ALTITUDE

Explore. Lead. Innovate

Altitude UNA-NCA Model United Nations

Background Guide

International Telecommunication Union

Table of Contents

Letter from the Under-Secretary-General

Hello Delegates, and Welcome to Altitude MUN 2022!

I am so excited to welcome you to this year's conference (in person!) after what have been two very tumultuous years. My name is Kavya Shah, and I am a sophomore at Georgetown University serving as your Under-Secretary for High School Committees. I began my Model United Nations journey in 8th grade, and over the years, MUN has taught me many valuable lessons about cooperation, diplomacy, and persistence.

As you embark on your MUN experience at Altitude, I hope you keep these traits in mind. While each of you will have moments in which you are challenged – whether it be by new experiences, new knowledge, or your fellow delegates – remember that MUN is about learning how to come together despite our differences. In doing so, two things are key: 1) *perspective* – making a good faith effort to understand why and how an individual or nation is pursuing a particular stance, and 2) *debating ideas, not individuals*. With this understanding, you will be able to work towards innovative *and* realistic solutions to some of our world's most pressing issues.

I'd also like to emphasize that Altitude, rather than a competition between delegates, is designed to be first and foremost a learning experience where delegates of all levels can participate and seek support. We expect delegates to keep an open mind and be willing to learn from each other throughout the conference.

Our conference centers around the UN Secretary General's *Our Common Agenda* report which outlines 12 commitments designed to accelerate global collaboration and progress towards the SDGs. Furthermore, we draw inspiration from the *UN Secretary-General's Top 10 Priorities for 2021*. As you look towards resolutions in your respective committees, we advise that you reference these reports and draw from their conclusions. Consequently, your preparation for the conference should go beyond the given background guide and delve into the specifics of your nation's stance and past collaborative efforts.

We look forward to seeing each of you at Altitude MUN 2022 in New York City! Please do not hesitate to reach out in the meantime with any questions or concerns.

Best,

Kavya Shah
Under-Secretary-General of High School Committees

The Committee

International Telecommunication Union

Committee Overview

What first started as the International Telegraph Union in 1865, is now the International Telecommunication Union (ITU), the leading agency for information communication technologies (ICTs). Its mission first started with the goal of expediting communications internationally using the telegraph. The agency's mission then proceeded to cover the ICT sector as it grew, including the internet, mobile technologies, and television. The ITU became a specialized agency under the United Nations (UN) in 1947, and through its history, has seen the rise of innovations that have transformed our world. As such, we recall inventions such as voice telephony, radiocommunications, and communications satellites.

Currently, the ITU is headquartered in Geneva, Switzerland with offices located across the world. The ITU aims to connect people around the world through technology, advocating more broadly for accessible communication. It acknowledges the significance of ICTs in one's daily tasks and activities and is continually improving the access and incorporation of such. Listed below are some of the achievements and operations of the ITU:

- Global telecommunication systems are possible as a result of the international agreements set by the ITU.
- Television, GPS navigation and all satellite related activities are managed by the ITU's coordination of these satellites.
- Internet connections are promoted by the ITU.
- Emergency communications channels are set by the ITU to offer a backbone for communications in the event of international emergencies.
- Innovation, revolution and partnerships are fostered by the ITU for continuous improvement and accessibility.

Furthermore, members in the International Telecommunications Union work hand-in-hand to promote ICTs and their advancement. The agency unites countries, universities, organizations and companies. Thus, the ITU promotes a diverse platform with a variety of experts in the field that contribute to the achievement of the ITU's mission. Member states of the ITU include the 193 UN member countries as well as over 900 organizations encompassing academia, international and regional organizations, and enterprises.

When it comes to the governance of the ITU, all administrative and financial operations are managed by the General Secretariat. The Secretariat handles activities such as planning meetings, security, strategies, communications, finance and legalities. The General Secretariat is divided into several departments, to each its specific functions. These departments and their main operations are:

- Office of the Secretary General: headed by the Secretary General and assisted by the Deputy Secretary General, this department manages the Union and optimizes the use of its resources.
- Strategic Planning and Membership: this department controls the strategic planning of the continuously evolving technologies in the telecommunications industry and plans ways to integrate them to meet the Union's objectives.
- Human Resources Management: this department deals with human resources functions to ensure compatibility with the Union's policies.
- Financial Resources management: this department works on all finance-related functions, such as budgets, plans, strategies and projects.
- ITU Telecom Secretariat: this department is in charge of planning and organizing TELECOM events of the Union which unite the global community to discuss ICT discoveries and networking.
- Conferences and Publications: this department tackles the logistics of the Union's activities.
- Information Services: this department manages the Unions information technology services and represents the union in inter-organization conferences regarding security and IT.

The ITU itself divides its work across three main areas, denoted by sectors. These are tackled in all the conferences and meetings set by the body. The first sector is the

ITU Radiocommunications (ITU-R) sector; the main purpose of this sector lies in the operations and management of radiocommunications services, radio-frequency spectrum and satellite orbits. The ITU-R Bureau organizes conferences and meetings throughout the year in addition to workshops and seminars that tackle management and systems.

The second sector of the International Telecommunications Union is **Standardization** (ITU-T). ITU-T allows systems to network and operate on a national and international level. On a yearly basis, standards are initiated or reconsidered to provide guidelines for proper network functionality and services.

Finally, the third sector the ITU handles is the telecommunication **Development** sector (ITU-D). The latter opens the door to the expansion and development of current and future ICTs. in addition to that, it also works on gathering and releasing extensive

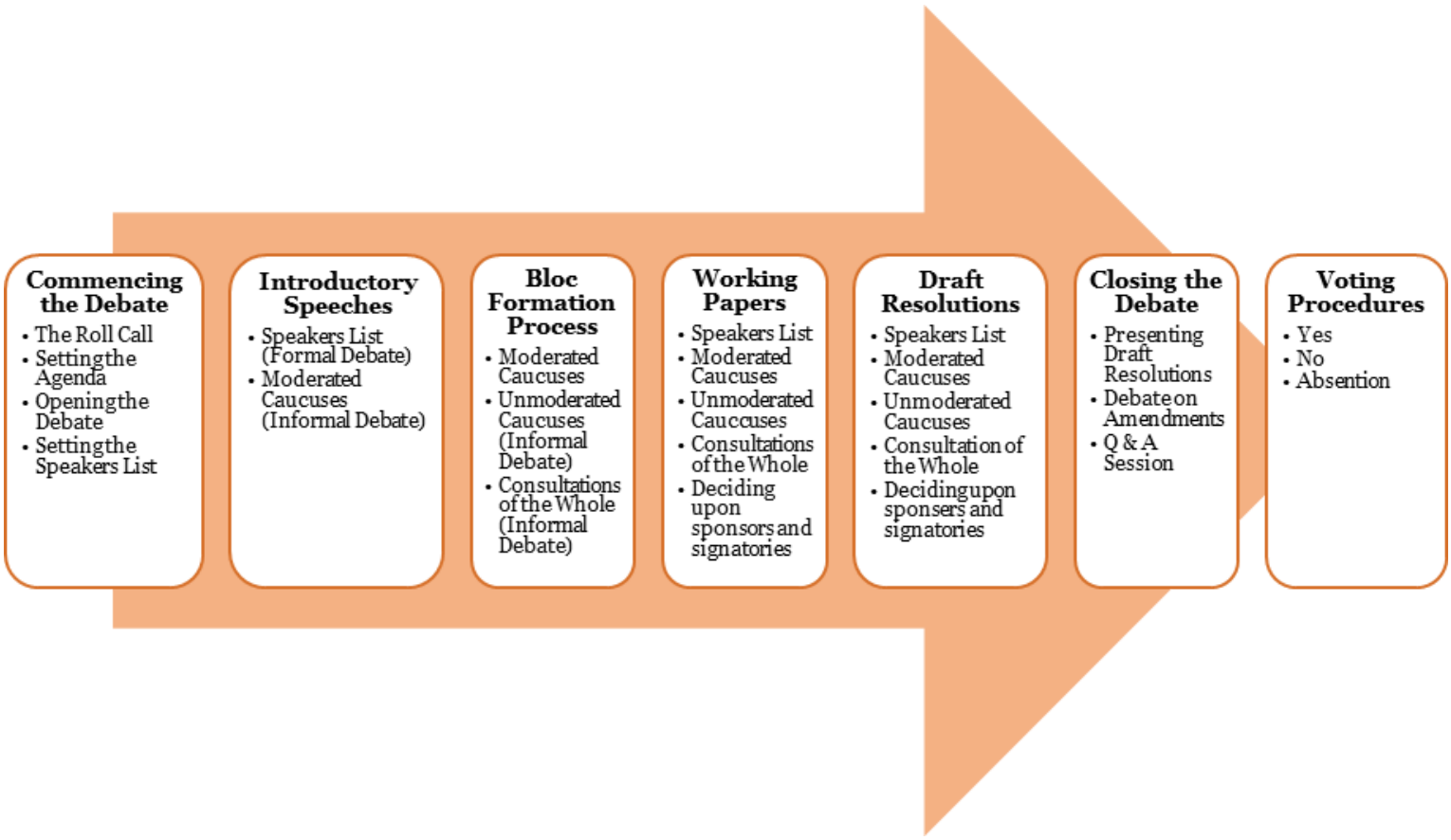
statistics related to ICTs and other related aspects.

