**Economic And Social Council - ECOSOC**

**Agenda 1: Combating Organized Cybercrime**

**Background Information:**

Organized cybercrime is the work of syndicate, corporate or state sponsored cybercrimes as well as encompassing cyberterrorism. Organized cybercrime can include ransomware and denial of service attacks as well as attacks on ICT infrastructure. Combating organized cybercrime is a priority in order to protect data and information in a digital world. As a growing dependence on the internet emerges, the number of cybercrimes rises parallel to it. The growing expansion of usership means that cybercriminals have started utilising more sophisticated and highly concealed forms. Therefore, it is crucial for member states to get ahead of this issue and protect the civilian population as to the best of their abilities.

Cybercrime is not always the work of individuals but has been shown to be carried out by government against government as well as foreign intruders and extremist groups. From the initial cyberattack, the Morris Worm in 1988 to date, hundreds of cyberattacks have been carried out on a multitude of scales. Some examples of such crimes throughout the years include:

* 1988: The Morris Worm
* 1998: Solar Sunrise
* 1999: The Melissa Virus
* 1999: NASA and the US Defense Department Hacked
* 2000:MafiaBoy
* 2009: Google China
* 2012: Red October
* 2013: Cyber Attack on the Singaporean Government
* 2013: #OPISRAEL
* 2015-2016- WikiLeaks and the Democratic National Committee
* 2017: NOTPETYA

**Key Terms:**

*Ransomware*

Ransomware is software that is designed to prevent users access to their own computer system and/or files unless they pay money to the perpetrator, often through bitcoin.

*Cyber-Dependent Crime*

Cyber-dependent crimes are those that include the creation, dissemination and deployment of malware, ransomware, attacks on infrastructure and denial of service attacks. These crimes are carried out and enabled through ICT infrastructure.

*Cyber-Enabled Crime*

Cyber-enabled crimes are those that, although can be carried out offline, are further enabled due to the internet and technology. The type of crimes classified under this category include online fraud, online money laundering and the purchase of drugs online.

*Cyberterrorism*

The Federal Bureau of Investigation (FBI) defines cyber terrorism as ‘any premeditated, politically motivated attack against information, computer systems or computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents’.

**UN Involvement:**

The United Nations mandated the Global Programme on Cybercrime to assist member states in the struggle against cyber-related crimes. This was talked of in General Assembly resolution 65/230 and the Commission on Crime Prevention and Criminal Justice resolutions 22/7 and 22/8. The Global Programme on Cybercrime is funded by the governments of Australia, Canada, Japan, Norway, United Kingdom and the United States of America.

**Guiding Questions:**

* What policies does your country have on cybercrimes or cyber-related crimes?
* Has your country and/or government experienced cyberattacks against it? Who initiated these attacks?
* Has your government or individuals within your country perpetuated a cyberattack against another country?
* Does your country already have initiatives to combat cybercrime, and if not, why?
* How would your country resolve issues of cybercrime or cyber-related crime?

**Suggested Resources:**

* <https://securityintelligence.com/the-business-of-organized-cybercrime-rising-intergang-collaboration-in-2018/>
* <https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime-activities.html>
* <https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018>
* <https://www.unodc.org/unodc/en/cybercrime/index.html>

**Agenda 2: The Question of Economic and Social Repercussions on Post-Conflict Zones**

**Background Information:**

Since 1945 there have been more than 140 wars with an estimated number of casualties of 20 million and around 67 million people displaced. Since 1989, there have been over 100 armed conflicts, from minor battles to wars, placing the global community far from peace and harmony. Post-conflict, the task ahead to resume to normalcy is huge and can be sorted into three categories;

*Reconciliation:*

Post-conflict, if groups are unwilling to solve the problems that were the root of discontent, it is likely that the future of the country will be bleak. The atrocities of war causes coupled with a possible shift in ethnic balance makes it crucial for governments to promote reconciliation through the creation of laws that prohibit discrimination. It is also important that law enforcement visibly implements the new laws in order for the civilian population to have confidence in the integrity of state organs. The prohibition of discrimination is also important to increase productive employment in order for rebuilding be efficient and effective. Discrimination is the enemy to reconcilliation.

