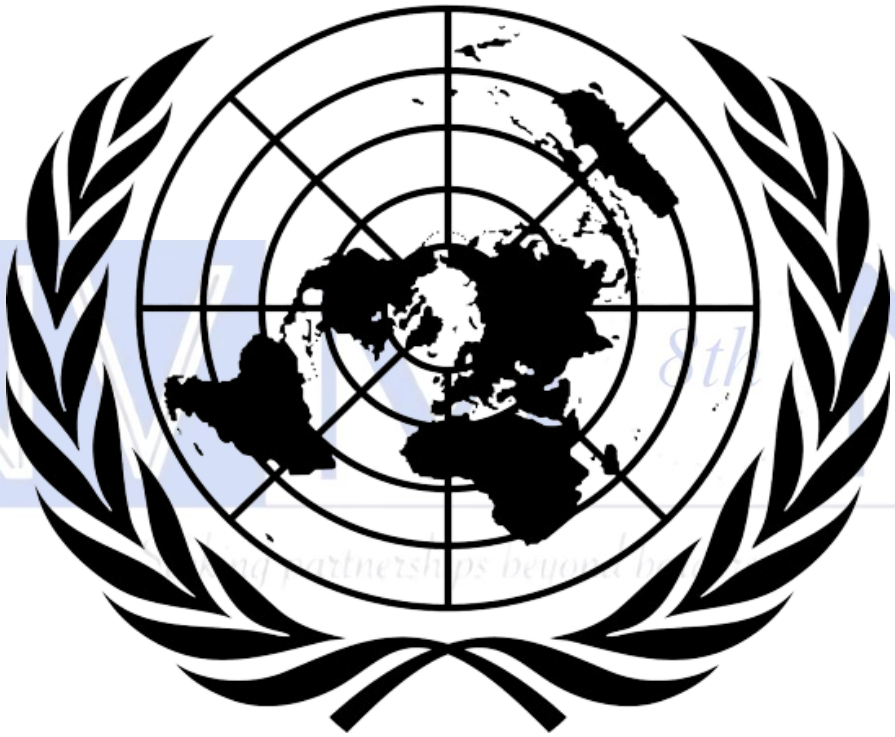
BACKGROUND GUIDE



UNITED NATIONS SECURITY COUNCIL

AGENDA: DISCUSSING CYBBER SECURITY AND STATE SPONSORED CYBER ATTACKS

INDEX

LETTER FROM THE EXECUTIVE BOARD

On behalf of the Executive Board, we extend a warm welcome to all of you and congratulate you on being a part of the United Nations Security Council (UNSC) at Nath Valley Model United Nations. We are sure that this background guide will give you a perfect launching pad as it encompasses a plethora of information that we believe will help you kickstart your research.

This being clear, kindly do not limit your research to the areas highlighted, but ensure that you logically deduce and push your research to areas associated with the issues mentioned. The Executive Board wants to make it clear that we are not looking for a repetition of existing solutions but adaptations and undeployed solutions presented in a practical manner are fair play.

Your goal should not be to recite your research and existing solutions but to put your minds to use for developing your own analysis of subject matters and bring forth novel solutions if possible. You can choose to learn more about it through the delegate resources provided and we will also conduct a session at the start of Day 1 to explain everything in detail. At no point during the debate will points be deducted for not knowing the procedure but it is encouraged to keep note of how Model UNs under this procedure work for a smooth discourse. We look forward to engaging with your diverse perspectives and contributing to the efforts of the UNSC during this simulation at Nath Valley Model UN. All the best!

Aryan Rakhe
Chairperson

Dhruv Surana
Vice Chairperson

TOPIC BACKGROUND

The growth of the Internet has allowed nations, organisations, and people to connect in ways previously unimagined. This new interconnectivity has allowed for collaboration, partnerships, and growth to reach unprecedented levels and has permitted the world to become a much smaller place. However, along with the benefits of the Internet, there are many new dangers created by this technology. The very nature of the Internet allows for individuals to hack information systems to steal information, cripple the delivery of services, and commit fraud. These cybercrimes are difficult to fight against, so it takes an international effort to combat them.'

This issue has come to the forefront in recent months after it came to light that organized hackers based in China were responsible for a series of hacks against American government offices and businesses? In 2015, the United States Office of Personnel Management was hacked which resulted in over 20 million government employees' sensitive information being leaked, including some confidential information about intelligence community officials? While government officials and experts have told press that the evidence demonstrates that the Chinese government was responsible for this breach*, the US government has not made an official statement on Chinese government involvement, and Chinese state media has denied any government involvement in the hacks', stating it was carried out by criminals within China'. In recent years, numerous hacks against businesses around the world have also been identified, perpetrated by groups ranging from underground hacking collectives like Anonymous, to cyber-wings of military organizations such as the Syrian Electronic Army' or ISIL. The objective of these hacks has been to steal or government secrets, cripple infrastructure, or co-opt communications systems, which angers corporations and governments wishing to protect their interests, their information, and their security.

