.icc-cpi.int/Menus/ICC).

Under no circumstances will sources like Wikipedia (http://www.wikipedia.org/), Amnesty International (http://www.amnesty.org/) or newspapers like the Guardian (http://www.guardian.co.uk/), Times of India (http://timesofindia.indiatimes.com/) etc. be accepted as credible.

ABOUT THE COMMITTEE: UNGA DISEC

The **United Nations (UN) Disarmament and International Security Committee (DISEC)** was created as the first of the Main Committees in the General Assembly (UNGA) when the charter of the United Nations was signed in 1945.

THE GENERAL ASSEMBLY (UNGA)

(IMPORTANT PROVISIONS)

COMPOSITION

Article 9

1. The General Assembly shall consist of all the Members of the United Nations.
2. Each Member shall have not more than five representatives in the General Assembly.

FUNCTIONS AND POWERS

Article 10

The General Assembly may discuss any questions or any matters within the scope of the Charter or relating to the powers and functions of any organs provided for in the present Charter, and, except as provided in Article 12, may make recommendations to the Members of the United Nations or to the Security Council or to both on any such questions or matters.

Article 11

1. The General Assembly may consider the general principles of cooperation in the maintenance of international peace and security, including the principles governing disarmamentand the regulation of armaments, and may make recommendations with regard to such principles to the Members or to the Security Council or to both.

2. The General Assembly may discuss any questions relating to the maintenance of international peace and security brought before it by any Member of the United Nations, or by the Security Council, or by a state which is not a Member of the UnitedNations in accordance with Article 35, paragraph 2, and, except as provided in Article 12, may make recommendations with regard to any such questions to the stateor states concerned or to the Security Council or to both.

Article 12

1. While the Security Council is exercising in respect of any dispute or situation the Functions assigned to it in the present Charter, the General Assembly shall not make any recommendation with regard to that dispute or situation unless the Security Council so requests.
2. The Secretary General, with the consent of the Security Council, shall notify the General Assembly at each session of any matters relative to the maintenance of international peace and security which are being dealt with by the Security Council and shall similarly notify the General Assembly, or the Members of the United Nations if the General Assembly is not in session, immediately the Security Council ceases to deal with such matters.

Article 13

1) The General Assembly shall initiate studies and make recommendations for the purpose of:

a) promoting international co-operation in the political field and encouraging theprogressive development of international law and its codification;

b) promoting international cooperation economic, social, cultural, educational, and health fields and assisting in the realization of human rights and fundamental freedoms forall without distinction as to race, sex, language or religion.

VOTING

Article 18

1) Each member of the General Assembly shall have one vote.

2) Decisions of the General Assembly on important questions shall be made by a two-thirds majority of the members present and voting. These questions shall include: recommendations withrespect to the maintenance of international peace and security, the election of the non-permanent members of the Security Council, the election of the members of the Economic and Social Council, the election of members of the Trusteeship Council in accordance with paragraph 1(c) of Article 86, the admission of new Members to the United Nations, the suspension of the rights & privileges of membership, the expulsion of Members, questions relating to the operation of the trusteeship system, and budgetary questions.

PROCEDURE

Article 21

The General Assembly shall adopt its own rules of procedure. It shall elect its President for each session.

COMMITTEE ONE: DISEC

DISEC (Disarmament & International Security Committee) was formed to respond to the need for an international forum to discuss peace and security issues among members of the international community. According to the UN Charter, the purpose of DISEC in the General Assembly is to establish general principles of cooperation in the maintenance of international peace and security, including the principles governing disarmament and the regulation of armaments and also to give recommendations with regard to such principles to the Members or to the Security Council.

Although DISEC cannot directly advise the Security Council's decision-making process, the UN Charter explains that DISEC can suggest specific topics for Security Council consideration. Aside from its role in the General Assembly, DISEC is also an institution of the United Nations Office for Disarmament Affairs (UNODA). The UNODA is concerned with disarmament at all levels; nuclear weapons, weapons of mass destruction, and conventional weapons, and assists DISEC through its work conducted in the General Assembly for substantive norm-setting support to further its disarmament initiatives.

