General Assembly First Committee

```Operation: Free Mali and Spain

The International Committee condemns the situation with the imprisonment of Mali and Spain. It is clear Nancy Pelosi imprisoned them without a trial, and with evidence not proved in court. The DISEC will declare that an Investigative committee will be made to look into this situation independently. Furthermore, Pelosi will apologize to Mali and Spain. Lastly, the international committee will issue a full trade embargo and stop all trade with the US if this does not this go through.```

Resolution Name: Internationally Safe Internet Security (ISIS)

Sponsors: the United States of America, State of Israel, Kingdom of Spain, French Republic, Dominion of Canada
Signatories: Kingdom of Belgium, Republic of India, Republic of Italy, State of Japan, Republic of Latvia, Republic of Mali, Kingdom of the Netherlands, State of Qatar, Kingdom of Sweden, United Kingdom of Great Britain, Northern Ireland, Republic of Poland, and Federal Republic of Germany.

The General Assembly,

*Understands* that a Cyber Attack is any virtual attack initiated in Cyberspace by a Nation or a Non-State Actor with clandestine intentions to alter, disrupt, deceive, degrade or destroy computer systems, networks or information with the aim of causing significant damage to critical infrastructures of a Nation and hence which would also affect the stability of the Nation, such an attempt is without consent,
*Aware* that Cyber Security refers to the different types of technologies present from predictive analytics to cryptography and more that functions as preventive methods used to protect a Nation, Organization or an Individual's privacy, devices, programs and data from an attack,
*Guided* by the purposes and principles of the Charter of the United Nations and reaffirming its role under the Charter, including on questions related to international peace and security,
*Defining* the dark web as the World Wide Web content that exists on darknets, overlay networks that use the Internet but require specific software, configurations, or authorization to access,
*Reaffirming* the fact that terrorist organizations are beginning to shift their operations onto the interwebs and the global darknet in order to continue recruitment, planning, etc.,
*Conscious* that cybercriminals and cyberterrorists are turning towards dark web software such as TOR and I2P,
```

Alarmed by the vulnerability of many individuals, corporations, and countries in terms of their cybersecurity index,
Emphasizes the fact that the Budapest Convention on Cybercrime has not been ratified by all states that have signed the same and member states who have signed it refuse to ratify the convention,
Perturbed by the fact that countries have been trying to use the terror of cybercrime to promote their own propaganda and internet control over their people, thus stopping the spread of democracy at a time when it is most needed,
Understands the repercussions of stricter internet usage on the human rights of worldwide individuals, including their right to privacy,
Recognizes the increase of cyber attacks on governments of United Nations member states and Organs, such as the Iranian-backed hackers that attempted to break into the accounts of the WHO amidst the COVID-19 crisis,
Emphasizes the need for effective measures against Cyber Attacks which need to be implemented, including cybersecurity awareness and restrictions on offending countries,

I. Suggests that Cyberspace is a domain of the Internet and the IoT (Internet of Things) to store, modify or exchange data via networked systems and associated infrastructures and hence cyberspace can be thought as the connection between human beings and telecommunication devices and computers without regards to physical geography;
II. Encourages the establishment of an international committee on cybercrime, an advisory body, funded by the member states and whose responsibility shall be to:
    A. Respect cyberspace and freedoms online by,
        1. Suggesting countries on cyber security strategies which would help to prevent cyber attacks,
        2. Informing the citizens of the global community through the United Nations news application about cyber attacks and preventive measures,
    B. Make reports on any suspicious activity in the cyberspace,
    C. Analyse the report and send it to states who have a risk of getting cyber attacked;
III. Promotes the member states to adopt a National Cyber Security Strategy whose ambition shall be to:
    A. Protect the safety and security of their citizens and their critical infrastructure,
    B. Promote and protect rights and freedoms online,
    C. Encourage cyber security for business, economic growth, and prosperity,
    D. Collaborate and support coordination across jurisdictions and sectors to strengthen cyber resilience, proactively adapt to changes in the cyber security landscape and the emergence of new technology;
IV. Encourages member states to impose strict rules on domain providers through their National Cyber Security Strategy, so as to:
    A. Increase the availability of domain names,

B. Avoid the influence of fake domains,
C. Encourage only real persons/groups to maintain and manage a domain,
D. Avoid disinformation provided through domains which don't even have certification for its information or any evidence for its reliability;

