Position Paper for the Security Council

The topics before the Security Council are: Countering Terrorist Control over Commodities and Resources, and Protection of Civilians through Cyber Security. The Republic of Angola, as one of the African countries that have proven their competence to the world, continuously strives for peace over a wide-range of its territory, and promotes the importance of maintaining a comprehensive relation to other countries, which helps in coping with its national interests.

1. Countering Terrorist Control over Commodities and Resources

The attack of terrorists to certain countries these days terrifies individuals of all ages. Due to the developed technology, news is easily transmitted to all parts of the world which alarms everyone. The damage caused by an outbreak starts with the threats the government receives from the terrorists, up to the citizens who are certainly the victims and lastly, the effect it has on the stability of the country itself. With the emergence of different territorial outbreaks today, operation for strong security must be enforced, concerning to withstand terrorist control over transporting commodities and resources of the country.

Angola stresses peace and security as the founding sources of creating a strong and well-built nation for the people. At present, there may be no threats surrounding Angola from the surfacing Islamic State of Iraq and Syria (ISIS), but a single attack on one region affects every nation's interests in global exchange. This concerns mostly the European Union who just engaged to establish a more active political cooperation with Angola. According to the Economic Complexity Index (ECI), Angola is the 54th largest export economy and the 117th most complex economy worldwide. There are also other problems facing the country like the current issue in Cabinda, a province in Angola, regarding the intense conflict between the government and the inhabitants in that region. Immediate actions are needed for these types of issues to prevent further destruction over the country's welfare.

Member states must exert effort on this case to ensure sustainable living for the people. Such collaborations are needed among the delegates to perform a well-rounded action to provide a resolution on this agenda. The Republic of Angola proposes the International Safety from Terrorism Awareness Campaign which encourages all states to be part with for the benefit of one another. The campaign aims to provide (1) a faster transmission of news about the outbreaks of terrorism on a certain country; (2) to guarantee the protection of the people of every state member; (3) to provide awareness not just to the local governments but also to the citizens, for them to make the first action to keep themselves away from the place of attack; (4) to pass a bill that encompasses the danger that lies upon the people when receiving threats due to one country's global connection and economic contribution; (5) to let all the member states take into consideration first the situation of the people before abiding into some business connections that are not really advantageous to the status of the country. The Republic of Angola strongly assures that this movement will make an immense change to avoid, control and be ahead of the terrorists' plans of attacking.

II. Protection of Civilians Through Cyber Security

In this day and age, the world has become smaller through the advancements in the field of communication. It has allowed internet, online banking, data banks and telecommunications to make our lives easier and our work faster, but these information and ease of access also make it vulnerable to hackers. They can steal information about your location and personal information. In some cases, they can steal millions of dollars in secure banks like the $81million cyber heist that was stolen from the Bangladesh central bank. In a possibly worst case, these hackers could steal the codes to a nuclear

weapon and detonate it in another country that would cause another world war. With the emergence of numerous cybercrimes, operations for strong cyber security must be integrated into the valuable information system of the military and the civilians. It should be able to withstand numerous attacks and, if infiltrated, should be able to control the damage.

In the past, Angola has experienced numerous wars like the Portuguese colonial war and the civil war. Today, Angola is not in war but they are struggling financially since the war has only stopped in 2002. On the bright side, Angola has a rich oil reserve, harnessed through oilrigs. With the rich oil reserve, they were able to improve their economy and they are currently the 2nd largest oil producer in Africa. However, hackers managed to deface the oil company's websites and shut down the power system of these oil rigs, thus, stopping production. In another incident, the website of the Embassy of Angola had been defaced by hackers, rendering the site useless. These two cases alone reveal a major need for experienced cyber security engineers and a robust cyber security system that will aim to prevent infiltration and cyber-attacks on computer programs for communication, fuel processing, infrastructure, power, etc, thus, prevent unwanted losses of precious data and hard-earned wealth.