ABOUT THE AGENDA

INTRODUCTION

The advent and rapid expansion of computing systems has made technology an irreplaceable aspect of daily life. Financial activities, academic work, and communications have been revolutionized by technology, and the disruption of these technologies and networks can wreak havoc on a global scale. The low entry costs and wide availability of hacking tools makes Cyber-Crime, Digital Crime and Cyber Warfare extremely prevalent; up to 80 million cyber-attacks take place each day. Civilian services, private enterprise, and government operations all rely on technology; all manner of weapons systems, including drones and nuclear weapons, are controlled by networks that could be subject to hacking and attacks. Sensitive government information is also often stored online and past leaks have put numerous individuals, including informants and military operatives, in great danger.

Millions of cyber-attacks take place each day and combatting this growing threat will necessitate a multilateral and collaborative approach. Cyber security, cyber warfare, and cyber terrorism are easily confused and conflated; clearly defining these terms is important to ensure universal understanding. According to "**The Cyber Index**" released by the **United Nations Institute for Disarmament Research**, (**UNIDIR**), a cyber-attack may be defined as an unauthorized attempt to infiltrate, gain access to, or shut down a computer, system, or network. Therefore, cyber security can be defined as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets."

Cyber warfare is "***warfare conducted in cyberspace through cyber means and methods***." The United Nations (UN) does not yet have an official definition of neither cyber-terrorism nor terrorism itself, but broadly, cyber terrorism may be understood as the unlawful attack or threat of attack against computers and cyber networks to terrorize peoples, groups or governments. While some states and regional groups have made efforts to combat cyber warfare through robust legislation, the inconsistencies of legislation between different states hinder their efficacy. The **UN General Assembly (GA)** has made important strides in increasing dialogue between states on this issue, and implementing practical measures will be an important way

forward, particularly in addressing non-state cyber-attacks, securing intelligence and weapons systems from cyber-attacks, and strengthening legislation and accountability mechanisms.

INTERNATIONAL AND REGIONAL FRAMEWORKS

While cyber security, cyber warfare, and cyber terrorism are relatively newer security threats, many regional agreements and initiatives between states already exist to strengthen cooperation on cyber security and deter breaches.

One of the key regional conventions is the **Budapest Convention on Cybercrime (2001)** adopted by the Council of Europe. The convention, which entered into force in 2004, commits States Parties to standardize national legislation and regulatory measures regarding cyber-crime and related issues, including criminal prosecution and jurisdiction. To address the relative novelty of cyber-crime, as well as its transnational nature, the convention takes a dual-pronged approach: tailoring domestic criminal law to prosecute instances of cyber-crime, and also creating procedures to support greater international cooperation in this area. The convention additionally encourages greater interstate cooperation and information-sharing regarding cyber-crime and preventative security measures. While nearly all of the Council of Europe members are States Parties, several other non- European states have also ratified the convention.

There is also an African regional convention**,** the **African Union Convention on Cyber Security and Personal Data Protection (2014).** Adopted in 2014, this convention promotes regional cooperation and provides a legal framework for strengthening cyber security and combatting cyber-crime. The convention was drafted to provide a holistic framework to address the cyber security needs particular to the African continent and to prevent African states from becoming safe havens for cyber criminals. While more than one year after its adoption it has not yet been ratified by any signatory, many states have used it as a guide to enact domestic cyber-crime legislation.

In addition to regional arrangements, several United Nations bodies have also responded to the increasing threat of cyber warfare and cyber-crime. In 1999, the **GA adopted resolution 53/70** on information technology and communications in relation to international security, the first resolution on this topic. In addition to drawing an explicit link between information and

communication technologies (ICTs) and security, the resolution calls on states to outline definitions and central concerns, and requests the Secretary-General prepare a report on the topic. Since the resolution was adopted, the Secretary-General has produced several reports to the GA outlining Member States' perspective on the issue to share information and build consensus on a way forward. In 2003, the **GA passed resolution 58/32**, which created a Group of Governmental Experts (GGE) to assist the Secretary-General in drafting a report on cooperative measures to combat cyber threats and strengthen cyber security measures. The GGE has been renewed for several terms and is key in providing recommendations and guiding the work of the General Assembly and the UN Secretariat in addressing this issue. In 2013, the **GA adopted resolution 68/167** on "the right to privacy in the digital age." The resolution notes that while states and international organizations should take measures to combat cyber warfare, cyber-crime, and serious informational breaches, these should not be allowed to violate human rights, particularly one's right to privacy. In 2014, the **GA adopted resolution 69/28**, based on the GGE's most recent report on "Developments in the field of information and telecommunications in the context of international security." The resolution calls on all Member States to consider pressing cyber security threats, and to discuss and communicate strategies to combat these threats to encourage a collaborative and multilateral approach.