V. Suggests the implementation of a cybersecurity education program through the National cyber security strategy by member states within the school curriculums all over the UN member states' educations that involves such as but not limited to:
   A. The cybersecurity program must be strongly involved with all curriculums within the member states such as, but not limited to:
      1. International Baccalaureate,
      2. The British Curriculum.
      3. US National Curriculum,
      4. AP/Honors Courses,
   B. The cybersecurity education program will be completely online-based,
      1. Assuming the resources are available to the schools/students,
      2. Requesting that governments work to provide schools and students with necessary resources if not available,
      3. Including smaller aspects of Computer Science education, such as basic programming languages, such as, but not limited to, Python, Java, C++, C#, Ruby, etc.,
   C. The cybersecurity program will include information about cyberterrorism,
      1. In older years, such as Grades 8-12, and corresponding years in other curriculums, as Year 9-13 in IB,
      2. Importance of cybersecurity as a whole, including their own personal lives,
      3. How to handle cybersecurity threats on a small, civilian level,
   D. The cybersecurity program will be implemented as a program from primary schools across the country;
      1. Promoting an early-age understanding of internet security,
      2. Promoting higher-level computer science in high school and college courses,
      3. Creating international-wide competitions to locate talented youth;

VI. Suggesting scholarships for winners of these competitions to increase opportunities for potential talent in the cybersecurity field,
   A. Funding international operations for hackathons and suggesting these be in partnerships with companies like Google, Facebook or Twitter,
   B. The cybersecurity education program will initially be formulated and written by UNOCT, (United Nations Office of Counter-Terrorism), to ensure that students get a strong, valid education;

VII. Calls upon the implementation of economic sanctions on countries/governments that are involved in acts of cyberterrorism against individuals, corporations, or other countries,

A. Cyber-attacks targeted at critical infrastructure of a state would not differ from a conventional act of aggression,
    1. Treating Cyber Attacks on infrastructures of the State will be considered an act of aggression as mentioned in UNGA Resolution 3314 (2014),
    2. Following Article 40 and Article 41 under the Chapter VII of the Charter of the United Nations, the Security Council will first hold talks between the nations to comply with provisional measures, only if such members fail to reach a consensus, will the UNSC take adequate measures to restore international security and peace,
    3. Following Article 51 under Chapter VII of the Charter of the United Nations, the present clause shall not directly or indirectly impair the inherent right of self-defence to any member state,
        a) If retaliation has been followed through in the name of self-defence, the same must be communicated to the UNSC immediately,
        b) An act of self-defence will not in any way affect the decision of the UNSC;
B. This will include writing the International Cybersecurity Protocol Guide as used by CTIT, referenced in Clause 4, which will explain in detail the following, but not limited to,
    1. An official list of cybercrime that can be prosecuted, whether it is against civilians, governments, etc.,
    2. How to prosecute said crimes, such as the ICJ, etc,
C. The economic sanctions can be made in the form of the following, but not limited to:
    1. Trade embargoes
    2. Arms embargoes;

VIII. Suggests the implementation of an international cyberterrorism bureau the Cybercrime Terrorism Investigative Task Force (CTIT), funded by the member states, that would be made up of a roster of the world's best computer scientists, investigators, and international peace and conflict specialists, that would be responsible for, but not limited to:

A. Investigating the realistic claims made by countries against others, in relation to cybercrime as a whole,
B. Making a proper evaluation of the crime committed, and then informing the relevant authorities of the crimes committed, and the severity of said crimes, so the UNOCT and the United Nations as a whole can make responsible decisions regarding the crime,
C. Aid in the distribution of new technology among member states,
D. Aid in constructing improved infrastructures in underdeveloped countries,
E. To provide funding and investments to promote ties between member states and also improve in the field of cyberspace;

IX. Recommends MEDC member states to assist LEDC member states in the creation of their own Cybersecurity programs to assist against the following, but not limited to:
    A. Hacking attacks,
    B. Terrorist groups with an online presence,
    C. Illegal weapon/sex/human trafficking, as well as drug trafficking;

X. Suggests for member states to take certain measures in order to prevent/control cyber crimes by means such as, but not limited to,
    A. Monitoring consumer patterns on the dark web,
    B. Collecting information about new websites on the dark web and scrutinizing and storing this information in their database,
    C. Profiling dark web markets and tracking the change in patterns to link intelligence to build profiles over time;

XI. Requests a stronger implementation of already written resolutions on cybersecurity by the United Nations, such as resolution S/2482 by the Security Council, which would be much more effective if it were strongly implemented across the United Nations member states;

XII. Encourages countries not to violate their citizens, or any other country's citizens, right to privacy;
    A. In terms of private communication,
    B. Video/Voice calls,
    C. The following, without any proper reasoning to do so, without a warrant, etc

XIII. Requests that political propaganda spread through the internet be considered incidents of domestic/international cyberterrorism if it,
    A. Directly has a harmful impact on an individual or nation,
    B. Is responsible for international interference, such as:
        1. The manipulation of national elections,
        2. Political involvement,
    C. The governmental release of false information to its citizens.