Member states must take action against these cyber criminals to ensure the protection of the civilian's information and financial security. Collaborations are needed among delegates to perform a well-rounded action to provide a resolution on this agenda. The Republic of Angola recommends that: (1) Strict Standards on Software Security Many cybercrimes are done through a software that is bug-ridden or it contains numerous flaws in the design. There is a need for greater standardisation and testing of software products to reduce the opportunity for hackers. A lot of software are produced with little consideration for security. We should cooperate to have a greater standardisation and have a high priority in the security of the software to minimize the hacker's chance to break in and steal the civilian's information; (2) Cyber Peace Treaty As entities and countries compete for wealth and power, and cyber espionage is becoming more common, a politically-motivated attack on the enemy's information systems could be waged. As experts say, a cyber-war in the near future is inevitable. A helpful resolution would be to require nations to sign a Cyber Peace Treaty wherein the signatories would agree that they will not use the internet infrastructure for cyber- attacks; (3) Law Enforcement Cyber criminals have a smaller chance of being caught when they steal $1 million from several people, versus cyber-theft of $1 million from a single person. If a person loses a big amount of money, the police response is immediate. If a cyber- criminal made a big amount of money from a thousand civilians, would the police respond to all those civilians? There is an apparent need to closely coordinate with the law enforcers to make sure that they are more prompt to deal with the cases of multiple individuals losing money on the net, as much as they are prompt to deal with a single individual's loss. No matter how many civilians report, they should be able to listen to each and every one of them so that the cyber-police could retrieve their stolen finances and information, and arrest the cyber-criminal; and (4) Launch Cyber-attacks on Cyber-criminals Numerous cyber-attacks in the world are harming civilians' lives through the stealing of their information and finances. Although some of the systems have been upgraded and there are numerous strong firewalls that protect the system against the cyber- criminal's infiltration, these are not enough as cyber-criminals are getting more clever and smarter at infiltrating systems. Because some of them want to disable civilians through the disruption of programs in the power stations, hospital, airports and the national grid, we must design systems that allow us to strike back at these cyber- criminals and be on the offense. When we strike back, we should be able to shut down their systems and arrest them. This will also send a clear message to the other cyber-criminals against infiltration.

Reference:

Angola. (n.d.). Retrieved from https://ec.europa.eu/europeaid/countries/angola_en

Security Council. (n.d.) Retrieved from https://www.un.int/angola/angola/security-council

Angola. (n.d.). Retrieved from
http://atlas.media.mit.edu/en/visualize/tree_map/hs92/export/ago/all/show/2013/

Ojakorotu, Victor. 2011. Perspectives on Terrorism. The Paradox of Terrorism, Armed Conflict and Natural Resources: An Analysis of Cabinda in Angola. Volume 5, Issues 3-4 p. 96

Bangladesh Central Bank Cyber Heist. (n.d.). Retrieved from http://www.ft.com/cms/s/0/39ec1e84-ec45-11e5-bb79- 2303682345c8.html#axzz43qh031rJ

Angola is the 2nd largest oil producer in South Africa . (n.d.). Retrieved from
http://www.opec.org/opec_web/en/about_us/147.htm

Cyber-attack on oil websites. (n.d.). Retrieved from https://www.recordedfuture.com/cyber-operations-against-oil-industry/

Falling oil prices may trigger more aggressive cyber attacks . (n.d.). Retrieved from
http://blog.neweggbusiness.com/news/falling-oil-prices-trigger-cyber-attacks/

Website of Embassy of Angola In Abu Dahbi Hacked by Moroccan Islamic Union-Mail . (n.d.). Retrieved from https://www.hackread.com/opangola-angolan-embassy-hacked-by-mium/

Britain will launch cyber attacks on terrorists. (n.d.). Retrieved from
http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/12000209/Britain-will- launch-cyber-attacks-on-terrorists-George-Osborne-warns.html

Proposal - Five concerns and five solutions for cyber security. (n.d.). Retrieved from http://www.global-economic-symposium.org/knowledgebase/the-global- polity/cybercrime-cybersecurity-and-the-future-of-the-internet/proposals/five-concerns-and-five- solutions-for-cyber security

What is cyber warfare? . (n.d.).Retrieved from
https://www.techopedia.com/definition/13600/cyberwarfare