ROLE OF THE INTERNATIONAL SYSTEM

Many UN bodies are engaged in issues around cyber security and cyber warfare. In addition to the creation of the GGE and the adoption of multiple resolutions on the topic, the GA First Committee has sought to increase dialogue and cooperation by requesting that Member States submit their views on international law and opportunities for cooperation in cyberspace, which many states have done. Many states within the GA have expressed the need to discuss concrete measures for cyber security improvements, particularly information sharing and confidence building measures (CBMs). The latest GGE report also provides a set of recommendations to the General Assembly, including greater investment in researching ICT threats and increasing multilateral dialogue and cooperation in addressing these threats. In the recently adopted resolution 69/28 on "Developments in the field of information technology and telecommunications in the context of international security," the GA recognized the importance of greater cooperation on this topic but did not provide for any concrete action to achieve it. The GA added this topic to the provisional agenda of the Assembly's 70th session, and the issues were discussed in the October 2015 meetings in the First Committee. Some Member

States stated their belief for the need of a comprehensive, overarching approach to cybersecurity that accounted for state specific security "deficiencies," while others maintained that existing international law was best for "cyber-stability" and information security with the addition of specific cyber-related provisions; the different perspectives on cyber security highlight the fragmentation amongst Member States on achieving unified solutions.

The International Telecommunication Union (ITU), the UN agency focused on information and communication technology, is heavily involved within this topic. The ITU writes reports and recommendations on increasing technological and telecommunications access, as well as identifying emerging threats and challenges. In 2007, the ITU launched the Global Cybersecurity Agenda (GCA), a collaborative platform to encourage cooperation and information-sharing on cyber-security centered on the following five pillars: legal measures, technical and procedural measures, organizational structures, capacity building, and international cooperation. The GCA is guided by the High-Level Experts Group (HLEG), a group of cyber-security experts, which provides information and recommendations on strengthening cyber security to Member States and relevant stakeholders working on this issue.

The ITU also hosts the World Summit on Information Societies (WSIS), an intergovernmental forum established in 2001.While the fundamental goal of WSIS is to universalize access to ICTs, it also notes that to build a global information society, there must be "a global culture of cybersecurity" to protect users and encourage broader use and applications. In 2005, WSIS agreed to a set of outcome goals contained within the Tunis Agenda for the Information Society. The goals include expanding access to information technologies, encouraging international and regional cooperation, including capacity-building and information-sharing, and building confidence and enhancing security measures in the use of ICTs.

In addition to the ITU, the United Nations Office for Disarmament Affairs (UNODA) and the United Nations Institute for Disarmament Research (UNIDIR) have made important contributions towards understanding current security threats and identifying gaps in national and international security and legislation. UNIDIR has written numerous reports on the relationship between information technology and international peace and security, particularly in the way these systems may be used to control weapons systems. Additionally, UNIDIR has

produced important research on the legality of certain cyber security mechanisms and how international law might address these particular forms of attacks and terrorism. UNODA and UNIDIR also provide recommendations for best practices that guide the General Assembly and the Secretary-General. Individual Member States have also made important contributions in strengthening cyber security mechanisms. Many states, including the United Kingdom and the United States, have dedicated domestic offices and initiatives for cyber security. Internationally, many developed states are investing

In technical support and capacity-building projects aimed at strengthening developing states' ability to respond to cyber threats. States have also signed regional and bilateral partnerships, such as the one between the United States and Canada, to increase cooperation, but these are generally with close regional partners and have not expanded to include a wider international context. Additionally multilateral programs are playing a larger role in international cooperation, such as the Commonwealth Cybercrime Initiative (CCI), which was created at a multilateral forum of Commonwealth states in 2011. The CCI aims to increase cooperation and information-sharing between Commonwealth states, as well as various international and regional organizations, to reduce cyber-crime and strengthen accountability and enforcement mechanisms. Cyber security and cyber-crime also have important implications for civil society, and many international organizations are taking steps which include private sector businesses and civil society organizations as key stakeholders in their programs and discussions.