INTRODUCTION TO THE AGENDA

One of the most significant challenges of the 21st century is the potential and existing threats to information security. These threats pose a significant risk to economies, national and international security, and public safety. The threats come from various sources and take the form of disruptive activities that target businesses, individuals, national infrastructure, and governments. These activities have the potential to cause substantial damage to the global community's stability, security, and economy. Information and communication technologies (ICTs) have significantly transformed the international security environment. While ICTs offer substantial economic and social benefits, they can also be employed for purposes that threaten international peace and security. Over the past few years, there has been a noticeable rise in the risk posed by ICTs as they are increasingly used for criminal and disruptive activities. The characteristics of information and communication technologies (ICTs) present unique challenges in addressing potential threats faced by states and other users. ICTs are widely available and omnipresent, lacking a clear distinction between civil and military use, and their purpose primarily depends on the user's intentions. The ownership and operation of networks are predominantly in the private sector or individual hands. The intricate interconnectivity of telecommunications and the Internet implies that any ICT device could be a source or target of increasingly sophisticated abuse. The malicious use of ICTs can be easily disguised, making it difficult to determine the origin, perpetrator, or motive of a disruption. In most cases, the perpetrators of such activities can only be identified through the target, effect, or circumstantial evidence. Threat actors have significant freedom to operate from virtually anywhere. These attributes enhance the prospects of using ICTs for disruptive activities.Since 2010, various bilateral, regional, and multilateral initiatives have emphasised the increasing importance of ensuring the secure use of ICTs, reducing risks to public safety, improving national security, and enhancing global stability. It is in the interest of all states to promote the peaceful use of ICTs and prevent conflicts arising from their use. Developing common understandings of norms, rules, and principles for using ICTs by states, and implementing voluntary confidence-building measures, can contribute significantly to advancing peace and security. While the international community's efforts to address this challenge to international peace and security are still in their early stages, there are several measures related to responsible state behaviour norms, rules, and principles that require further consideration. Effective cooperation among States is crucial to minimise risks to international peace and security and establish an accessible, stable, secure, and open ICT environment that benefits everyone.

THREATS, RISKS, AND VULNERABILITIES

Information and communication technologies (ICT) have become an integral part of our daily lives, transforming the way we interact, work, and conduct business. However, along with the benefits, there are also significant threats, risks, and vulnerabilities associated with ICT that can have a significant impact on individuals, organisations, and society as a whole.

- One of the most significant threats to ICT is cybercrime, which includes a wide range of malicious activities such as hacking, phishing, identity theft, and ransomware attacks. Cybercriminals can exploit vulnerabilities in ICT systems and steal personal or sensitive information, disrupt business operations, and cause financial harm
- ICT systems are also vulnerable to cyber attacks by state-sponsored actors, which can disrupt critical infrastructure, communication systems, and other essential services. These attacks can cause significant economic and social damage, affecting not just one country but also the entire region or even the world. In addition to external threats, ICT systems can also be vulnerable to insider threats such as employees with access to sensitive information who misuse their privileges for personal gain or sabotage. Insiders can also inadvertently cause data breaches or system failures. ICT systems are also prone to risks from human error, equipment failure, natural disasters, and other unexpected events. For instance, an accidental data leak or a power outage can cause significant disruptions to businesses and individuals.
- The global network of ICTs has become an arena for disruptive activity. The motives for disruption vary widely, from simply demonstrating technical prowess, to the theft of money or information, or as an extension of State conflict. The source of these threats includes non State actors such as criminals and, potentially, terrorists, as well as States themselves. ICTs can be used to damage information resources and infrastructures. Because they are inherently dual-use in nature, the same ICTs that support robust e-commerce can also be used to threaten international peace and national security. At present, terrorists mostly rely on these technologies to communicate, collect information, recruit, organize, promote their ideas and actions, and solicit funding, but could eventually adopt the use of ICTs for Attacks. States are also concerned that the ICT supply chain could be influenced or subverted in ways that would affect the normal, secure, and reliable use of ICTs. The inclusion of malicious hidden functions in ICTs can undermine confidence in products and services, erode trust in commerce and affect national security.

