**Letter From the Secretary-General**

**Letter From the Under-Secretary-General**

**Introduction to the Committee UNOCT**

**Introduction to Hacking and Cybersecurity**

1. **Definition of Hacking**
2. **Why is Cybersecurity Important?**

**2.1. Vulnerableness to Cybersecurity**

**2.2. Commonness of Cybercrime**

**2.3. Invasion of Personal Privacy**

**2.4. Being a Threat to National Security**

**Hacking Spectrums**

1. **Black Hat Hackers**
2. **White Hat Hackers**
3. **Ethical Hackers**

**Historical Background**

1. **Early Origins of Hacking**
2. **Early Cybersecurity Measures and Improvement of Them**
3. **Major and Cybersecurity Incidents**
4. **Key Figures and Groups in Hacking History**

**International Strategies for Cybersecurity**

1. **Importance**
2. **Case Studies**

**Letter From the Under-Secretary-General**

***Letter from the Secretary-General***

*HASMUN'24 Secretary-General Letter*

*Most distinguished participants and dearest guests,*

*I am delighted to welcome you to the HASMUN’24 Conference of Kadir*

*Has University as the Secretary-General. Your participation and unique*

*perspectives will contribute to the success of this event.*

*With 8 diverse committees, each crafted to address the urgent need*

*forsolutions across a broad spectrum of specializations, we're set for*

*impactful discussions and innovative ideas. With our special 15th year of*

*Kadir Has University Model United Nations Club celebration, our*

*committees are:*

*• United Nations Office of Counter-Terrorism (UNOCT)*

*• International Atomic Energy Agency (IAEA)*

*• United Nations Population Fund (UNFPA)*

*• United Nations Industrial Development Organization (UNIDO)*

*• United Nations Office for Outer Space Affairs (UNOOSA)*

*• World Food Programme (WFP)*

*• International Monetary Fund (IMF)*

*• Historical Crisis Committee (HCC)*

*We, as the HASMUN'24 team, have made marvelous efforts to serve you,*

*participants, one of the greatest Model United Nations Conferences.*

*I want to conclude my words by thanking everyone involved in the*

*Academicand Organization teams for their greatest work. Delegates, I look*

*forward to your valuable contributions and meeting you in person.*

*#welcomehome*

*Best regards,*

*Aylin Rassad*

*Secretary-General HASMUN'2*

**A.Introduction to the Committee UNOCT**

UNOCT, or the United Nations Office of Counter-Terrorism, serves as the central coordination body within the United Nations system for all counter-terrorism efforts. Established in 2017, UNOCT aims to enhance the efficiency and effectiveness of the UN's counter-terrorism efforts. It provides guidance and support to member states in implementing the UN Global Counter-Terrorism Strategy and other relevant resolutions. UNOCT also works to strengthen national, regional, and international counter-terrorism capacities through various initiatives, partnerships, and activities. As a pivotal player in global security, UNOCT plays a crucial role in creating a sense of cooperation and collaboration among member states to address the multifaceted challenges posed by terrorism and violent extremism.

The United Nations Office of Counter-Terrorism (UNOCT) was approved in a resolution on 15 June 2017, with the consensus of the 193-nation [UN General Assembly](https://en.m.wikipedia.org/wiki/UN_General_Assembly).

2022 experienced paramount counter-terrorism milestones and achievements, despite the rise of new and complex challenges, including those rising because of the use of new and emerging technologies by terrorist groups. As the COVID-19 pandemic affected each and every nation both on an international and national level, UNOCT scaled up its efforts to help Member States achieve a world free from terrorism by adapting and innovating. In the unprecedented environment, promoting multilateral cooperation remained at the center of UNOCT’s work. The UNOCT Strategic Plan and Results Framework establishes a consolidated results framework capturing all outcomes under each of the Office's Strategic Goals, in support of its vision to Together, Build a Future Without Terrorism.