CYBER TERRORISM, CYBER WARFARE, AND NON-STATE ACTORS

The broad accessibility and reach of online networks have impacted the way non-state actors (NSAs) use technology to carry out cyber-crime and cyber-attacks against states and private entities. Many NSAs use technological networks to launch direct attacks against governments and international organizations. Threats of violence or attack are often carried out through the Internet to preserve anonymity, which creates panic and fear among the populace. Cyber networks may also be used to communicate details in the execution of a terrorist attack, as was the case in the 11 September 2001 attacks against the United States or to directly to launch an attack. Cyber-attacks may specifically target computer and cyber networks to release sensitive information or disrupt essential infrastructure. For example, in 2010, an attack code virus directed against a uranium-processing facility in Iran wreaked havoc, shutting down safety

protocols and disrupting the functioning of the refinery. States may also be intentionally complicit in non-state cyber-attacks against other states, private enterprises or international organizations by knowingly allowing groups to operate unhindered within their territory. Other states unwillingly harbor criminals due to a lack of security and monitoring mechanisms. The broad access of cyber networks makes it difficult for any one state to successfully target and eliminate online terrorist activity.

LINKS TO NON-CYBER CRIMES

Cyber warfare, cyber terrorism, and security breaches have very serious consequences for online networks and technology systems, but online activities can also have real implications for security threats that are carried out offline. Cyber-crime, including hacking, identify theft, and illicit financing, can be used to fund terrorist activities that take place offline. Reports have suggested that NSAs have been dealing in illicit online sales of human organs and counterfeit medicines to finance their organizations, in addition to more commonplace cyber-crimes such as fraud, credit card theft, and money laundering. In one instance, Younis Tsouli, an individual working with Al Qaeda, stole $3.5 million USD through credit card theft, which was then used to fund 180 websites hosting Al Qaeda propaganda videos. Charities and non-profit organizations have also been used as covers for illicit activity, with some organizations infiltrating and overtaking existing charities. The relative anonymity and high penetration of Internet financing tools, such as cell phone-driven transfers, make them an ideal way to raise funds globally. Internationally, the **International Criminal Police Organization (INTERPOL)** is a key actor in coordinating criminal and judicial responses between states. While on a national level many states have increased investigation and surveillance to capture these crimes, a lack of sufficiently detailed legislation specific to cyber-crime presents challenges in prosecuting these crimes.

ADDRESSING THE THREAT

The interconnected and expansive nature of cyber-crime has meant numerous and varied initiatives by states in creating effective solutions to deal with both cyber warfare and cyber-crime, as well as managing the offline impacts of online activities. Some states have responded to these threats with greater monitoring and law enforcement oversight to catch and prosecute cyber terrorism, but this is not universal due to the high cost and difficulty of implementation.

Other states have created and enforced stricter anti-money laundering legislation and monitoring to cut off financing, while others require identification to access certain computer networks. Some states have been successful in harmonizing cyber-crime and cyber security strategies and many more are working on implementing such strategies. These strategies include a range of activities from establishing awareness programs for users, making cyber-crime reporting mechanisms more accessible, and partnering with private financial institutions to increase security measures. The development of a more unified approach to cyber-crime represents a key opportunity for the international community to address.

SECURING INTELLIGENCE AND WEAPONS SYSTEMS

Increasing reliability and capacity of ICTs has impacted the way military information and weapons systems are maintained and protected. Sensitive security information, such as the identities and locations of informants, strategic weapons depots, and military strategies are kept electronically and are therefore subject to attack and release, jeopardizing the security of these materials. Cyber espionage and hacking are particularly salient due to releases of sensitive documents by organizations such as Wikileaks. Many leaks were accessed due to hacking, which has revealed the inadequate network protections of many states and international organizations, including the UN. The linkage of many weapons systems to cyber networks also makes them vulnerable to hacking and cyber-attacks. Nuclear weapons control systems can be attacked on an individual basis, such as a single missile, or on a broader level, by infiltrating overarching control structures. Increasing reliance on computers for multi-step verification and security procedures are intended to further fortify these systems and prevent them from accidental activation or use; however, many computerized weapons systems controls include multiple-step processes, remote override, automatic shut-downs, and other safeguards as enhanced security measures. However, the use of these complex cyber systems also increases the opportunity for hacks and security breaches. The inadequacy of existing measures to protect nuclear weapons systems has raised public concern about the security of the weapons themselves and the possibility of them being used as a result of security breaches.