*Reconstruction*

The reconstruction of physical infrastructure and effective provision of social services is critical to the revival of a country’s post-conflict economy. Common problems post-conflict include a shortage of food and housing. Food, shelter, clothing and medical services therefore must be given priority post-conflict to ensure the civilian population has the basic means of survival. One of the highest issues is that none of the problems in a post-conflict country can be solved completely in isolation and thus reconstruction has to occur simultaneously on all fronts for it to be effective. This makes reconstruction a lengthy process requiring the utmost patience from governments and the civilian population.

*Economic Development and Poverty Reduction*

It was recognized during the Industrial Revolution that sustained development was important in reducing the risk of armed conflict and war. In order to be successful in improving economic conditions, countries must adopt goals that are consistent with the objective of improving general economic welfare as well as the need to employ a system of ownership and allocation of resources based on the country’s problems and social preferences of the civilian population. The principal goals of economic policy which were adopted more than 50 years ago are still relevant to post-conflict states due to their intention to prevent armed conflict within countries and between them. By increasing economic development and following these goals, poverty reduction is highly likely to follow and with it, the civilian populations trust and respond to the government.

It is important to realise that although these steps to achieve normalcy may come across as obvious and obtainable, it is likely that countries will still be recovering decades after a conflict and this recovery can cause unrest within the country.

**UN Involvement:**

ECOSOC has played a role in developing mechanisms to respond to problems countries who are emerging from conflict face and in doing so, helps prevent the deterioration of human security. In 2002, in resolution 2002/1, ECOSOC created a framework for advisory groups on African countries who are emerging from conflict (Ad Hoc Advisory Groups). Its role was to assess the humanitarian and economic needs of these countries and elaborate on long-term programmes of support. In this framework, ECOSOC set up two advisory groups on Guinea-Bissau and Burundi. These groups proved to be flexible and efficient mechanisms to bring synergies among development partners in support of the countries looking for recovery and stability. In 2006, the council decided to terminate the mandate of Ad Hoc Advisory Groups and instead add it to the agenda of the Peacebuilding commission.

**Suggested Resources:**

* <https://www.un.org/development/desa/dpad/wp-content/uploads/sites/45/publication/CDP-bp-2005-8.pdf>
* <https://www.undp.org/content/dam/undp/library/crisis%20prevention/undp-cpr-post-conflict-economic-recovery-enable-local-ingenuity-report-2008.pdf>

**Guiding Questions**

* Has your country or your country’s allies been a part of a now finished conflict? If so, how did this conflict affect it then and are its effects being felt now? How did it affect the other party?
* Has your country provided aid to another country after a conflict? In what form did this aid take?
* What effect has conflict had on ethnic populations within your country?
* Has your country had people emigrate out because of post-conflict conditions? If so, what conditions, and what can be done to resolve issues like these?

**References:**

* ARN. (2020). Top 10 most notorious cyber attacks in history. [online] Available at: https://www.arnnet.com.au/slideshow/341113/top-10-most-notorious-cyber-attacks-history/ [Accessed 25 Feb. 2020].
* Dictionary.cambridge.org. (2020). RANSOMWARE | meaning in the Cambridge English Dictionary. [online] Available at: https://dictionary.cambridge.org/dictionary/english/ransomware [Accessed 25 Feb. 2020].
* Digital Guardian. (2020). The Biggest Moments in Cybersecurity History (in the Past 10 Years). [online] Available at: https://digitalguardian.com/blog/biggest-moments-cybersecurity-history-past-10-years [Accessed 25 Feb. 2020].
* Itpro.co.uk. (2020). [online] Available at: https://www.itpro.co.uk/security/29726/what-is-cyber-terrorism [Accessed 25 Feb. 2020].
* The Windows Club. (2020). Cybercrime and its classification - Organized and Unorganized. [online] Available at: https://www.thewindowsclub.com/organized-and-unorganized-cybercrime [Accessed 25 Feb. 2020].
* Un.org. (2020). UN Economic and Social Council. [online] Available at: https://www.un.org/en/ecosoc/adhocmech/conflict.shtml [Accessed 25 Feb. 2020].
* Unodc.org. (2020). Global Programme on Cybercrime. [online] Available at: https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html [Accessed 25 Feb. 2020].