- The varying degrees of ICT capacity and security among different States increase the vulnerability of the global network. Differences in national laws and practices may create challenges to achieving a secure and resilient digital Environment.
- The potential for the development and the spread of sophisticated malicious tools and techniques, such as bot-nets, by States or non State actors, may further increase the risk of mistaken attribution and unintended escalation.

- The rapid increase in the use of mobile communications devices, web services, social networks, and cloud computing services expands the challenges to security.
- Different levels of capacity for ICT security among different States can increase vulnerability in an interconnected world. Malicious actors exploit networks no matter where they are located. These vulnerabilities are amplified by disparities in national law, regulations, and practices related to the use of ICTs. Overall, the threats, risks, and vulnerabilities associated with ICT systems are significant and ever-evolving. It is essential to adopt a proactive approach to manage these risks effectively, including implementing robust security measures, educating users on best practices, and continuously monitoring and updating ICT systems to prevent and detect potential threats.

MAJOR COUNTRIES AND ORGANISATIONS INVOLVED

GROUP OF SEVEN

In 1996, the Group of Eight
(8), established a subgroup on High-Tech crime that aimed to deal with
cybercrime. The Subgroup began with a mission to enhance the abilities of G8 countries to prevent, investigate, and prosecute crimes involving computers, networked communications and other new technologies?. Over time, the mission was expanded, and started to include work with Less Economically Developed Countries (LEDCs), on topics such as counterterrorism through the internet, and the protection of critical information. The main principles of this subgroup were:

1. There must be no safe havens for those who abuse information technologies.
2. Investigation and prosecution of international high-tech crimes must be coordinated among all concerned states, regardless of where harm has occurred.
3. Law-enforcement personnel must be trained and equipped to address high-tech crimes.

United States of America

The United States of America has a vital role in the global fight for cybersecurity and has been trying to develop methods for effective cybersecurity in the past decade. Being confronted by multiple cyberattacks conducted by other nations, it is crucial for them to address the issue with high priority.
The number of data breaches in the U.S. increased from 157 million in 2005 to 781 million in 2015, while the number of exposed records jumped from around 67 million to 169 million during the same time frame. In 2016, the number of data breaches in the United State. amounted to 1093 with close to 36.6 million records exposed.
With cybercrime increasing exponentially, it is only logical for the government to have created, invested and subsidized specialized agencies that focus on cybersecurity and general investigations on cybercrime. One good example is the National Cyber Security Division (NCSD) which is essentially a division within the United States Department of Homeland Security. The NCSD was first formed on June 6, 2003, and had 2 overarching objectives:
- [ ] To build and maintain an effective national cyberspace
response system.
- [ ] To implement a cyber-risk management program for protection of critical infrastructure.
Since its creation, the NCSD has increased the security of automated control systems that operate elements of the national critical infrastructure and has collaborated with the private sector and all sorts of stakeholders to increase cybersecurity and strengthen response and recovery methods. For further information on the United State's policies and strategies, you can click here to find out more.

China

While the Chinese government has been accused multiple times of conducting espionage on countries like Australia, Canada, the United States and India, it has taken steps to strengthen its cybersecurity in the past decade. On 7th November, 2016, China created a new law which was named "Cyber Security Law of People's Republic of China", which aimed to increase cybersecurity and national security, protect the rights and interests of citizens and promote healthy economic and social development. The law essentially:

1. Enhanced the principle of cyberspace sovereignty
2. Defined the security obligations of internet products and services providers
3. Detailed the internet service providers' security obligations
4. Perfected the rules of personal information protection
5. Established a security system for key information infrastructure.
6. Instituted rules for the transnational transmission of data at critical information infrastructure 25

Although the law faced some controversies, it has actually helped the Chinese Economy, as businesses have greater confidence, and are more willing to invest in certain projects such as Research and Development (R&D) in China.

Russian Federation

The Russian Federation has taken a different, more comprehensive and integrated approach to information security compared to Western Capital's focus on more technical network-centric cyber security26. Although Russia has focused extensively on the control of information, it has been affected by multiple cyberattacks, such as WannaCry (A ransomware attack that took in May 2017). Russia has previously stated that "uncontrolled information poses a threat to the government and society" and has shown a general interest in strengthening cybersecurity globally.