Drones are also controlled and secured by computer systems, making them equally vulnerable to infiltration and unauthorized access. There has been evidence of military drones being hacked and picking up false signals meant to confuse the operating system. One of the

challenges of securing autonomous weapons systems (AWS) is their newness and the constantly evolving technology expanding their use and capabilities. The rapid change in technology necessitates constantly updated security protocols, therefore there are no existing best practices to guide the development of cyber security strategies for these weapons. While many security breaches and cyber-attacks are attributed to non-state entities, many states also attempt to breach and hack into others states' networks. In 2013, cyber-attacks on United States networks were attributed to operatives linked to the Chinese government. In response, China accused the United States of conducting similar intelligence-gathering attacks, to which the US admitted responsibility. State-sponsored cyber-attacks can exacerbate existing tensions and create challenges in addressing cyber security in a collaborative manner. While states have made some progress in initiating multilateral confidence-building measures to ease tensions and mistrust, they have largely been coordinated between states who are already cooperating on this issue, failing to address more pressing tensions and hostilities between states.

In order to create a climate of collaboration, CBMs at a bilateral or multilateral level will be an important step in increasing dialogue and cooperation on this issue. While the cyber vulnerabilities of weapons systems have been widely discussed internationally, the topic has not been formally addressed within the GA, thwarting open and productive conversations and the development of multilateral strategies. While there is significant concern that a breach of sensitive information or weapons systems could threaten international peace and security, there is no unified approach to protect against these attacks. Strengthening protections for lethal autonomous weapons systems (LAWS) is especially challenging as the legal standing of the weapons themselves is still the subject of great international debate. While the implications of LAWS are significant, there is pronounced disagreement on whether these weapons should continue to be developed, and whether any use of these weapons might contravene existing international law. Multilateral efforts to protect these weapons from attack will be extremely difficult to accomplish until the weapons themselves have been adequately discussed and monitored.

ACCOUNTABILITY AND LEGAL INSTRUMENTS

There remain significant challenges in ensuring accountability for cyber-crimes, both domestically and internationally. While many states have imposed strict legislation on cyber-

crime, cyber warfare, and cyber terrorism, the transnational nature of these crimes limits the effectiveness of varying national legislation and may also create challenges when tracking and prosecuting cyber-crimes that are committed in, and affect multiple states. Individuals or groups who find their cyber warfare activities limited or more heavily penalized in one state may move their activities to a state with weaker legislation against cyber warfare; however, the imposition of strict legislation in one state does not prevent that same state from remaining a target of cyber-attacks. While national initiatives and legislatures play an important role in increasing security measures tailored to their own needs, this approach also leads to inconsistencies between states, creating gaps in security.

Harmonizing national legislation between states and drafting a broader, global strategy to combat this issue will make it easier for different law enforcement agencies to work together to combat attacks originating from multiple states. The ITU has published a Cybercrime Legislation Toolkit to guide states in creating consistent legislation to combat cyber-crime, but states will also need to maintain open communication to ensure broader consensus on the way forward, particularly as new threats emerge and evolve. Determining jurisdiction is a significant challenge in prosecuting crimes of cyber warfare. Jurisdiction is the authority to apply and enforce a law; while it is usually based territorially, other features of a case, such as the location of the injured party or the origin of the perpetrator, may complicate and change jurisdiction. When crimes are committed by individuals or groups based in various states against another state, the jurisdiction over the crimes committed may be challenging to determine. Cyber-crimes are generally understood to involve a “transnational dimension” if the crime in question is committed and/or substantially planned in more than one country, or if it occurs in one state and has direct ramifications upon or within another state.

Additionally, between one-half to one-third of states believe their existing legislation is insufficient to address extraterritorial cyber-crimes; in these cases, having jurisdiction over extraterritorial crimes is not enough to ensure accountability for crimes committed. The fragmented and disparate nature of cyber networks and cyber warfare also make evidence-gathering and prosecution of cyber-crimes extremely difficult. Using firewalls, IP address blocks, and other tools, individuals committing acts of cyber warfare can hide their true location and thereby avoid prosecution. Without cooperation between various governments and agencies, individuals and groups can go undetected for years, continuing to launch attacks.