Apart from the current sectors discussed, the International Telecommunications Union covers a variety of areas in which action takes place. These areas are: Accessibility, Artificial Intelligence, Broadband, Environment and climate change, Cybersecurity, Digital Divide, Emergency Telecommunications, Entrepreneurship and SMEs, Internet, Gender Equality, and Youth and Academia. Further, the ITU has Study Groups which are opportunities for the members in the Union to cooperate and work together on prominent issues and areas tackled. Each Study Group is responsible for a certain field whereby they manage activities and implement frameworks based on technicalities of the area. Each of the sectors of the ITU (R-D-T) have different study groups dedicated to different areas.

Item	ITU-R	ITU-T	ITU-D
Sector	Radiocommunication Sector	Telecommunication Standardization Sector	Telecommunication Development Sector
Mandate	Coordinate the allocation of Radio Frequency Spectrum and adopt Radiocommunication Recommendations *(Art. 13 ITU Constitution)*	Study technical, operating and tariff questions and adopt recommendations to standardize telecommunications *(Art. 17 ITU Constitution)*	Facilitate and improve telecommunications development *(Art. 21 ITU Constitution)*
Conference/ Assembly	World Radio Conference (WRC).	World Telecommunications Standardization Assembly (WTSA)	World Telecommunications Development Conference (WTDC)
	Revisions to the ITU Radio Regulations are considered at WRC	The Work Program for the Next 4 Years in ITU-T is defined at WTSA	WTDC is dedicated to the role of telecommunications in Development
	Every 3-4 years	Every 4 years	Every 4 Years
	Next Conference is in 2018	WTSA 2016	WTDC 2017

At a Glance: The Conference

The Flow of Debate



Key Terms and Concepts

- **Absolute Majority:** Also known as a two-thirds majority, an absolute majority is ⅔ of the quorum (or 66.7% of the quorum). Assuming a committee quorum is 60, the absolute majority would be two-thirds of 60, which is 40.
- **Decorum:** The constant order and respect expected from all members of the committee throughout the Conference.
- **Draft Resolution:** Once delegates have compiled their ideas through the working paper, delegates must transform them into an official resolution format. This formal document is known as a Draft Resolution. The reason behind it incorporating the word ‘draft’ is because the resolution is yet to

be adopted by the Committee. Moreover, a Committee may have more than one Draft Resolution but it can only have one official resolution at the end.

- **Friendly Amendment:** Amendments are considered **friendly** if all of the sponsors of the original Draft Resolution agree to it.
- **Interruptive Points:** Interruptive points are those that can be put forth at any time during the debate process. However, at Altitude MUN, the interruptive points cannot be used to interrupt a delegate giving a speech.
- **Motion:** Delegates will use motions to move from one part of the debate to another. As such, motions will be the outlet used to decide upon the next course of action throughout the conference.
- **Non-Interruptive Points:** Unlike interruptive points, non-interruptive points can only be used when a Chairperson explicitly asks if there are any points or motions on the floor.
- **Point:** Contrary to motions, which delegates put forth to decide upon the next course of the debate, points are used for the sole purpose of facilitating the conference's procedure.
- **Present:** Delegates can vote on a resolution with 'yes', 'no', or 'abstention'.
- **Present and Voting:** Delegates have to vote on a resolution with either a 'yes' or 'no'.
- **Roll Call:** The first part of the Conference is known as the roll call. During the roll call, the name of each participating nation will be called aloud in alphabetical order by the Dais. Delegates can either respond with 'present' or 'present and voting'. A roll call will be taken everytime delegates reconvene at the conference setting after postponement of the debate.
- **Sponsors:** The nations that have contributed the most in terms of developing a particular document, particularly the Draft Resolution.
- **Signatories:** Signatories are nations that wish to see a certain document debated. Signatories do not have to be members of the bloc writing the document.
- **Simple Majority:** A simple majority is 50% of the quorum plus '1'. For instance, let us assume that the quorum for a committee is 60. Therefore, the simple majority for this committee would be 31.
- **Quorum:** The total number of nations present at the committee.
- **Unfriendly Amendment:** Amendments are considered **unfriendly** if at least one of the sponsors of the original Draft Resolution disagrees with it.
- **Working Paper:** The first step in the resolution formation process, the working paper is an **informal document** where delegates can begin gathering ideas and forming solutions in point format. It essentially a 'rough draft' of the Draft Resolution that will follow.

- **Yields:** If a delegate finishes their Speakers List speech and still has some speaking time to spare, they must yield their time. Delegates can either yield their time to the Chairperson, to questions, or to another delegate. Delegates should note that they only have the option to yield their time during the formal debate (the Speakers List).

Rules of Debate

Written Motions

Instead of voicing them aloud, these motions are written on formal notes and delivered to the Chairperson by way of an Usher.

Format:

From: Delegates should insert the full names of their nations here.
To: Chairperson
Purpose:

- **Appeal to the Chairperson's Decision:** If the delegate wishes to motion for an appeal to the Chairperson's decision, the purpose should look similar to the following:

"The delegate of (insert full name of nation) motions for an appeal to the Chairperson's decision because (insert reasoning behind the appeal)."

- **Right of Reply:** If the delegate wishes to motion for a right of reply, the purpose should look similar to the following:

"The delegate of (insert full name of nation) motions for a right of reply to (insert full name of target nation) because (insert reasoning behind the right of reply)."

Verbal Motions

These motions can be verbalized aloud when the Committee Chairperson opens the floor for any points or motions. One significant aspect to take into account is that verbal motions need to be seconded.

The Debate

"The delegate of (insert full name of nation) motions to open the debate to discuss (input the Committee topic)."

- **The Speakers List**

"The delegate of (insert full name of nation) motions to set the Speakers List for a speaker's time of (insert the suggested length of speaking time per delegate)."

To pass, this motion requires a simple majority.

- **Moderated Caucus**

"The delegate of (insert full name of nation) motions to suspend the debate and move into a moderated caucus with a total time of (insert total duration of the caucus) and a speaker's time of (insert the suggested length of speaking time per delegate) to discuss (insert desired topic)."

To pass, this motion requires a simple majority.

- **Unmoderated Caucus**

"The delegate of (insert full name of nation) motions to suspend the debate and move into an unmoderated caucus for a total time of (insert total duration of the caucus) to (insert desired purpose of unmoderated caucus)."

To pass, this motion requires a simple majority.