The UN Office of Counter-Terrorism (UNOCT) propelled a few activities within the field of cybersecurity and unused technologies. The UNOCT/UNCCT Cybersecurity and New Technologies program points to improve capacities of Member States and private organizations to anticipate cyber-attacks carried out by terrorist groups against basic framework.

The program looks to relieve the effect of cyber-attacks and recuperate and reestablish targeted systems such assaults occur.

In 2022, UNOCT/UNCCT and INTERPOL propelled the CT TECH activity, pointed at reinforcing capacities of law enforcement and criminal equity specialists in chosen partner nations to counter the abuse of new and emerging technologies for fear-based oppressor purposes, such as terrorist groups, as well as supporting Member States in leveraging new and rising advances within the battle against terrorism.

CT TECH is funded by the European Union and implemented under the UNCCT Global Counter-Terrorism Programme on Cybersecurity and New Technologies.

The Office also provides expertise in international fora on the use of unmanned aerial systems (UAS) and delivers capacity-building assistance in Open-Source Intelligence (OSINT), dark web, cryptocurrencies, and digital forensic investigations. Past UNOCT projects have focused on the use of social media to gather open-source information and digital evidence to counter terrorism and violent extremism while respecting human rights. CT TECH is financed by the European Union and actualized beneath the UNCCT Global Counter-Terrorism Programme on Cybersecurity and New Technologies. The Office moreover gives skill in universal fora on the utilization of unmanned aerial systems (UAS) and conveys capacity-building help in Open-Source Intelligence (OSINT), dark web, cryptocurrencies, and digital forensic investigations.

Past UNOCT ventures have centered on the use of social media to capture open-source data and computerized evidence to counter terrorism and violent extremism regarding human rights.

**B. Introduction to Hacking and Cybersecurity**

1. **Definition of Hacking**

Initially, the word “hacking” meant a sort of commitment to create and innovate computer programming, therefore, hackers were thought of as the valuable brains behind the computer revolution. But the word started to be referred to people who are committing acts such as computer crime, network intrusion, and even cyberterrorism quite quickly. Under these circumstances, hackers have been usually known as a threat to cybersecurity. This usage has become so dominant that it’s almost not known that other meanings exist.

Now, even though the term hacker is associated with a security hacker, (someone who can access data and break into computers via their knowledge of bugs or exploits that would be inaccessible under normal circumstances.) hacking can also be used by legitimate figures in legal situations. For example, law enforcement agencies can use hacking to gather evidence on criminals, which can include the usage of anonymity tools like VPN or “dark web” to mask their identities and imitate criminals.

1. **Why is Cybersecurity Important?**

**2.1. Vulnerableness to Cybersecurity**

We can send any data like videos, photos, or emails instantly in today's world. However, we rarely think about the protection of our data in our everyday life. Among many websites and applications we use, there has been an inclination towards using protections like warning users when they choose a weak password, data encryption, firewalls with default settings, and virus protection. Cybersecurity assures that organizations keep their security protections and user assets against any type of possible security risks in the cyber environment.

Our data becomes pretty much vulnerable as soon as it’s put on the internet to cybercrime but we are also really reliant on information systems and connected digital technology.

**2.2. Commonness of Cybercrime**

Cybercrimes are more common than we think. Over half a million people are affected by cybercrime in 2024, even though it’s just the very beginning of the year.



**2.3. Invasion of Personal Privacy**

Being a cybercriminal means that you are an expert at finding new ways to steal sensitive information. It is no longer effective to have a strong password as it used to be to protect the person's data.

540 million Facebook profiles and user records were exposed in 2019, and more than 3 billion Yahoo accounts were part of a 2013 breach that exposed names, birth dates, email addresses, and passwords. As a result, more than 14 million people (1/15 people) fall victim to identity fraud each year.

**2.4. Being a Threat to National Security**

According to the Department of Homeland Security, “Our daily life, economic vitality, and national security depend on a stable, safe, and resilient cyberspace.” It’s a national security issue because the amount of unprotected databases and networked systems creates an area to foreign nations, terrorists and extremist groups that aim to disrupt physical basis, gain an economic advantage, steal state secrets and erode confidence in citizens.

**C. Hacking Spectrums**

1. **black hat hackers**

Black hat hackers are individuals who engage in unauthorized and often malicious activities in cyberspace. They may also release malware that destroys files, holds computers hostage, or steals passwords, credit card numbers, and other personal information. Their characteristics include:

Illegality and operating outside the boundaries of the law, breaking into systems, stealing data, or disrupting services. They often work anonymously to avoid any possible detection.

Many black hat hackers are driven by financial gain, either through direct theft or by selling stolen data or services on the dark web.

Black hat hackers tend to lack ethical considerations and exploit vulnerabilities without regard for the consequences.

**characteristics and motivation**

Black hats or also known as malicious hackers primary motivation is collective, personal, or financial gain. These hackers may be amateurs, professional criminals, or nation-state or terrorist supported. Occasionally, they may also be insiders, employed, formerly employed, or affiliated with the victim.

**used tactics and techniques**

The way they use their tactics and techniques may be listed as:

The exploit of weaknesses in software, networks, or human behavior to gain unauthorized access.

They may create malicious software such as viruses, worms, ransomware, or trojans to compromise systems or steal data.

The usage of deceptive emails or websites to trick individuals into revealing sensitive information like passwords or credit card details. The manipulation of people into revealing confidential information or performing actions that compromise security is expected by Black hat hackers as well as distributed denial-of-service (DDoS).

These attacks are a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

**examples**

Kevin Mitnick was once considered to be the most wanted cybercriminal in the United States, Mitnick gained unauthorized access to several computer systems and got away from law enforcement for years.

Gary McKinnon, hacked into numerous of United States military and NASA computers over a year period, causing significant disruptions and leaving messages concerning of U.S. foreign policy.

Evgeniy Bogachev was a Russian hacker believed to be responsible for the GameOver Zeus botnet, which was used for stealing millions of dollars from bank accounts worldwide.

1. **white hat hackers**

**responsibilities**

The term white hat refers to an ethical hacker whose job involves hacking into computer systems in order to detect security risks.

When a company is in meed of testing its information system’s security, it hires white hats to attempt to hack information systems. This ethical hacking process helps detect vulnerable parts in a system.

The responsibilities of a white hack are listed below as:

Being responsible for reverse engineering malware and viruses,

Analyzing attacks and security incidents for their root causes,

Scanning a target network with vulnerability scanners,

Designing plans of attack to try and exploit (and then patch) vulnerabilities,

Providing technical support,

Reviewing and updating documentation.

**contributions to cybersecurity**

White hacking, also known as ethical hacking, offers numerous benefits and developments to organizations in today's evolving digital landscape. By actively picking out vulnerabilities and weaknesses in their systems, companies and organizations can enhance their overall cybersecurity stance and protect sensitive data from malicious attacks.

1. **ethical hacking**

**Definition**

There are different types of hacking. These are:

White-hat hacking,

Black-hat hacking,

Grey hat hacking,

Miscellaneous hacking.

Ethical hacking, also known as penetration testing or white-hat hacking, is the practice of deliberately attempting to transfixing a computer system, network, or application with the owner's permission and request. The main goal of ethical hacking is to identify and address security vulnerabilities before malicious hackers can exploit them for purposes that benefit them.

**Importance**

Ethical hacking is important for cybersecurity because it is used to secure crucial data from adversaries. Ethical hacking helps prevent malicious actors from exploiting the organization or an individual. It also helps bolster cybersecurity measures and reduces the risk of getting blackmailed.

**tools and techniques**

Ettercap is a tool used in ethical hacking. It combines network and host analysis features. An SSH connection can be sniffed by using this program. It allows using API to create custom plugins. It helps add a few characters to the server or a customer's network when interacting in real life. It also supports passive protocols and a thorough examination of the action.

