The Republic of Colombia

Positions for the International Criminal Police Organization

I. Addressing the Role of Transnational Organized Crime Groups in Human Trafficking

The Republic of Colombia fully *understands* the importance of addressing the role that transnational crime groups play in Human Trafficking, and we *commit* to fighting this crime against humanity that has currently entrapped nearly 25 million people. In discussing solutions for dealing with these groups, it is important to note how these groups operate. Colombia is very familiar with transnational organized crime; we unfortunately have a tainted history due to cartel activity. Although we have had trouble in fighting transnational organized crime groups throughout our history, we hope that the international community will benefit from our insight, and we *pledg*e to work alongside INTERPOL in fighting these organizations. Organized crime cells often prefer to operate in countries that are either in the beginning stages of development, or in countries that are suffering from conflict, whether it be internal or external. Transnational crime groups capitalize on this instability; they enjoy a freedom to engage in their activities without fear of exposure. A commonly employed tactic by such organizations is to enter impoverished areas and declare opportunities for a better quality of life. Upon individuals consenting, they are stripped of all personal belongings and thrust into a life of servitude.

Domestically, the issue of human trafficking is a real and present danger for the Republic of Colombia, as it is for many Central and South American countries. Colombia unfortunately is known as a 'Sex Destination' for 'Sex Tourism', in which foreigners from different nations visit for the sole purpose of engaging in prostitution with women, and sometimes even children. Also, the current political unrest of neighboring countries in the region brings in an influx of displaced individuals, providing organized crime groups with thousands of potential victims. We agree with the U.S. Department of State's assessment of the situation. They state that, "high risk victims of human trafficking are displaced persons, indigenous Colombians, and Colombians in regions where armed criminals are active". The rising problem of human trafficking jeopardizes the freedom of innocent civilians and allows the manifestation of larger problems to develop in the region. The growing prominence of organized crime groups has led to the increased involvement of our administration in combating the nefarious acts being committed.

Internationally, The Republic of Colombia would like to draw attention to undertakings on this issue coming from well developed countries. Canada assists countries with this problem through ASEAN; they help countries plagued with human trafficking by providing governments with funding and resources to fight organized crime groups. The Republic of Colombia moves to adopt a similar initiative with Project **E.S.C.A.P.E.** in which **C**entral and South American countries would be able to **E**nhance member state intelligence, **S**upply the needed resources, **C**ombat organized crime groups, **A**pprehend members of these organizations, **P**rotect the current and possible victims of human trafficking, and **E**ncourage the safe development of citizens from threats of transnational organized crime. The Republic of Colombia *notes* the ongoing issue of human trafficking and the increasing influence of transnational organized crime groups; we request that members of INTERPOL and the international community join forces to protect the hundreds of thousands of current and potential victims of human trafficking.

II. Combating the Threat of Cyberterrorism

The Republic of Colombia *commits* to protecting the cyber network from incursions. Recent events around the world have shocked not only Colombia but almost all member states of this distinguished body. The 2017 WannaCry Ransomware attack showed the world the vulnerabilities of cyber infrastructure for financial networks, electric grids, medical facilities, and our home governments themselves. **Domestically**, we have been directly affected by attacks like these. Our National Institute of Health was directly affected by the ransomware attack, and forced to temporarily take down its website during the attack. In 2014, Colombian President Juan Manuel Santos' email was hacked during crucial FARC negotiations, and information was released to the public that caused political division and jeopardized the negotiation process. The fallout of this attack could have been catastrophic and deadly, given the scale and sensitivity of the Colombian conflict. The hacking of the President's email during the negotiations was another even that showed us that even the highest levels of our government are susceptible to cyber-attack. Colombia has a vested interest in protecting its cyber infrastructure, and Colombia is well aware of the risks that ransomware attacks pose for all member states. We are grateful that INTERPOL's response in this field of crime is growing. In 2014, INTERPOL opened a permanent cyber security branch office in Singapore that has been actively working to address cybercrime. Much work on this branch of INTERPOL is still needed, and the Republic of Colombia is *willing* to assist INTERPOL much as we possibly can in addressing cyberterrorism.

Internationally, cooperation in fighting these attacks is essential, given the fact that many of these attacks are not bound by national borders. In response to the growing threat of cyberterrorism, Colombia *proposes* **I.N.T.E.R.N.E.T.** for members of INTERPOL to adopt. **INnovating Training Exercises** such as The Digital Security Challenge that are held annually, need to be expanded and held more regularly. Only through constant training and testing of our cyber infrastructures can our officers be fully equipped and prepared to combat the rising tide of cyber terrorism. We propose a biannual joint-training exercise focusing on defending cyber infrastructure. An internationally tested and stable cyber defense system should be implemented in countries vulnerable to cyber attacks. **Responsiveness** is key in addressing the issue of cyberterrorism**.** Even the slightest delay in dealing with a Denial of Service Attack or ransomware attack on a state's critical infrastructure can have devastating effects on the populace and possibly our global economy, and the training exercises we are proposing will surely improve response time. As a body we need to work on our collective response time, again considering that cyber attacks can affect multiple member states at once. We can limit the impact of DOS attacks if we can detect the early warning signs and isolate them to a single contaminated system. To accomplish this, greater interstate communication is necessary. **New** inter agency initiatives need to be established. The European Union's actions to create in 2017 TITANIUM is an example of an effective cybersecurity program, and similar programs should be implemented in South America and in other regions. Permanent interstate corporation will increase cybersecurity for all member states. We should also work towards expanding the UNODC's role in cybersecurity. **Established** leading cyber corporations need to be integrated into the existing framework in a higher degree. The Republic of Colombia recently struck a deal with software giant Microsoft to help combat credit card fraud with in our borders. We *encourage* member states to find solutions through the private sector while working with organizations like INTERPOL and the UNODC. Private companies can offer valuable insight into cybersecurity systems that they may have played a part in creating. Also, referring to their judgment could help alleviate some of the training costs. **Technology** sharing needs to become the status-quo for cybersecurity. The Republic of Colombia understands the sensitivity that involves the sharing of technology, and we understand that there will certainly be debate over a proposition like this, so we are looking forward to negotiating with other member states to find solutions that work best for everyone. It is our ultimate belief that by implementing **I.N.T.E.R.N.E.T**, international cyber infrastructures will be safer from cyberterrorism, and in the event that an attack happens, response will coordinated, swift, and sufficient.