- **Consultation of the Whole**

"The delegate of (insert full name of nation) motions to suspend the debate and move into a consultation of the whole for a total time of (insert total duration of the caucus) to discuss (insert desired topic of discussion)."

To pass, this motion requires a simple majority.

- **Adjournment and Resumption of Debate**

"The delegate of (insert full name of nation) motions to adjourn the meeting for the purpose of (insert the purpose of adjournment)."

"The delegate of (insert full name of nation) motions to resume the debate."

To pass, this motion requires a simple majority.

- **Closure of Debate**

"The delegate of (insert full name of nation) motions to close the debate and move into the introduction of draft resolutions."

To pass, this motion requires an absolute majority.

- **Debate on Amendments**

"The delegate of (insert full name of nation) motions to close the introduction of draft resolutions and commence the debate on amendments."

To pass, this motion requires an absolute majority.

To pass, each amendment requires a simple majority.

- **Voting on Resolutions**

"The delegate of (insert full name of nation) motions to close the debate on amendments and commence the Resolution voting procedure."

To pass, this motion requires an absolute majority.

In order to pass and become the Committee's official Resolution, the Draft should garner at least a simple majority.

Points

Interruptive Points

- **Point of Personal Privilege:**

This point can be utilized by a delegate whenever they experience a certain personal discomfort that hinders their ability to fully participate in the conference at hand.

- **Point of Order:**

A point of order is brought up when a delegate feels as though the rules of procedure have been broken.

Non-Interruptive Points

- **Point of Parliamentary Inquiry:**

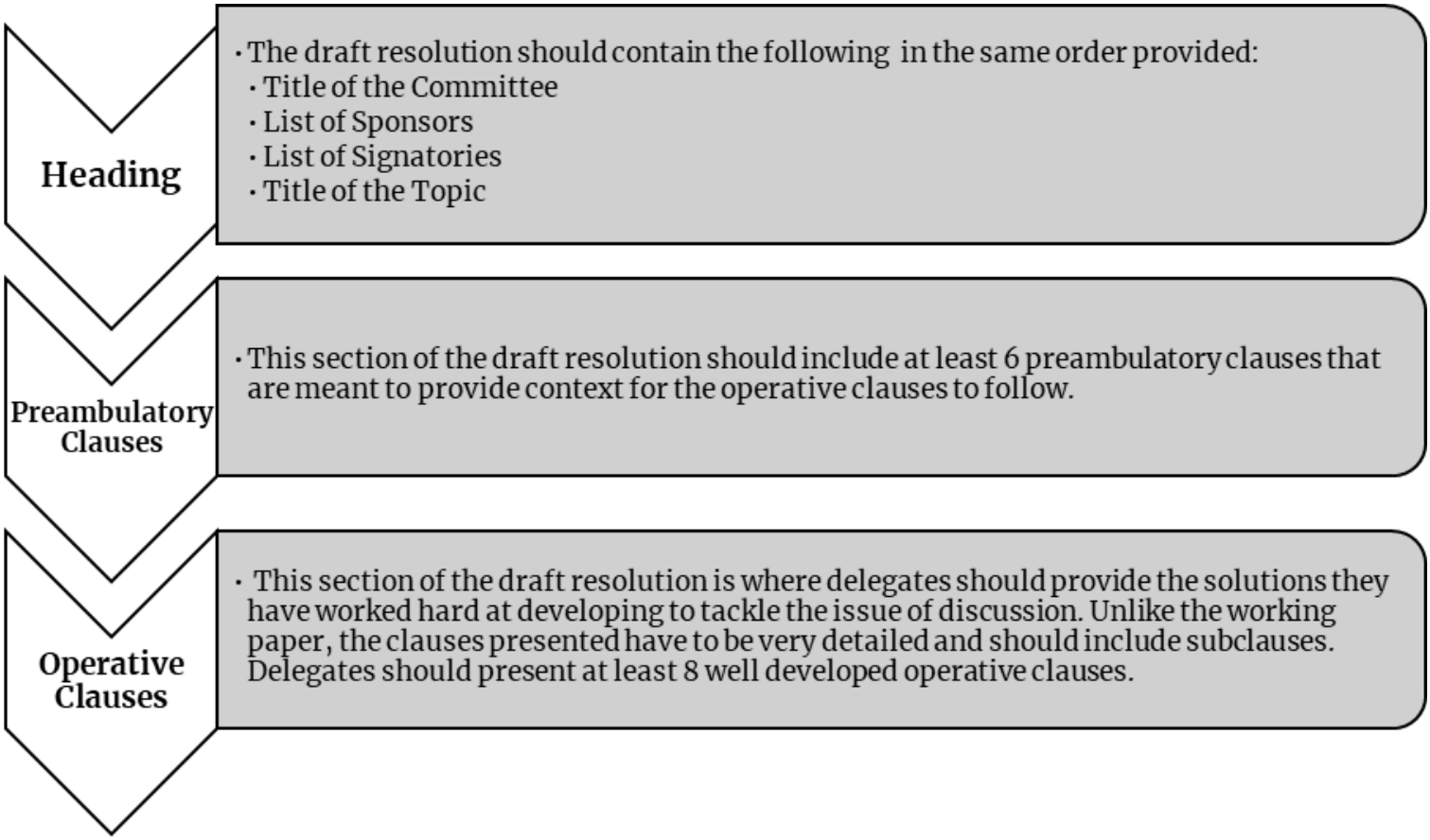
This point can be used whenever a delegate would like to ask the Dais members a question regarding the overall rules of procedure.

- **Point of Information:**

A point of information, also known as a point of inquiry, can be exercised by delegates whenever they would like to ask a question regarding something they do not understand about the issue at hand.

Resolution Formation Process

Flow and Structure of a Draft Resolution



The Topic

‘Reevaluating Cybersecurity Standards in a Post-pandemic World’

Topic Overview

Information Technology

Information technology (IT) is present in all aspects of life. It refers to the use of technology in a variety of entities as a means of storing and organizing data by developing computer systems and networks. IT consists of three pillars that support parallel goals of ensuring efficient services, reinforcing security and maintaining appliances. The latter are IT governance, IT operations, and Hardware and Infrastructure. In addition, well-designed IT systems operate to prevent problems that may arise from slow functioning and data burdens. Information technology has been growing exponentially in the last decades. According to a study based in Zurich, such innovations affect all realms of our society including social, cultural, political and economic facets. In that sense, our perspectives are based on such systems, and policies are also set accordingly.

IT in the Social and Cultural Realms

It comes as no surprise that technology has affected our society. Each technological advancement has influenced our decisions, education, and communications; it has brought the world together with devices found in our pockets and hands on a daily basis. Most of our day to day tasks have been affected by IT. For instance, the shift to online education during the rise of Covid-19 has been made possible with technology present nowadays. Additionally, with the access of search engines such as Google, anything can be known at any time no matter where. The presence of IT makes seeking knowledge easier and more accessible. On the other hand, this vast improvement of technology has yielded negative consequences that in turn affect individuals of a society. Cyberbullying, for instance, showcases the use of IT in a negative application. A reduction in personal interaction has also been examined due to the rise of technology, whereby people prefer chatting and talking to individuals from behind the screen rather than face to face. Social media and rapid access to information via IT has also contributed to a rise in disinformation, which poses a risk to the very foundation of democracy – a well informed citizenry.

The future holds further connections between people across the globe. Take for instance Virtual Reality, Augmented Reality, and Extended Reality – the advancement and expansion of such instances have the potential to change the course of all our operations and activities, be it in

the medical, educational or societal sectors. The possible consequences of these technologies, both positive and negative, and their long-term impact must be studied further.

IT in the Political Realm

Information technology has also caused politics to take shape as we currently know them. For instance, the internet has granted access to all necessary information to current events around the globe. News events are directly spread and available to everyone. Disadvantageously, the access to false information and rumor is also easily spread as a result of the internet and information technology. Opinions are easily influenced especially in this realm, and this has taken both a positive and a negative impact on individuals. For example, raising awareness on prominent human rights violations is possible through information technology. Manipulation is also an instance of such fluid opinions. Along the same line, in terms of politics, IT has seen occurrences of dividing people or even accepting and uniting them.

Moreover, IT has helped governments in the areas of services and improving them such as combating corruption and fraud. Encryption and protection of information has also helped in improving a country's security. On the contrary, it also played a role in developing advanced technologies used in an adverse way, such as weapons technology and waging war.

IT in the Economic Realm

Economically, information technology has played an advantageous role mainly in reducing the burden of distance in commerce. It has contributed to the overall growth in the economy across the globe. A significant example is the 'work-from-home' setup, which has since taken over jobs and institutions as a result of Covid-19. Similarly, the rise of economic commerce has come as a result of the development of IT. Despite the location one is in, the purchase of products through online resources is simple and feasible anywhere without the need to visit stores. In addition to that, the integration of communication systems and computing has facilitated the necessary data organization processes in a company. In other terms, IT systems are currently found in all enterprises and have replaced the "paper" when it comes to storing all data and information. Through the advancement of technology, new jobs are created and older jobs are replaced. This is a sword with two edges which necessitates the updates and development of individuals to keep up with trends and prevent job loss. Further, reduced costs are seen as a result of the advancement of technology which in turn improves efficiency of processes.

Cybersecurity

Cybersecurity has been an increasingly hot topic across different institutions and governments globally. This particularly lies in the realized importance of security and safety of data and information found in our frequently used devices. Prior to understanding cybersecurity, the definition of related terms is essential.

Firstly, an **information system** is a network that combines manpower and technology to accumulate data and organize it. Such networks are utilized in different industries as means of maximizing efficiencies and organizing safe operations. Usually, Information Systems are composed of a variety of components that work in harmony to provide the necessary functions. These are hardware sources for tangible elements, software for intangible functions, telecommunications for connectivity and transmission, data for knowledge, and human resources for human influence and analysis.

Consequently, **cyber attacks** are attempts of breaching the information systems of individuals or organizations. These occur on a daily basis across businesses with the purpose of imposing harm and collecting benefits from these firm's data bases. Statistically speaking, according to Cisco, 53% of cyber attacks yield losses of half a million dollars or more. Different cyber attacks are encountered and are distinguished by their purpose. For instance, malware targets vulnerable entities and incorporates malicious software, such as viruses. Other cyber attacks are phishing, ransomware, distributed denial-of-service, insider threats, advanced persistent threats, and man-in-the-middle attacks.

The latter imposes the importance of cybersecurity to prevent such attacks. Cybersecurity uses information technology and its development to protect networks of entities and avert cyber crime. This importance has reflected an increase in spending of a firm to ensure security and minimize cyber attacks. The successful implementation of cybersecurity standards counter cyber threats efficiently and information breaches are put to a minimum. This integrates layers and domains of cybersecurity set as countermeasures of the different cyber attacks. Further into discussion, with the advancement of technology, there currently exists several cybersecurity technologies that optimize its purpose without interfering with customers. These technologies are Identity and Access Management, comprehensive data security platform, and security information and event management.

Topic in Depth

Rise of the Internet

The internet dates back to the 1960s which came as an outcome of wanting researchers to share information. It first started with having an idea of a global network using the computer initiated by a computer scientist at MIT. In 1969, the creation of the first world wide-area computer network saw light as it was funded by the Advanced Research Projects Agency (aka ARPANET) which later grew over the years. Moving on, in order to prevent some networks from collapsing as a result of the collapse of one network, the creation of Internet Protocol (IP) was developed in 1973. Overall, the 70s saw positive trends in terms of advancements in networks and organizing network information.

In the 1980s, advancements mainly focused around the PhoneNet system which offered the chance for email communications. Further along the line, the HTML and the URL replaced the ARPANET yielding the birth of the World Wide Web we currently know and use. Significant firs and concepts were launched including Amazon, Internet Explorer, Java, Yahoo and eBay. Similarly, Google was founded in 1998. The rise of viruses and cyber threats also started around this era. For the 2000s, advancements were also experienced mainly in the realm of the spread of Wi-Fi and mobile internet. As our days proceed, the internet is on a constant development cycle and newer areas are constantly discovered. For instance, the Internet of Things (IoT) showcases recent expansions of the internet.

Rise of Cybersecurity

Cybersecurity came as a result of the rise of threats and has come a long way in terms of advancement. Cyber crime develops with the improvement of technology. In the 1960s, the use of the word hacking began to be used, however the purpose differed. Rather than the commercial benefits from hacking, it was previously solely used for causing trouble and accessing systems. Nevertheless, this created the idea of improving the security of computers to offset possibilities of hacking. Moving into the 1970s, the first "virus", Creeper, was established which printed a message across a network of computers (recall ARPANET). Countermeasure Reaper was created to eliminate Creeper. At this point during time, governments acknowledged the vulnerabilities of hacking into systems and the problems that are implied by them. Hence, further effort was put to provide such security. The 70s also saw the first cyber attack and the arrest of the first cyber criminal, Kevin Mitnick.

The first cyber attack opened the horizon of attacks in the 80s such as the attack on AT&T. Furthermore, cyber espionage became a concern in governments, especially during the Cold War. This led governments to start looking into the security of computers to prevent such attacks. As a result, the "Trusted Computer System Evaluation Criteria" was established in the United States in 1985. The latter rooted the level of security and trust incorporated in computers which was the foundation of cybersecurity in future commercial computers. As time passed, the threats became more and more significant and harmful to governments. For instance, in 1986, Marcus Hess threatened to sell all information he breached from the US military computers and the Pentagon to the KGB. This opened eyes to quick advancements and mitigated security threats, leading to the release of the first anti-virus product in 1987. In parallel, more viruses and worms continued to develop and impose threats to secure information on computers and networks. These viruses kept on progressing to offset the improvement of the anti-viruses in the market which in turn encouraged the creation of new viruses. To add, the first event in cybersecurity to be made public was the creation of the worm by Robert Morris which targeted the determination of the size of the internet and networks. Its spread however led to negative outcomes including clashes and slowed down the

internet. As a result, the creator was charged under the Computer Fraud and Abuse act. He was the first instance of this type of accusation. Other important aspects in the 80s was the widespread use of antiviruses as a counteract to the viruses, as well as the establishment of the Computer Emergency Response Team.

Throughout the 1990s, the cybersecurity sector saw much growth in regards to the prosperity of the internet. Yet with this growth, a variety of new viruses emerged such as the DiskKiller, ILOVEYOU, Melissa, and Polymorphic. These instances resulted in significant financial damage, such as the 80 million dollar damage caused by Melissa. In addition to that, an anti antivirus was initiated by cybercriminals during that era along with the release of macro viruses. Companies invested more time and energy on minimizing cyber attacks and developing the necessary antiviruses to combat them. All in all, these viruses interrupted systems and caused their failures or slow downs. Rather than the previous aims of cyber attacks, it was during this time where breaches had the purpose of financial advantages. Moreover, in 1995, the Secure Socket Layer was implemented which protected individuals and their purchases. The latter set the corner stones for the HyperText Transfer Protocol Secure (HTTPS).

The 2000s continued the growing path of the internet as computers were becoming accessible to a lot of homes and businesses. Newer types of viruses were discovered: website hidden malware, infiltrated messaging services, distributed denial of service attacks, and more. In addition to that, the first hacker group 'Anonymous' was established, combining the skills of a variety of individuals for hacking. The group initiated several cyber attacks across different goals over the years. Breaching the information of individuals' credit cards happened in the 2000s. Retailers were hacked and their information databases were accessed and stolen from. In addition, personal accounts also were hacked around that time. For instance, 3 billion individuals with Yahoo accounts were hacked. Both examples shed light on the importance of protecting personal information and securing databases, even within retailers.

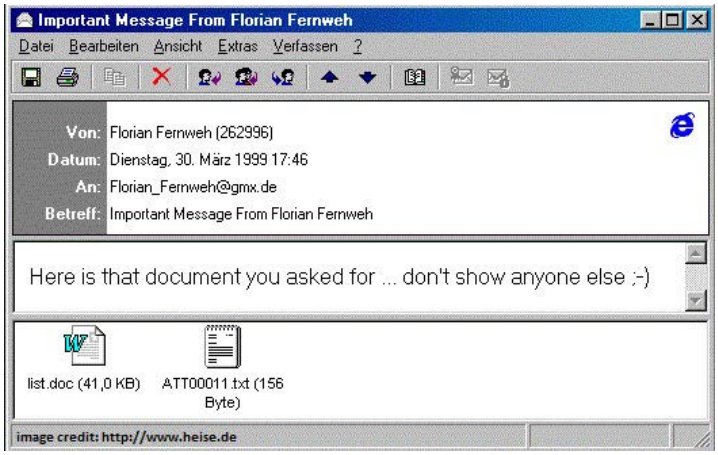
Furthermore, the rise of state sponsored attacks soared after a North Korean sponsored group hacked into Sony and breached information of films and images. As other decades, the advancement of cybersecurity was seen and new methods were introduced, such as computer forensics, multi factor authentication, and web application firewalls. The rise of cyber attacks and their advancement has opened eyes across governments, organizations and firms which further encouraged the counteracts and the prevention of such attacks through cybersecurity. In 2003, the US Government recognized the importance of cybersecurity. Similarly, in 2018, the European Union enforced the General Data Protection Regulation which sets a baseline for data and security. This field maintains an exponential growth and the

integration of new concepts is seeing light every day.

Security Breaches

In this section, some of the biggest cyber crimes in history are discussed and tackled by the FBI. The aim is to understand the impact of these breaches and fathom the importance of cyber security.

1. **A Byte Out of History:** in 1994, criminals across different continents worked together to hack the network and systems of US banks. They were led by a programmer in Russia and were able to steal $10 million in total from bank accounts. This case was set out to be the first online bank robbery in history.
2. **Botnet Operation Disabled:** this cyber fraud operation was based on the Coreflood virus which entails hackers the opportunity to steal personal and financial information by monitoring users' keystrokes. This virus infected two million computers and was operated by an attacker who controlled infected computers via a botnet. Such attacks imposed a threat on the economic security of the US as well as information security.
3. **Cyber Criminal Forum Taken Down:** Darkode forum hosted 250 to 300 hackers and cyber criminals across the entire world. It was a protected meeting place that aimed at trading all cyber-related threats. These include credit card information, botnets, stolen personal information, malware, and softwares that help in cybercrime. A counterattack to the forum was the Operation Shrouded Horizon which arrested and charged organizers and traders of the forum.
4. **Melissa Virus:** what started as a virus that was unleashed to computers in 1999 soon became a wildfire that disrupted the email servers of more than 300 corporations and agencies. Its estimated cost for recovery and cleanup amounted to $80 million and over one million accounts were hindered.



More instances can be discussed endlessly as security breaches and cybercrime remain an ongoing problem that individuals and organizations face on a daily basis. Another significant security breach that jeopardizes governments integrity and information security is the whistleblowing of WikiLeaks and their access to secret information.

Pertinent Features

ITU and Cybersecurity

One of the areas of action of the International Telecommunication Union is cyber security. This lies in the importance the ITU holds to ensure security and confidence in the Information and Communication Technologies (ICTs) used. The ITU believes that cybersecurity is a liability a

government should adopt to prevent any incidents that might occur.

In ITU-D, the Union offers developing countries a cybersecurity program that aims at helping them enhance their cybersecurity capabilities and trust in digital technologies and ICTs nationally. Furthermore, the ITU-D understands the vulnerabilities faced by everyone using ICTs and their interconnectivity and ultimately works to enhance cybersecurity to protect data infrastructures globally. It offers a Guideline to Developing a National CyberSecurity Strategy which provides the foundation of creating an effective cybersecurity framework. This framework entails strategies to prevent threats, prepares for them and provides a response strategy to offset the vulnerabilities imposed.

In addition to that, the Union highlights the importance of having institutions that are specific in dealing with cyber threats and attacks in order to have the proper implementation of a cybersecurity framework. Hence, the ITU has introduced National Computer Incident Response Teams (CIRTs) and has helped member states in establishing them and enhancing their significance in cybersecurity. Currently, the Union has established or helped in the establishment of 118 National CIRTs.

The ITU also issued a Global CyberSecurity Index (GCI) which sets as a reference to measure effectiveness of present cybersecurity mechanisms and the commitment of member states to cybersecurity at a global level. The index focuses on five main pillars that structure the approach and identifies the conformity and commitment; these are:

1. Legal Measures
2. Technical Measures
3. Organizational Measures
4. Capacity Development
5. Cooperation

Current Cybersecurity Frameworks and Standards

There exists a significant amount of cybersecurity frameworks across the internet. For the purpose of this background guide, the focus will be on the framework set by the National Institute of Standards and Technology (NIST). This framework focuses on improving critical infrastructure cybersecurity. It aims at providing technical guidance to cybersecurity for public and private sectors in the United States as it acknowledges the risk cyber threats impose on National security levels as well as on an organization's level. The main foundation of the standards rely on developing the cybersecurity activities in an entity to minimize risks and improve risk management. Further, it is divided into three main parts:

1. Framework Core: this part is dedicated to list a set of cybersecurity activities and information in this regard across a variety of sectors and industries. Its purpose is to guide organizations to develop individual organizational profiles.

2. Implementation Tiers: the tiers play a role in understanding the different cybersecurity characteristics and their approaches to manage cyber risk which further enhances priorities and objectives.

3. Framework Profiles: the profiles established in the framework core are essential in prioritizing cybersecurity activities in a way that aligns with an organization's goals, risks and mission.

The set framework is applicable in any sector regardless of the purpose, size or level of current cybersecurity. The latter is related to the organizing structure offered as well as the flexibility based on the different standards and guidelines assessed to fit current trends. Since it is established on a foundation of standards, as previously mentioned, its international application and call for collaboration is made possible.

Furthermore, frameworks in general are all based on standards. These standards build common ground for security recommendations and requirements, they also address the needed qualities for security in a specific area. For this reason, cybersecurity standards are disseminating internationally and within organizations. Another role is to have a clear and common definition for the frequently used terms, such as the role of the ITU-T.

To add, there exists multiple organizations that work on developing standards for cybersecurity; they are either issued by international organizations, regional, national or industrial. Regardless of the organization, their purpose remains the same, which revolves around providing guidance to improve cyber security. For instance, the ITU-T's Study Group 17 works on establishing recommendations regarding cyber security and related softwares and functions. It also discusses previous and current cybersecurity standards from different organizations as well as their gaps. One of the standards issued by the previously mentioned study group is the ICT Security Standards Roadmap. Other institutions that develop standards include the Institute of Electrical and Electronics Engineers, International Standards Organization, Internet Engineering Task Force, and European Committee for Standardization.

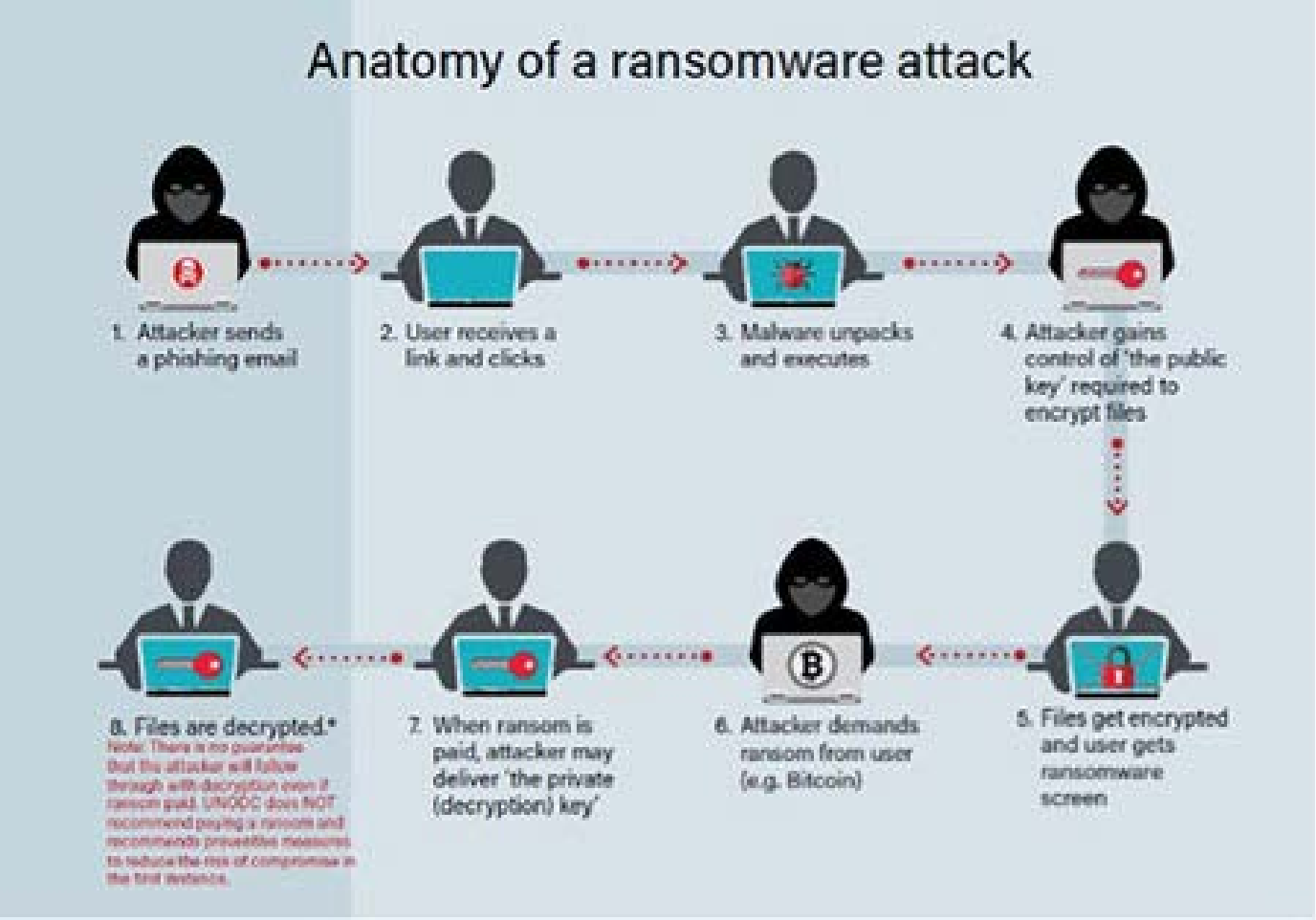
Current Trends of Cyber Threats and Cybersecurity

Cybersecurity has been and will continue to advance on a vast horizon, cyber threats and risks will also proceed to develop and impose danger to society and security. With the rise of technological advancement, cybersecurity is seeing a hopeful improvement that mitigate the new threats. Despite that, hackers and social engineering attacks are becoming more and more creative and intuitive with their threats. They adapt to current cyber securities and think of newer ways to impose threats and access personal and organizational information.

One of the current trends of cyber threats is the vulnerability of the Internet of Things devices. These refer to tangible systems that connect to the internet and share data apart from computers and phones, they include smartwatches or voice assistants (Amazon Echo, Google Home). These additional devices in a household offer the chance for newer cyber attacks and breaches. Mobile cyber threats are

also a vulnerability in terms of network security such as public Wifis and Mobile Internet. The latter highlights the importance of integrating cybersecurity activities to prevent these risks as much as one can.

Moreover, ransomware, a threat that has been present for a long while, is also significantly growing and has become easier to use for hacking and financial purposes. In 2020, a ransomware attack was directly related to the death of a sick woman who was unable to have access to treatment at a hospital as it was locked out of its systems. Such attacks have become more and more developed as they have integrated machine learning, as did cyber security, collaboration and untraceable financial gains, such as cryptocurrency payments.



Adding to the list of threats, the rise in the use of cloud services and cloud computing has also offered the high risk and vulnerabilities in cyber attacks. Much effort is being placed on

improving the cybersecurity of cloud services as it is a target for hackers, primarily due to the amount of information and data stored in these clouds. Further, data breaches on the cloud cost around $3.86 dollars, which validate the necessity of proper cyber security.

Fortunately, the cyber security field is also seeing improvement to further face the threats and reduce vulnerability. This first starts with the spread of the data privacy concept. Personally Identifiable Information breaches have raised the awareness of data privacy which has led to the establishment of laws and regulations that acknowledge the latter as a discipline. Organizations are also working on improving their privacy and security in order to optimize their operations and build consumer trust. One of these data privacy operations is Multi-factor authentication (MFA). This has been on the constant rise and development, they are constantly incorporated in organizations and within users. However, MFA is still subject to some malware and threat, especially those that rely on SMS authentication.

Artificial Intelligence (AI) and machine learning are having a significant impact on cyber security. In fact, organizations are referring to these technologies to further enhance their security infrastructure. Not only is AI the future of technology (Technology 4.0), but the implementation of such technologies in firms have helped save $3.58 million in 2020. The main focus of AI is to build automated security systems that play a role in threat detection, risk data identification and attacks prevention. On the other hand, cyber criminals are also referring to such technologies as means of automating their attacks and threats. Cybersecurity still remains a skill that requires development and improvement to be able to withstand all possible threats, it requires advancement, research and investments to keep one step ahead of cyber criminals.

Cryptocurrency and Cybersecurity

Another trend is the shift to a digital economy, i.e. cryptocurrency, the latter further creates new cyber threats that were not previously present. For instance, in 2014, $350 million in bitcoin were stolen, other attacks have also occurred over the years. Cryptocurrencies are perceived as possibly the future of currencies as they operate independently of any central banks.

The blockchain technology used by these currencies subject the latter to vulnerabilities and motive for cyber crime. The security of these

coins depend mainly on these technologies and the algorithms implemented. Moreover, there exists negative effects incurred by cyber attacks on cryptocurrencies, particularly in their volatility and effects on other currencies. Hence, an increase in cybersecurity plays an essential role in reducing the risk of cryptocurrency volatility. Further into discussion, studies show that cyber attacks on cryptocurrencies also indicate possible attacks on other sectors such as financial and governmental. Despite that, blockchain technology has the potential to improve cyber security and minimize the risks implemented by the threats, however, much procedures and advancements are needed, in addition to proper legislation to spread its integration.

Impact of COVID-19 on the Internet and Cybersecurity

In 2020, when Covid-19 proliferated immensely and the whole world shut down, the shift to technological advancement matched the speed of lockdowns. Schools, Organizations, and Governments all shifted to a remote lifestyle be it online education, work and meetings. In addition to that, ICTs and their uses increased exponentially with the shift into the online world ranging from e-commerce to telemedicine.

The latter has increased cyber threats and risks as the shift came on a fast basis. Ransomware is also increasing due to the pandemic and the shift to remote work quickly. As a result, the number of attacks and their impacts has increased significantly during this time. Further, other cyber threats are also surging such as malware, phishing and malicious domains. Statistically, there has been an increase in phishing websites to reach around 350% since the beginning of Covid-19, cyber criminals and groups have also been on the rise with an increase in personal gains as a motive to perform cyber threats. In general, studies have shown that 47% of people working from home face phishing scams. In addition to that, in Switzerland alone, for instance, the country has seen an increase of 200 attacks compared to the regular average of 150 cyber attacks during April of 2020. Such attacks and scams have incurred high costs on governments and institutions. To elaborate, an average of $137,000 is the cost of a data breach during Covid-19.

Fortunately, governments, firms and international organizations have been improving their securities and networks within this pandemic and increasing cybersecurity measures. Organizations like Ernst & Young, KPMG, Mckinsey, and PwC have lookes into ways to improve cybersecurity during this pandemic. Others like the National Institute of Standard and Technology have provided guidelines to improve the security and protect IT services during the remote shift in work. However, a lot still needs to be done as the pace of cyber threats is also accelerating. This requires the adjustment of frameworks on a national and international level, while also increasing the role of international organizations in monitoring and facilitating cyber security activities. The universal awareness of cyber security and its

impact on reducing cyber threats is also primary to reduce present threats.

Cyber Attacks on Healthcare Institutions

With the rise of Covid-19, healthcare institutions became a target for ransomware attacks. Their numbers have increased significantly as cyber criminals became aware of the importance systems and networks are in these institutions. Through exploited emails containing infected links, cyber criminals enter hospital systems and lock them out, which leads hospitals or any institution to pay requested ransom. Given the importance of such systems, during the crisis, criminals target the institutions for financial gains.

Generally, hospitals and medical centers became vulnerable and susceptible to cyber attacks as there has also been an increase in the use of Information Technology services and networks. Apart from disrupting the systems used, another purpose of the cyber attacks such institutions are facing is related to having access to studies, data and strategies used for vaccination and medication. Healthcare supply chains are also a target for cyber criminals as they offer access to intellectual information and demands. All of these cyber threats have delayed patient care and impacted the responses of hospitals negatively. Significant attacks have occurred on healthcare institutions since the start of the pandemic on both a national and international level, some of which include:

- Cyber attack on a Czech hospital;
- Ransomware attack on a vaccine trial group in the United Kingdom;
- Cyber attack on US Health Agency;
- Cyber attack on the construction company building emergency hospitals in the UK; and
- State sponsored attack on US, UK and Canadian Universities working on the development of a Covid-19 vaccine.

The latter necessitates healthcare organizations to promote an approach to minimize the risks as well as respond to any risks that may arise and reduce its impact on the systems. Although nations have been working on improving the cybersecurity of such institutions by releasing guidelines and frameworks, further action is required, especially that such organizations do not have the proper cyber security activities.

Global Efforts

Convention on Cybercrime- Budapest

This treaty builds a framework or guideline for tackling cyber crime, it was established in 2001 and entered in force in 2004 under the Council of Europe. It is the first treaty that undertakes cyber crime on an international level particularly in fields of computer fraud, violations of network security and human rights. It also aims at setting a common criminal policy to protect the society from the rising threats. The Budapest Convention on Cybercrime has 66 ratifications; however, it allows any country to adopt its framework and use it as its own guideline.

Under its 46th article, the Budapest Convention on Cybercrime established a Cybercrime Convention Committee which is constituted of the State Parties that ratified it. The aim of this committee is to offer consultancy to members who require additional instructions on the application and implementation of the convention. It also collects the necessary information to implement for future amendments. All in all, the committee tries to enhance the application of the convention by adopting practical disciplines and recommendations to integrate in the convention.

Although the convention is seen as a gold standard, it still lacks the necessary approaches to promote human rights and protect their personal information from breaches. It also further requires adoption of international cooperation and appropriate legislation. Being established in 2001, the convention also requires further improvements to meet the current trends and changes in cyber security and the mitigation of risks.

Global Cybersecurity Agenda

The Global Security Agenda was released in 2007 by the International Telecommunication Union. It is a framework that advocates international cooperation to root the trust and confidence of ICTs globally. Its key is to build on currently operating measures and improving them, in order to reduce efforts. In addition to that, some of the initiatives that it built upon was the Child Online Protection to foster cyber security solutions across the globe. Moreover, the agenda was set by the High-Level Experts Group as they are leading experts in policy-making and applications related to cybersecurity.

Furthermore, the GCA approaches its objectives through five pillars that set the strategies of the work to be achieved:

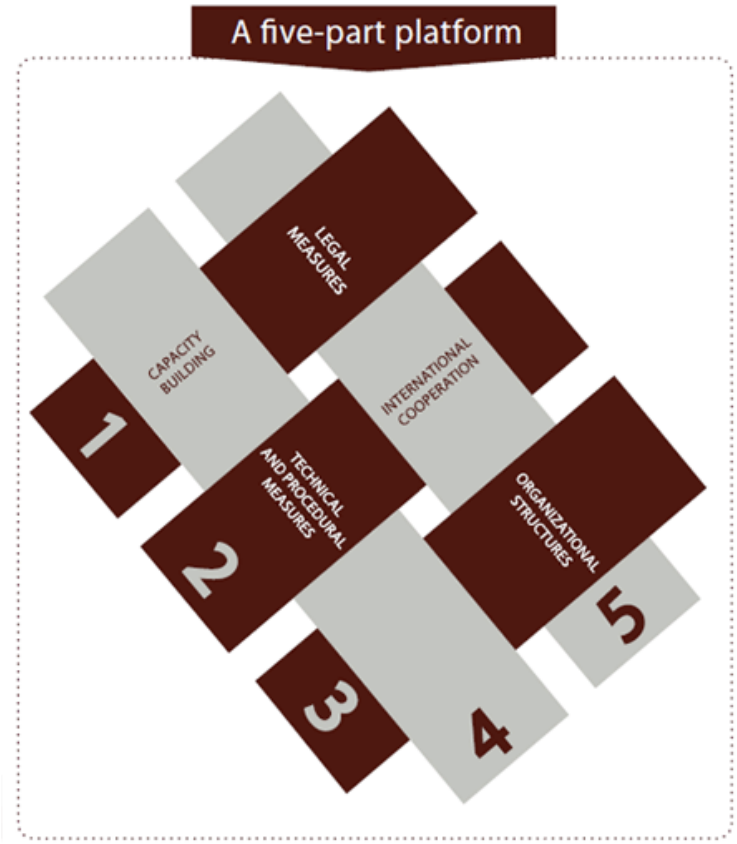
1. Legal Measures: this work area incorporated all legal issues relating to cyber crime, such as prosecution of cyber criminals.

2. Technical and Procedural Measures: this work area targets technicalities of ICTs and their vulnerabilities such as protocols and standards.

3. Organizational Structures:this work area revolves around establishing an index that assesses an organization of its cybersecurity readiness, based on its organizational structure.

4. Capacity Building: this work area focuses on enhancing ICTs in a way that includes cyber security and relevant criteria during the development process.

5. International Cooperation: this work area calls for cooperation on an international scale, in terms of monitoring, harmonizing, assessing and advocating.



The GCA still misses some key factors that require consideration. One of which is the establishment of a global ICT Security accreditation framework based on existing standards, as a way to reduce cyber vulnerabilities.

Global Programme on Cybercrime

The Global Programme on Cybercrime was established to aid Member States in preventing cyber crime by strengthening its technical assistance and infrastructure. It was founded in 2013 by the UN Office on Drugs and Crime. The program plays an essential role in identifying the necessary requirements and assistance for cyber crime and threats prevention, specifically in developing nations. Its main areas of action are in Central America, Africa, Middle East and South-East Asia. To add, the fundamental objectives of the Global Programme on Cybercrime is to increase the efficiency and results of investigations related to cyber crimes and criminals relating to the violation of human rights. It also tackles governmental responses to cyber threats and frameworks to have sustainable responses. Finally, it looks into options to strengthen the collaboration between national and international organizations which work together for stronger law enforcement and increased awareness of potential cyber risks.

Learning Outcomes

- Delegates will understand the different cyber threats that are present and the negative outcome they can have on a country, organization or entity's infrastructure.
- Delegates will grasp vital knowledge on the importance of cyber security in the prevention of threats and respective costs incurred, as well as the impact COVID-19 has had on cybersecurity and the new risen threats as a result.
- Delegates will become aware of the necessary standards present that have a proper approach to cyber security and their integration.

Recommendations

- Cyber threats are on the rise despite growing cyber security activities; delegates should look towards the future trends of cyber security and integrate them in the current standards and frameworks.
- Delegates are encouraged to look for new ways to implement AI and machine learning.
- Delegates should discover ways to promote the security of cloud computing.
- Delegates are recommended to improve the cyber security of hospitals and healthcare institutions to strengthen their infrastructures (probably integrate AI in systems).
- Delegates should discover the gaps and challenges present in current cyber security activities as well as their frameworks and standards and suggest improvements.
- Delegates are invited to explore ways to mitigate the threats that rose from Covid-19 and implement them in the standards and frameworks that are currently present.
- Delegates should determine steps to improve cyber security and the skills of those who work on its development.
- Delegates are suggested to check prosecution measures for the cyber criminals based on the degree of crime.

Key Questions

- Does your country have laws that promote data privacy?
- Does your nation implement data security and cyber security frameworks?
- Does your country follow specific standards for cyber security?
- Has your nation faced cyber threats and attacks? What was its response?
- Does your country have a strong cyber security infrastructure?
- Does your country have a proper response plan to cyber attacks?
- What are the average costs your country spends on cyber security activities?
- What are the costs of cyber attacks your country has faced?
- How can the risks of cyber threats be mitigated in both the private and public sector?
- How can we be one step ahead on hackers and other cyber criminals?
- How can we ensure the feasibility and applicability of frameworks and agreements in a country?

Annexes

Relevant Institutions

- Information Security Forum
- National Institute of Standard and Technology
- European Cyber Security Organization
- Cybersecurity Infrastructure Security Agency
- Global Cyber Alliance
- European Union Agency for Cybersecurity
- National Cyber Security Centre
- Institute of Electrical and Electronics Engineers
- United Nations Office on Drugs and Crime
- Cyber Peace Institute
- Interpol

Relevant Legal Treaties, Frameworks, and Conventions

- National Cybersecurity Strategy
- Global Cybersecurity Index
- Global Cybersecurity Agenda
- ICT Security Standards Roadmap

Relevant Conferences

- World Summit on the Information Society
- ITU Plenipotentiary Conference
- World Telecommunication Development Conference
- World Telecommunication Standardization Assembly
- International Conference on Cyber Security
- IEEE International Conference on Cyber Security and Resilience
- The International Conference on Cyber Security Intelligence and Analytics
- International Conference on Cyber Warfare and Security

Further References

- https://www.itu.int/en/history/Pages/ListOfITUConferencesAssembliesAndEvents.aspx
- https://www2.deloitte.com/global/en/pages/about-deloitte/articles/gx-future-of-cyber.html
- https://www.itu.int/en/action/cybersecurity/Pages/CYB4COVID.aspx

---

References

"Conferences and Meetings." *ITU*, https://www.itu.int/en/ITU-R/conferences/Pages/default.aspx.

"COVID-19 Cyberthreats." *INTERPOL*, https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats.

"CYB4COVID." *ITU*, https://www.itu.int/en/action/cybersecurity/Pages/CYB4COVID.aspx.

"Cyber-Attacks, Cryptocurrencies, and Cyber Security." *CESifo*, https://www.cesifo.org/en/publikationen/2020/working-paper/cyber-attacks-cryptocurrencies-and-cyber-security.

"Cybersecurity in the Healthcare Sector during COVID-19 Pandemic." *ENISA*, 26 Aug. 2021, https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-healthcare-sector-during-covid-19-pandemic.

Deb, Sagarmay. "Information Technology, Its Impact on Society and Its Future." *Advances in Computing*, Scientific & Academic Publishing, http://article.sapub.org/10.5923.j.ac.20140401.07.html.

"Discover ITU's History." *ITU*, https://www.itu.int/en/history/Pages/DiscoverITUsHistory.aspx.

"Full List." *Treaty Office*, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.

"General Secretariat Departments." *ITU*, https://www.itu.int/en/general-secretariat/Pages/departments.aspx.

"Global Programme on Cybercrime." *United Nations : Office on Drugs and Crime*, https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html.

"History of Cyber Security." *Cyber Security Degree*, 23 June 2021, https://cyber-security.degree/resources/history-of-cyber-security/.

"Impact of COVID-19 on Cybersecurity." *Deloitte Switzerland*, 15 Dec. 2020, https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html.

"Information Technology Definition & Meaning." *Merriam-Webster*, Merriam-Webster, https://www.merriam-webster.com/dictionary/information%20technology

"ITU Cybersecurity Activities." *ITU*, https://www.itu.int/en/action/cybersecurity/Pages/default.aspx.

Jefferson Online. "An Internet History Timeline: From the 1960s to Now." *Jefferson Online*, 10 Mar. 2020, https://online.jefferson.edu/business/internet-history-timeline/.

K;, Muthuppalaniappan M;Stevenson. "Healthcare Cyber-Attacks and the COVID-19 Pandemic: an Urgent Threat to Global Health." *International Journal for Quality in Health Care : Journal of the International Society for Quality in Health Care*, U.S. National Library of Medicine, https://pubmed.ncbi.nlm.nih.gov/33351134/.

Kaspersky. "2021 Top Ten Cybersecurity Trends." *Www.kaspersky.com*, 23 Aug. 2021, https://www.kaspersky.com/resource-center/preemptive-safety/cyber-security-trends.

"Knowledge, Technology and Complexity in Economic Growth." *Real Colegio Complutense*, https://rcc.harvard.edu/knowledge-technology-and-complexity-economic-growth.

Nicole.keller@nist.gov. "Cybersecurity Framework." *NIST*, 26 Oct. 2021, https://www.nist.gov/cyberframework.

"Our Vision." *ITU*, https://www.itu.int/en/about/Pages/vision.aspx.

"Resources." *United Nations*, United Nations, https://unite.un.org/digitalbluehelmets/resources#treaties.

Smith, Aaron, et al. "People Think Technology Impacts Politics Positively and Negatively." *Pew Research Center: Internet, Science & Tech*, Pew Research Center, 30 May 2020, https://www.pewresearch.org/internet/2019/05/13/publics-think-technology-impacts-the-political-environment-in-both-positive-and-negative-ways/.

"The History of Cybersecurity." *CompTIA's Future of Tech*, https://www.futureoftech.org/cybersecurity/2-history-of-cybersecurity/.

"Welcome to the History of ITU Portal." *ITU*, https://www.itu.int/en/history/Pages/home.aspx.

"What Does ITU Do?" *ITU*, https://www.itu.int/en/about/Pages/whatwedo.aspx.

"What Is a Cyberattack? - Most Common Types." *Cisco*, Cisco, 28 Sept. 2021, https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html#~types-of-cyber-attacks.

"What Is an Information System?" *Master's in Data Science*, https://www.mastersindatascience.org/learning/what-is-an-information-system/.

"What Is Cybersecurity?" *IBM*, https://www.ibm.com/ae-en/topics/cybersecurity.

Written by Algirde Pipikaite, Lead. "These Are the Top Cybersecurity Challenges of 2021." *World Economic Forum*, https://www.weforum.org/agenda/2021/01/top-cybersecurity-challenges-of-2021/.

Written by Belisario Contreras, Manager. "3 Ways Governments Can Address Cybersecurity in the Post-Pandemic World." *World Economic Forum*, https://www.weforum.org/agenda/2020/06/3-ways-governments-can-address-cyber-threats-cyberattacks-cybersecurity-crime-post-pandemic-covid-19-world/.