Netsparker: This is the newest web application security scanner, which finds vulnerabilities in web applications. It is available as a SAAS product. It uses the most recent scanning technology to help detect dead vulnerabilities. In addition, it has a very low configuration requirement and can quickly analyze over 1000 web apps.

One of the ethical hacking tools that aids in directing security tests is the Burp Suite. For testing web applications, this is useful. It includes several tools that support the testing procedure as a whole.

It is capable of identifying over 2000 online applications' spam. Open-source software programs can be scanned by it. Additionally, it has the ability to identify malware and defects using advanced examination techniques precisely.

One of the most well-known tools for cracking passwords is John the Ripper. It also facilitates the password strength test. Brute force technology is used by this program to crack passwords. The kind of password encryption is automatically detected. It is the greatest password-hacking tool because of this feature. Several algorithms, including MD4, LDAP, DES, Hash LM, and others, are used by this program.

One open-source security tool is called Nmap. It is mostly used to monitor and assess operating system and organizational security. Experts in information security make use of it. It was used for both local and distant hosts to set up viruses, network audits, network mapping, etc.reshark: Using open-source hardware for ethical hacking is also permitted. It enables real-time network traffic investigation. Sniffing technology is used. It includes a number of highlights, including the Packet browser, Power GUI, and export results in multiple configurations. Additionally, it supports a variety of protocols. Also, it is available for other operating systems, including Linux, Windows, Mac, etc.

Moral hacking is a specialty of White-Hat hacking. Some of the techniques for ethical hacking are listed below:

Phishing,

Sniffing,

Social Engineering,

SQL injection,

Session hijacking,

Footprinting,

Enumeration,

Cryptography and so on.

These hacking strategies help Ethical hackers to stabilize systems and networks more securely.

**D. Historical background**

**Early Origins of Hacking;**

**World War II Era (1939–1945):** When we look at the stages of development in human history, we can easily say that technological developments always gather speed under the conditions of competition, and the most effective and full-scale competition occurs in basically war times.

In times of WW2, huge military operations were dedicated to break the codes and ciphers used by the Axis Powers to transmit crucial and encrypted information. In 1939, Alan Turing, Gordon Welchman, and Harold Keen developed “The Bombe”, known colloquially as the Turing Machine, which is the first universal machine that translated and worked with any symbols and also an advanced electronic device that capable of deciphering the messages that were encrypted by The Enigma Machine.

Another codebreaking mission at Bletchley, USA, involved breaking the Lorenz cipher, another encryption machine developed by German engineers in 1945. The codebreakers in Bletchley developed the Colossus Machine (the first semi-programmable electronic computer).

These developments in codebreaking during wartime laid the groundwork for modern computing and cybersecurity.

**Internet Kicks In (1970–1995):** Since it first emerged, the internet has always been a huge focus of interest among technology enthusiasts who want to exploit the system’s vulnerabilities, and these interests would soon make its impact felt by the entire world.

Kevin Mitnick, one of the most infamous hackers in history, was a technology enthusiast who was initially interested in radio and computing. He managed to penetrate some of the most highly guarded networks in the world, especially in the USA, including Nokia and Motorola, from 1970 until he got caught as a result of an operation led by the FBI in 1995. He was eager to learn how the system works, but that desire led him to become one of the most wanted criminals in American history. And when he was imprisoned, he wasn’t able to access any kind of phone or internet-connected devices for security reasons.

In summary, Kevin Mitnick's hacking exploits highlighted the importance of cybersecurity in an increasingly connected world.

**Early cybersecurity measures and improvement of them;

Bob Thomas and The Creeper (1970’s):** The history of cybersecurity is considered to have started in 1971, when Bob Thomas, a programmer and a scientist, programmed a virus that was used for security-related reasons. It was not vicious; on the contrary, it has helped to fill the gaps in security that have occurred with the globalization of the internet.

That virus, named after a villain in the popular show Scooby Doo, "Creeper,” was designed to protect the forerunner of the internet, which is ARPANET (Advanced Research Projects Agency Network). ARPANET was established by the U.S. Army to make it possible to run all military instruments in a synchronized manner.

**First antivirus softwares for public use (1980’s):** In 1987, it was going to be the year that not just one but multiple commercial antivirus softwares were published. In fact, there were debates and competitions between three major developers about who developed the first antivirus software on that date.

1) Andreas Lüning and Kai Figge released their first antivirus software to be used on the popular home computer Atari ST.

2) In Czechoslovakia, Peter Paško, Rudolf Hruby, and Miroslav Trnka have successfully developed and published the first version of the NOD antivirus, which is known as ESET NOD32, today.

3) And in the USA, computer programmer and business manager John McAffe founded the McAfee company, which became one of the best antivirus software programs today.

These developments marked the beginning of the antivirus software industry, which continues to play a critical role in protecting computer systems worldwide.

**Internet Becomes Global (1990’s):** Since the internet started to become widespread around the globe, people have started to put their personal and important information on the internet, like credit card information, addresses, etc.

And naturally, expecting computer-specialized criminals to ignore that potential source of money would be foolish. They immediately started to steal data from people and governments via the Web. By the middle of the 1990s, internet security had increased incrementally, and firewalls had to be coded for public usage even faster.

In 1991, the European Institution for Computer Antivirus Research (EICAR) was founded to improve the development of antivirus software.

**Threats getting even more serious (2000’s):** In the early 2000’s, crime organizations started to carry out professional cyberattacks and governments began to increase security measures and so the definition of hacking as a crime was greatly expanded. Governments have started to give much more serious criminal sentences to the hackers engaged in malicious hacking actions.

1. **U.S. Cyber Security Strategy (2003):** In 2003, The U.S. started to focus on preserving national security by applying a strategy against cyber espionage and attacks. This strategy aimed to reduce cyber threats, strengthen military defense, and enhance internal cooperation.
2. **China’s Cyber Security Laws and Security Measures:**
	1. **China’s Great Firewall:** In 2013 the Government of China has introduced a national security system called “Great Firewall” to control the internet as a whole and prevent cyber attacks. This system restricts the internet usage for the Chinese People and blocks access to foreign websites.
	2. **Chinese CyberSpace Strategy:** In 2016, China introduced a new cyber strategy which outlines China’s aim to ensure national security and secure protection against cyber crimes and espionage. The strategy is determined to strengthen China’s cyber infrastructure and increase international cooperation.
3. **EU General Data Protection Regulation (2016):** The EU adopted the GDPR to ensure the protection of personal information about EU citizens and to protect against cyber espionage. This agreement regulates the data process of EU citizens by companies in the EU. Just like in many other areas, the European Union has very strict regulations regarding the protection of personal data and internet security. Some principles and their detailed information are listed below.
	1. Personal data shall be:
		1. processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);
		2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with [Article 89](https://gdpr-info.eu/art-89-gdpr/)(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);
		3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
		4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

**Major and cybersecurity incidents**

**The Morris Worm (1988):** One of the first major cybersecurity incidents was the “Morris Worm,” which was created by a student at Cornell University named Robert Morris in 1988. It was the first global “worm attack” that affected and spread rapidly through computers.

Morris's initial objective was actually to map the entire internet by creating a computer worm program that replicates itself and essentially spreads to every computer on the internet. Morris neglected to mention a significant issue, though: the worm had the ability to re-infect a computer that it had already infected. The worm program had a one-in-seven chance of spreading to a computer that it had already infected. This was a remarkably high ratio, given that the internet in 1988 only had 60.000 machines linked to it.

Gradually, that one in seven chance was enough for computers to run hundreds or even thousands of copies of the relatively small worm program; eventually, thousands of copies of this small worm program were operating on every computer connected to the internet. The answer was eventually discovered by unplugging, cleaning, and then reconnecting all internet-connected PCs.

**Operation Moonlight Maze (1996–1999):** Moonlight Maze was a U.S. governmental investigation into a huge data breach involving classified information. The first phase of organized attacks started in 1996 and hit NASA, the Pentagon, state universities, and personal technological devices by Russian hackers. In fact, despite the enormous data breach and insecurity, it wasn’t discovered until the end of 1998, when some of the investigators detected suspicious activities in restricted files.

The U.S. authorities were outrageous yet calm enough to establish a task force named Moonlight Maze that was composed of 40 experts working on law enforcement, the military, and government. These experts have claimed that if all the stolen files were put on top of each other, they would be three times higher than the Washington Monument, which is 169 meters tall.



It was obviously the Russian government that was blamed. However, there was not enough evidence to support the accusation of the U.S. that the attacks were governmental, except for an IP address located in Moscow. Nevertheless, a few weeks later, a small cyber crime team that works in the Air Force Office of Special Investigations decrypted the Moonlight Maze code commands and found out the codes were crypted in Cyrillic, which has helped to confirm that Russia was behind the cyber attacks.

Classified naval codes, information on missile guidance systems, and other highly valuable military material were among the information retrieved during the breach. Tens of thousands of files, including technical studies, military maps, U.S. troop configurations, military hardware designs, encryption techniques, and information about the Pentagon's war strategy, were also taken by the attackers and made available to anyone willing to pay for them.

The potential for catastrophic destruction and the crippling of US missile defense systems existed for anyone who obtained the stolen material. The result was a review of US cybersecurity procedures. The Pentagon had improved its firewalls and intrusion detection systems in addition to ordering $200 million in new cryptographic equipment as a result of the attack's discovery and investigation, according to the same ScienceDirect piece.

**WannaCry Ransomware Attack(2017):** The WannaCry ransomware attack was a huge worldwide cyberattack that occurred in May 2017 by the WannaCry cryptoworm (a computer worm that encrypts data in victim's computer and demands money to decrypt it), which targeted computers that specifically used Microsoft operating systems. The reason behind this distinction was that the WannaCry cryptoworm had benefited from a vulnerability caused by the leaking of the source codes of EternalBlue, which is an exploit developed by the United States to target computers using Microsoft operating systems. Once a computer is infected, the worm encrypts the files and displays a ransom note that tells its required to be ransomed to get access to the encrypted files.



However, just a day after the attacks, Microsoft officially released security updates for outdated products like Microsoft XP, Windows Vista, and Windows 8, and organizations were advised to update their operating systems in order to protect themselves from further threats.

A few days after the attack, WannaCry was temporarily neutralized. A security researcher discovered a "kill switch" that essentially turned off the malware. However, many affected computers remained encrypted and unusable until the victims paid the ransom or were able to reverse the encryption.

The attack had a huge impact on businesses, hospitals, and other organizations. It disrupted operations and caused lots of financial damage, and it also highlighted the importance of regular Microsoft updates. Never forget to update your Windows!

**History of a Utilitarianist Aspect of Hacking: White Hat**

Just like in every field of history, when a new tool emerges, there will be those who seek self-interest as well as those who want to use it for society itself. The implication of this issue on hacking was just like the way history proved it.

In the early days of hacking, the term white hat was not widespread at all. Instead, hackers were generally classified as black hats who used their skills in computing for their personal purposes or gray hats who plied between the dark side and the light side.

One of the first instances of an ethical hack being used was a security evaluation done by the United States Air Force, and this evaluation revealed the existence of some security vulnerabilities.

White hat operations were characterized as a "mischievous but perversely positive 'hacker' tradition" by The New York Times in 1981. The company penalized a National CSS employee for not revealing the password cracker sooner rather than for writing it after he reported its existence and how he had used it on client accounts. The warning letter read: "The company realizes the benefit to NCSS and encourages the efforts of employees to identify security weaknesses in the directory and other sensitive software in files."

As a result, the hacking community has experienced an important evolution with the rise of ethical hacking, often known as white hat hacking, that emphasizes a better way to use hacking skills for society itself. History has shown that there was not any difference between ethical and malicious hacking in the early stages of the field. But as the importance of cybersecurity became more clear, the necessity of ethical hackers to find security gaps and protect systems became more apparent as well. ⁤

**Key figures and groups in hacking history**

**Adrian Lamo:** Adrian lamo, a.k.a. “homeless hacker” had an infamy because of his attacks that targeted some top tier computer networks. He hacked systems belonged to Microsoft, Yahoo!, and The New York Times. But unlike other malicious hackers, Lamo’s intention was to fix their security gaps for free rather than damage them. Lamo was eager to be hired by a cybersecurity company, but by the time, his infamous registry prevented him from being hired by any company.

**Gary McKinnon:** Garry McKinnon was a notorious British hacker that harmed more than 90 U.S. and NASA computers. He deleted critical files related to operating systems which caused a complete shutdown in computers located in the United States Army’s military district in Washington. McKinnon also left a note on the military’s website saying “your security is crap”

But the more interesting thing is, McKinnon’s motivation was one of a kind: he believed that UFOs are real and the U.S. was covering them. He claimed to be searching for evidence of UFOs and free energy suppression.

**Anonymous:** An unofficial online community of hackers and political activists, Anonymous got its start in 2003 as a collective on the anonymous discussion board 4chan. Social network platforms and encrypted online chat rooms are used by members of the Anonymous community for communication and collaboration. The group is best known for its cyberattacks against corporations, the Church of Scientology, governments, and government-affiliated organizations.

People who want to be identified as members of the group hide their identity in public by wearing Guy Fawkes masks. Guy Fawkes, also referred to as Guido Fawkes, was one of several medieval English Catholics who participated in the failed assassination attempt of 1605 known as the Gunpowder Plot. An attempt was made with the Gunpowder Plot to ensure greater religious tolerance under King.

**E. International Strategies for Cybersecurity**

1. **Importance**

**National Security**: Given the wide adoption of digital technologies across economies and societies, cybersecurity has become increasingly important to a country’s national security. It encompasses military security, political security, economic security, and cultural security.

**Impact on International Trade:** Digital trade is crucial for almost every company, but it also introduces new complications. When products or services that contain a computer or can be connected to the internet cross borders, cybersecurity risks emerge. Concerns about foreign states or corporations abusing digital products to collect privacy data, plant vulnerabilities, or cause harm mean that digital products sold across borders are subject to increased scrutiny and controls. Companies can be targeted for bans by host governments, affecting their ability to operate internationally.

**Geopolitical Implications:** Cybersecurity is intertwined with geopolitics. How a country reacts to cybersecurity threats is influenced by national capability in managing cyber risks, the level of trust between the government and business, and geopolitical factors. Companies need to prepare by building strong cybersecurity governance cultures, playing politics, developing exit and re-entrance plans for markets, and helping host governments improve their cybersecurity capabilities.

**Reputational Impact:** Cybersecurity breaches can have a devastating impact on business reputations. Companies that fail to protect their networks and data may face negative publicity, loss of customer trust, and damage to their brand image globally.

International Cybersecurity Priorities: Fostering Cybersecurity Innovation Globally U.S. Department of Commerce June 26, 2017

1. **Case Studies**
* **Small Business Cybersecurity Case Studies by NIST:**
* NIST (National Institute of Standards and Technology) provides a series of case studies illustrating common cybersecurity challenges faced by small businesses:
	+ ATM Skimming and Bank Fraud: A business trip to South America led to ATM skimming and bank fraud.
	+ Construction Company Keylogger Attack: A construction company fell victim to keylogging malware and bank fraud.
	+ Stolen Hospital Laptop: A stolen laptop from a hospital caused security concerns due to lack of encryption.
	+ Hotel CEO’s Email Compromise: Unwanted guests infiltrated a hotel CEO’s email account
* **Kroll’s Cyber Security Case Studies:**
* Kroll, a global leader in risk management, shares case studies showcasing successful cybersecurity initiatives:
	+ Reducing Hospitality Company’s Cyber Risk: Managed detection and response.
	+ Enhancing Asset Management Firm’s Security Visibility: Managed detection and response.
	+ Elevating Housebuilding Company’s Cyber Security Maturity.

**References**

[https://en.wikipedia.org/wiki/United\_Nations\_General\_Assembl](https://en.wikipedia.org/wiki/United_Nations_General_Assembly)y

<https://www.un.org/counterterrorism/>

<https://www.un.org/counterterrorism/cybersecurity>

*Editorial: introduction to hacking and hacktivism - David J. Gunkel Northern Illinois University, USA*

<https://en.wikipedia.org/wiki/Hacker>

*Cyber Security and Ethical Hacking: The Importance of Protecting User Data*

*Importance of Cyber Security in Digital Era - Prof. Ms. Tejaswini Untawale*

[www.statista.com](http://www.statista.com)

<https://online.utulsa.edu/blog/why-is-cybersecurity-important-top-six-reasons/>

<https://www.kaspersky.com/resource-center/definitions/hacker-hat-types#:~:text=Black%20hat%20hacker%20definition,numbers%2C%20and%20other%20personal%20information>[.](https://www.kaspersky.com/resource-center/definitions/hacker-hat-types#:~:text=Black%20hat%20hacker%20definition,numbers%2C%20and%20other%20personal%20information.)

[https://www.cisecurity.org/insights/spotlight/black-gray-white-hat-hackers#:~:text=Black%20hats%20–%20malicious%20hackers%20whose,or%20affiliated%20with%20the%20victim](https://www.cisecurity.org/insights/spotlight/black-gray-white-hat-hackers#:~:text=Black%20hats%20%E2%80%93%20malicious%20hackers%20whose,or%20affiliated%20with%20the%20victim)

<https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/>

[https://en.m.wikipedia.org/wiki/Black\_hat\_(computer\_security)](https://en.m.wikipedia.org/wiki/Black_hat_%28computer_security%29)

<https://www.tripwire.com/state-of-security/the-ten-most-wanted-hackers-by-the-fbi-10>

<https://www.coursera.org/articles/what-is-a-white-hat?utm_medium=sem&utm_source=gg&utm_campaign=b2c_emea_coursera_ftcof_career-academy_arte_march_24_dr_geo-multi-set3_pmax_gads_lg-all&campaignid=21103949440&adgroupid=&device=t&keyword=&matchtype=&network=x&devicemodel=&adposition=&creativeid=&hide_mobile_promo&gad_source=1&gclid=Cj0KCQjwhtWvBhD9ARIsAOP0GoiJBdEtybt66t73DKnq-sh0EctMAOKpY6_esoX4M18-LsJcVHkrPz4aAqA2EALw_wcB>

[https://medium.com/@analyticsemergingindia/ethical-hacking-understanding-the-role-of-white-hat-hackers-in-cyber-defense-9d28fa3a0733#:~:text=Ethical%20hacking%2C%20also%20known%20as,sensitive%20data%20from%20malicious%20attacks](https://medium.com/%40analyticsemergingindia/ethical-hacking-understanding-the-role-of-white-hat-hackers-in-cyber-defense-9d28fa3a0733#:~:text=Ethical%20hacking%2C%20also%20known%20as,sensitive%20data%20from%20malicious%20attacks).

<https://cmitsolutions.com/tribeca-ny-1166/blog/tools-and-techniques-of-ethical-hacking/>

<https://www.institutedata.com/blog/how-important-is-cyber-security-in-international-relations/>

<https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/case-study-series>

<https://www.kroll.com/en/insights/publications/cyber/case-studies>