TIMELINE OF EVENTS

DATE	***DESCRIPTION OF EVENT***
1982	The first ever U.S. cyberattack on a Soviet gas pipeline takes place, resulting in its explosion.
1989	Tim Berners-Lee invents the World Wide Web
1997	The G7 Establish a committee on High-Tech Crimes
2000	United Nation Convention Against Transnational Organized Crime - Palermo Convention.
2000	The United Nations holds a conference on the Prevention of Crime and the Treatment of Offenders, which discussed computer related crimes.
2001	Convention on Cybercrime (Europe) - Budapest Convention
2004	The Convention on Cybercrime is created
2009	Creation of the Internet Governance Forum
2011	The Paris G20 summit suffered from a malware attack which gave access to hackers confidential G20 data.
2015	Germany Parliament Offices were compromised and internal data was uncovered.
2017	Ukraine Government Officials had malware on a Ukrainian tax website which spread the virus between other nations such as the United Kingdom, United States and France. Confidential information was lost.
2018	Northern Ireland Parliament Offices were hit by a brute force attack which gave hackers access to members' mailboxes.

INTERNATIONAL TREATIEAS AND RESOLUTIONS

There are several treaties and resolutions related to countering the use of information and communication technologies (ICTs) for criminal purposes, including cybercrime, terrorism, and other illicit activities. Some of the key international instruments in this area include

UN Convention against Transnational Organized Crime - This convention was adopted in 2000 and aims to promote international cooperation in preventing and combating transnational organized crime. It includes provisions related to countering the use of ICTs for criminal purposes, such as the use of the internet to facilitate human trafficking.

UN General Assembly Resolution 55/63 -

This resolution was adopted in 2000 and recognizes the need for international cooperation in combating the misuse of ICTs for criminal purposes. It encourages member states to adopt national legislation and cooperate with each other in preventing and combating cybercrime.

Budapest Convention on Cybercrime -

This is the first international treaty specifically designed to address cybercrime. It was adopted in 2001 by the Council of Europe and has since been ratified by more than 60 countries. The convention establishes a framework for international cooperation in investigating and prosecuting cybercrime, including provisions related to data protection, electronic evidence, and jurisdiction.

UN General Assembly Resolution 58/199

This resolution was adopted in 2004 and calls for the establishment of a global culture of cybersecurity and the protection of critical information infrastructures. It also encourages member states to strengthen their national cybersecurity capabilities and cooperate to prevent and combat cybercrime.

UNODC: Study Guide UN General Assembly Resolution 70/237 (2015) -

This resolution recognizes the potential of ICTs to promote sustainable development, while also highlighting the need to prevent their misuse for criminal purposes. It calls on member states to develop effective legal and regulatory frameworks to address cybercrime and to promote international cooperation in this area.

ASEAN Convention on Cybercrime -

This convention, adopted by the Association of Southeast Asian Nations in 2015, establishes a framework for regional cooperation in preventing and combating cybercrime. It includes provisions related to data protection, electronic evidence, and international cooperation.

UN Security Council Resolution 2322 (2016) -

This resolution calls on member states to prevent the use of ICTs for terrorist purposes and to strengthen their capacity to detect and respond to such threats. It also calls for increased cooperation and information-sharing among member states, as well as with the private sector.

UN Security Council Resolution 2321 -

This resolution was adopted in 2016 and imposes sanctions on North Korea for its nuclear and ballistic missile programs. It also includes provisions related to countering the use of ICTs for criminal purposes, such as the use of cyberattacks to generate revenue for the North Korean regime.

G7 Declaration on Responsible States Behavior in Cyberspace (2017) -

This declaration, adopted by the leaders of the G7 countries, affirms the importance of international law and norms in cyberspace and calls on all states to behave responsibly and refrain from using ICTs for malicious purposes. It also includes specific commitments related to improving cybersecurity and countering cybercrime.

These instruments represent important steps toward addressing the growing threat of cybercrime and other illicit uses of ICTs. However, their effectiveness depends on the extent to which they are implemented and enforced by individual states and on the level of international cooperation and information-sharing in this area

CASE STUDIES

A Byte Out of History

$10 Million Hack,

It was hardly the opening salvo in a new era of virtual crime, but it was certainly a shot across the bow.

Two decades ago, a group of enterprising criminals on multiple continents—led by a young computer programmer in St. Petersburg, Russia—hacked into the electronic systems of a major U.S. bank and secretly started stealing money. No mask, no note, no gun—this was bank robbery for the technological age.

Our case began in July 1994, when several corporate bank customers discovered that a total of $400,000 was missing from their accounts. Once bank officials realized the problem, they immediately contacted the FBI. Hackers had apparently targeted the institution's cash management computer system—which allowed corporate clients to move funds from their own accounts into other banks around the world. The criminals gained access by exploiting the telecommunications network and compromising valid user IDs and passwords.

Working with the bank, we began monitoring the accounts for more illegal transfers. We eventually identified approximately 40 illegal transactions from late June through October, mostly going to overseas bank accounts and ultimately adding up to more than $10 million. Meanwhile, the bank was able to get the overseas accounts frozen so no additional money could be withdrawn.

The only location where money was actually transferred within the U.S. was San Francisco. Investigators pinpointed the bank accounts there and identified the owners as a Russian couple who had previously lived in the country. When the wife flew into San Francisco and attempted to withdraw funds from one of the accounts, the FBI arrested her and, soon after, her husband. Both cooperated in the investigation, telling us that the hacking operation was based inside a St. Petersburg computer firm and that they were working for a Russian named Vladimir Levin. (See the sidebar for more on the San Francisco angle of the case from one of the agents who worked it.)

We teamed up with Russian authorities—who provided outstanding cooperation just days after a new FBI legal attaché office had been opened in Moscow—to gather evidence against Levin, including proof that he was accessing the bank's computer from his own laptop. We also worked with other law enforcement partners to arrest two co-conspirators attempting to withdraw cash from overseas accounts; both were Russian nationals who had been recruited as couriers and paid to take the stolen funds that had been transferred to their personal accounts.

In March 1995, Levin was lured to London, where he was arrested and later extradited back to the United States. He pled guilty in January 1998.

Believed to be the first online bank robbery, the virtual theft and ensuing investigation were a needed wakeup call for the financial industry…and for law enforcement. The victim bank put corrective measures in place to shore up its network security. Though the hack didn't involve the Internet, the case did generate media coverage that got the attention of web security experts. The FBI, for its part, began expanding its cyber crime capabilities and global footprint, steadily building an arsenal of tools and techniques that help us lead the national effort to investigative high-tech crimes today.

Botnet Operation Disabled

In an unprecedented move in the fight against cybercrime, the FBI has disrupted an international cyber fraud operation by seizing the servers that had infected as many as two million computers with malicious software.

Botnets are networks of virus-infected computers controlled remotely by an attacker. They can be used to steal funds, hijack identities, and commit other crimes. The botnet in this case involves the potent Coreflood virus, a key-logging program that allows cyber thieves to steal personal and financial information by recording unsuspecting users' every keystroke.

Once a computer or network of computers is infected by Coreflood—infection may occur when users open a malicious e-mail attachment—thieves control the malware through remote servers. The Department of Justice yesterday received search warrants to effectively disable the Coreflood botnet by seizing the five U.S. servers used by the hackers.

"Botnets and the cyber criminals who deploy them jeopardize the economic security of the United States and the dependability of the nation's information infrastructure," said Shawn Henry, executive assistant director of the FBI's Criminal, Cyber, Response, and Services Branch. "These actions to mitigate the threat posed by the Coreflood botnet are the first of their kind in the United States," Henry noted, "and reflect our commitment to being creative and proactive in making the Internet more secure."

SCOPE FOR DISCUSSION IN THE COMMITTEE

Impact on Global Stability: Discuss how state-sponsored cyber threats can destabilize international relations and global security.

Legal and Ethical Implications: Explore the legal frameworks and ethical considerations surrounding cyber warfare and state-sponsored cyberattacks.

Cyber Espionage: Highlight the methods and implications of state-sponsored cyber espionage, including its impact on national sovereignty and privacy.

Critical Infrastructure Vulnerabilities: Analyze the risks posed by cyber threats to critical infrastructure such as energy, transportation, and healthcare systems.

International Cooperation and Regulation: Evaluate the role of international organizations (like the UN) in regulating and mitigating state-sponsored cyber threats through cooperation and diplomacy.

Attribution Challenges: Discuss the difficulties in attributing cyberattacks to specific states and the implications for accountability and response.

Cyber Warfare Strategy: Examine state strategies in cyber warfare, including offensive capabilities, defensive measures, and deterrence strategies.

Human Rights and Cybersecurity: Consider how state-sponsored cyber activities intersect with human rights, including freedom of expression and privacy rights.

Impact on Economic Stability: Assess the economic consequences of cyber threats, including financial sector vulnerabilities and economic espionage.

BIBLIOGRAPHY

- https://digitallibrary.un.org/record/3831879?In=en
- https://documents-dds-ny_un.org/doc/UNDOC/GEN/N10/469/57/PDF/N1046957.pdf?
- https://documents-dds=ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf
- https://documents-dds-ny_un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf.
- https://rm.coe.int/1680081561
- https://www.itu.int/en/action/cybersecurity/Pages/un-resolutions.aspx