Even when the location of an individual or group can be located, evidence gathering, and therefore charging and prosecuting those responsible can be thwarted by the variation of laws across regions and states. The nature of electronic evidence often means it can be tampered with or altered with relative ease, muddying investigations. The inability to exercise effective control over evidentiary materials jeopardizes the admissibility of certain evidence, and thereby the strength of the case. Inconsistent monitoring and regulation mechanisms can make investigations across borders extremely difficult to conduct via traditional means. Finally, while legal instruments to both prevent and prosecute acts of cyber warfare are essential to preserving peace and security, some of these instruments have raised concerns about possible breaches of human rights. While the International Covenant on Civil and Political Rights (1966) states that combatting incitement to terrorism is sufficient basis to limit free expression, restrictions must be both necessary and proportional to the threat posed by propaganda. Some states have unjustly labeled controversial online content as a security threat, which has been used to silence political opposition and civil society. The ambiguousness and difficulty in proving that certain content does, in fact, incite terrorism makes it more difficult to block legitimately dangerous content, but also to identify cases where governments are using security as a pretext to silence opposition. In discussing a unified approach to cyber security, states must remain cognizant of their international human rights violations, and draft legislation with precision and respect for these rights.

CYBER ESPIONAGE

Espionage can be defined as "the practice of spying or of using spies to obtain information for the advantage of the self". It is typically carried out by governments to obtain military and political information. However, with the developments in the field of Information and Communications Technology (ICTs), this is no longer solely the domain of governments, as state as well as non-state actors are employing the use of computer networks for gaining illicit access to confidential information for personal gain. Cyber Espionage accounts for 22% of data breaches, with 87% of electronic spying conducted by governments, 11% by organized crime, 1% by competitors and the remaining 1% by a former employee. Cyber espionage is prevalent because it often has no or few consequences. These activities may get support from the home countries from which these criminals or crimes emanate; however, due to the nature of the Internet, it is sometimes difficult to tell from where the true source of an attack may be coming.

Cyber espionage is not confined by traditional regional borders and comprises a wide array of attack techniques that can be used against target-rich organizations.

In some countries, for instance, hacker clubs watched by the government become potential recruitment candidates for the nation-state-run cyber warfare units. The remote, hidden ability to capture proprietary data increases the criminal element's efficiency and effectiveness by reducing the time and expense of gaining the knowledge in a traditional manner. State support is also a reason why attribution is so challenging and, often, even impossible. In many instances, the information gleaned from cybercrime benefits a country's industrial development, race to market, or defense posture. Clearly, countries that have great cybercrime success would be unwilling to participate in any prosecution-based norm. Unless there is global agreement, criminal actors will simply move to where they can comfortably take root. Furthermore, when nation-states use crime ware from the APT (Advanced Persistent Threat) underworld, their attacks look like every other attack, so it is nearly impossible to determine attribution. In addition, cybercrime itself may offer nation-state actors a veil under which to hide while spying.

ROLE OF THE COMMITTEE

While preparing for this topic, delegates should consider how the General Assembly can address these challenges and build towards a more unified approach on cyber security. Specifically, delegates should consider: What legal frameworks would be helpful in drafting legislation on this topic? Delegates may also want to consider alternatives to legislation, such as capacity-building, CBMs, and the implementation of existing and new legislation. How can key challenges, including lack of coordination, multiple points of enforcement, and challenges of jurisdiction be overcome? Which UN organs and agencies would be well-suited to assist in strengthening cyber-security measures?

QUESTIONS TO PONDER

1. Has your nation had to respond to any internal cyber-attacks? If so, how?
2. As cyberspace lacks true borders, how can they be regulated between nations?
3. What defines an act of cyber warfare and how should cybersecurity be heightened to prevent them?
4. How can the international community lessen collateral damage that goes hand in hand with cyber-attacks or acts of cyber terrorism?
5. If any, what are the penalties for cyber terrorism in your country?
6. What actions has your country taken to prevent cyber-attacks within your own country?
7. What actions has your country taken to prevent cyber-attacks internationally?
8. What is the different procedure when dealing with a individual cyber attacker versus a sovereign state?
9. Should governments have a role in cyber security, and if so, what should that role be?
10. What is cyber warfare? How does it affect the international community?
11. As new technology emerges, what are some future security concerns regarding cyber-attacks?

ADDITIONAL REFERENCES

- https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf
- https://news.un.org/en/story/2017/07/560922-half-all-countries-aware-lacking-

national-plan-cybersecurity-un-agency-reports

- http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf
- https://www.cnet.com/news/un-chief-wants-international-rules-regulating-cyber-warfare/
- https://futurism.com/cyber-warfare-rules-protect-ourselves/
- https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram