Forum: Third General Assembly

Issue: Strengthening international cooperation to combat cybercrime

Student Officer: Nafe Ahmed

Position: Head Chair

Introduction

The cooperation of UN members over the years have allowed our world to develop as a single entity using digital information systems. Entire global sectors of a nation's economy are reliant on digital infrastructure without it transactions of goods would not be possible. With increasing inter-connectivity of member states, we can foster the development of transnational dialogue and act as the backbone to not only strengthen bilateral relationships but also as a stepping stone to further develop our world. However, with increasing digital presence comes the increasing risk of cybercrime and cyber espionage. The rapid way that nations are developing and using more complicated digital information systems is truly breathtaking, but we must be wary of the fact that at any time, a digital attack may be imminent. However due to the sophistication of the technology that cybercriminals use to commit crimes makes it hard for governments to track and prosecute those involved. This alongside, the lack of laws that counter-act cybercrimes in many nation's legalisations has hindered official's in properly coordinating ways to catch these criminals hence, some cybercriminals avoid large punishments and can be very difficult to chase. One of the essential ways that the world can counteract this sort of aggression from individuals who seek to diminish the world's increasing prosperity is to increase understanding between nations which will allow the them to strengthen the world's solidarity in fighting these sorts of attacks on sensitive digital information. Without cooperation, countries have realised the extent of the damage that these crimes can cost on economic and political security and in some cases, public relations.

It is essential the world takes notice of the increasing number of online users, as over 40% of the world population have access to the internet. This allows cyber-criminals or hackers to have an endless number of targets to which they can hack and gain sensitive information from. Labelling this environment as a place of common crime, originally created for the share of information and a platform to begin a modern era of connectivity, is unacceptable and has become a perfect place for cybercrimes to occur. The magnitude of cybercrimes varies, ranging from small personal acts that primarily focus on websites to the breach of sensitive national security data. Either way, the digital space known as the internet needs to be regulated and monitored in a fashion in which all members nations will be satisfied and in which they can stand as a united front against those who seek to violate the original ideology of the creation of a virtual space.

Definition of Key Terms

Cybercrime

It is an illegal activity that uses a computer, or a device connected to network to access data or information that is classified as sensitive. It can sometimes be classified as the subject of the crime (hacking, phishing etc.) or utilized as a tool to commit a crime (hate crimes, identity theft etc.).

Cybercriminal

An individual who commits a cybercrime by using any device that can connect to a network or a computer. Cybercriminals use computers to commit crimes in a few different ways. They can solely attack a single computer by stealing people's personal information stored on laptops or by install malicious data on them remotely. Also, by using the computer to commit an offense such as committing fraud or illegally gambling. Finally, a person who uses a computer to store sensitive information obtained illegally is a cybercriminal.

Cyber Security

It is the practices, processes and technologies that can protect a computer from attack, damage and unauthorized access. A computer can have platforms and applications that provided multiple forms of cybersecurity such application security.

Virus

A computer virus is a type of malicious code or program that has been written to change the way a computer functions. It is designed in a way that allows it to spread from one computer to another. It usually gets on a specific device by attaching itself onto a legitimate document or program so it bypasses any system firewalls or defense mechanisms.

Spoofing

. It is a malicious practice in which a communication (i.e. a message, an SMS) is sent from an unknown source disguised as a known source. One of the most common type of spoofing is email spoofing, it is where an email from an unknown user is sent but it is perceived to the recipient as a known contact.

Firewall

It is a software or hardware security system that is used to regulate the incoming and outgoing network traffic. It usually acts a barrier between a trusted and untrusted network. If data from the

untrusted does not match the policy that has been set up on the firewall protocol, then it is denied from reaching its intended destination.

Cryptography

It is a method in which data is stored or transmitted in a form that is unreadable to anyone who does not know the code that deciphers it. This means it can only be read by the person who the data was intended for. This means this data achieves confidentiality, integrity and is authentic.

Background Information

Member nations must work together to ensure that digital space is kept safe for everyone to use and that the sharing of information, sensitive and insensitive alike, are dealt in the correct manner. Only with great diplomacy and understanding can nation forge relationships that will lead to the creation of a safe cyber space. One of the main flaws that make cybercrime, a common criminal offense to commit is its profitability with little to no physical risks. The reason due to its high profitable is the fact that sensitive data pertaining to a countries major sectors such as military or defense division can be manipulated by perpetrators to cause severe damage to a single nation functioning without having to leave the vicinity of one's house. With the increasing expansion of networking system, a perpetuator can commit a cybercrime in a certain crime from a nation halfway across the world. This proves that one country alone cannot eradicate cybercrime in its borders by itself, it needs the assistance of others to catch these criminals committing these transnational crimes.

Types of Cybercrime

The increasing number of cybercrime can be attributed to the advancements and sophistication of day-to-day technology. Computers are becoming highly advanced and easier to use. This increases the easiness of the committing cybercrime. There are many types of cybercrimes ranging from identity theft to global tax fraud.

Identity theft

This is when a criminal takes personal information found online and uses it to commit unauthorized actions for personal gain. This form of cybercrime is one of the easiest to commit as it attacks an individual on a personal level. In many cases, medical records are stolen by cybercriminals, so they can illegally access many healthcare benefits that certain people get. In a study done in 2017, it was found that the amount of money stolen from US consumers has increased over the years from $15.3 billion in 2015 to $16 billion in 2016. These sorts of attacks may lead to victims having massive financial loses or ruin their reputation on reports such as credit reports if the thief isn't caught. This shows that nations must come together to ensure that

citizens of their country are not robbed of their hard-earned money by crackdown on cybercriminals.

Hacking

This is when a criminal gains illegal access to a website or any form of sensitive information. Hacking happens on a multitude of levels. There have been cases in which, entire divisions of a country's governmental offices have been hacked by criminals. Usually these hackers seek out large sums of money but also have ulterior motives such as to tarnish the reputation of the government. At the same time, a business's computer can be victim to hackers in which the steal information and then alter the computers software to change the website and ultimately alter the creator of the websites goal of the original intent of the website.

Theft of sensitive data and intellectual property

These two felonies have become very common types of cybercrime. Theft of sensitive data entitles a criminal stealing data that holds sentimental value to a person or a business. This information could potentially be leaked to the public which can cause the loss of public image and/or financial stability. Thefts of sensitive data can in some cases be very dangerous to the stability of relationship between two nations. Therefore, ensuring the safety of this data is key to making sure that transnational dialogue is maintained.

At the same time, the theft of intellectual property is similar to the theft of sensitive data but in this case, this is a case in which a felon steals copyrighted materials. This means that commercial entities that holds a copyright or a patent has the intellectual right stolen online by a criminal in another country. In some situations, these could lead to disputes between countries and damage cooperation attempts in eradicating cybercrime.

The Difficulty of a Global Response

The reasons behind the lack of a worldwide crackdown are the difficulty in getting countries to cooperate. There is still a problem with nations not being able to set differences aside and transcend national borders to theorize and implement global strategies to eradicate cybercrime. This is mainly due to a number of underlying issues that arise when countries come together to discuss strengthening cooperation in ensuring our cyber space is safe for everyone.

Differing legislations

This is probably one of the most common issues when dealing with issues that pertain to international matter. Cases arise, when a cybercrime offense is committed in a country however the criminal originates from another country. This creates a situation in where a nation's law enforcement would be reluctant to release a criminal from their country to stand trial in another

country. This usually hinders the persecution of the criminal and inadvertently strains relationship between countries as they are unwilling to hear the other side's ideas.

Another problem that may arise is the differing in legislation regarding the offense of a cybercrime. Some nations to this day lack concise laws that can be used in the court of law. The problem may occur, if a nation's judicial system of one country feels that cybercriminals should have harsher sentence as opposed to another. This further creates more dilemma and cause a breakdown in communications between the two countries involved.

Different rates of occurrence

The rate of cybercrimes occurring varies from country to country, for more-economically developed countries such as the USA and China, cybercrimes maybe more common as opposed to less-economically developed countries. In 2016, cybercrimes accounted for 1.33 billion dollars in damages in the United States of America; this is compared to Kenya losing 23 million dollars due to cybercrimes in 2014. This means that eradicating cybercrime varies in priority on governmental agendas. This causes a setback. Countries may not be willing or have the resources to use in order to regulate cybercrime in their country. This is one of the main things that prevent total international cooperation. Something that is essential that is required to remove crimes against our shared digital space.

Internet reliability

The increasing reliability of business and the governments on the internet means that if new legalization was introduced global, it could hamper business and governmental divisions economically with their daily accessibility of these companies, something which they are reliant upon.

The Budapest Convention on Cybercrime

Also known as the Convention on Cybercrime, it is one of the only guideline introduced by the Council of Europe. It was fundamentally a foundation for legislation against cybercrime for which countries had agreed upon. It was the framework that would be used to enhance international cooperation of member states. It covers the fundamentals to working against cybercrime, such as what entitles a cybercrime. The Convention on Cybercrime was originally drafted in 2001. In 2003, there was an Additional Protocol added to the document. The protocol classified any xenophobic and racist propaganda published on the internet would be classified as a punishable cyber offense. The treaty was used to show the destructive effects of cybercrimes. Also, it is stressed to be something that governments could use to help model their respective policies against cybercrime. It includes procedure that law enforcement could integrate into laws to aid the capture of cybercriminals.

The Involvement of UN Bodies

Since cybercrime has developed into a transnational issue over the recent years due to higher percentages of the population having access to the internet. As of 2011, at least one third of the global populations had access to the internet. As of March 2017, around 49.4% of the world has access to internet, this shows the rapidly increase rate of which technology is being integrated into our lives. According to UN reports, there will be an excess of electronic devices that have internet. It is estimated that the ratio of the network device will outnumber the population by six to one. This massive global community on the web means there will no doubt be crimes that violate Internet protocols will happen. Therefore, the UN Office of Drugs and Crime (UNODC) has taken a leading step with global organization to reduce and ultimately eradicate cybercrime.

UNODC have put a focus on this pressing matter due to the fact that internet safety is crucial to the global population. The internet is a platform to access a massive database of information and data. By having it comprised, will lead to the lack of development and hinder the progression of member nations. Online information systems are becoming more important as economics boom. The global economic sector is becoming heavily reliant on network devices as physical money (i.e. bills and coins) are becoming redundant, causing the rise of internet banking services.

With this problem, the UNODC created a strategy that with the support and cooperation of member nations would flourish. This is the Cybercrime repository. This repository was established with the help of the Commission on Crime Prevention and Criminal Justice (CCPCJ) in 2015. Its job is to function as a database and legislation that would nations could use to help them tackle cybercrime and correctly prosecute cybercriminals. The repository is made up of three main parts; The Database of Legalisation, The Case Law Database and The Lesson Learned Database. The first part is an extensive guideline on the procedures that are to be used in the court of law. This database is very detailed to the point it includes the legislation of over 180 countries and can be searched by country, procedural aspects and types of offenses. The Case Law Database provides real-life situations in which law enforcement operations were successful in getting rid of cybercrime or cyber offenses. By including these detailed records give nations the ability to see how another member nation dealt with a cybercrime on a legal and operational prospective efficiently. Finally, the Lesson Learned database is one where information is gathered from various sources such as the UNODC Comprehensive Study on Cybercrime and different established nation that have strong policies to ensure high cybersecurity. This will give nations a wide range of information to which they can combat cybercrime.

To compliment the Cybercrime repository, UNODC hosts a Crime Congress every five years with the previous one being held in 2015 in Doha, Qatar. One of the key areas that were address, was cybercrime. There was a focus on cybercrime to address the issue to translate many policies and legislation into practice. Another problem that was identified was the effect of cybercrime on development. It is very crucial to tackle to cybercrime in order to achieve the sustainable development

goals set out by the member states of the UN. Cybercrime can potentially hinder economic growth and has caused the divide between member nations. The next Crime Congress set to be held in Japan in 2020 will look to improve and add to the Doha Declaration where cybercrime strategies were decided upon.

Major Countries and Organizations Involved

The People's Republic of China

China is reportedly one of the largest victims of cybercrimes. This is due to its large population and high proficiency in working with highly advanced digital systems. The majority of the cybercrimes that occur in China usually originate from China itself. Instead of dealing with this uphill task of apprehending cybercriminals by themselves, they have requested help from other member states. This is evident in 2014 when China released a policy paper outlining a way to strengthen the China – EU relations in order to abolish cybercrime. China was open to talks with leaders of the European Union in which a strong plan could be devised while at the same time would respect the countries policies. The policy paper included many things with an emphasis on improving communication on security policies such as cybercrimes.

However, many countries have been reluctant to partner with China in working to remove cybercrime from society due to the large number of cybercrimes originating from China. Some of the largest and most destructive cybercrimes originate from China, causing countries to fear they may be targeted more strongly by Chinese cybercriminals by developing a close relationship with China.

United States of America

Alongside China, the United States of America is one of the biggest victims of cybercrimes. The United States have implanted many programs to ensure that cybersecurity is as strong as it possible can be. Every year, a US Cyber Crime Conference is held which provides training and supports to law enforcement agencies on how to tackle cases where technology is used as a tool to commit a crime. Over the years, the United States has worked with China to improve countermeasures against cybercrime.

Russian Federation

The Russian Federations has been well- known to reject any international cooperation to solve cybercrime with foreign law enforcements. They are also not a member of the 55 parties that have signed to follow and implement the Budapest Convention of Cybercrime in their nation's legislation. They rejected the Convention due to a lack of overlap between Russian policies and the conventions ideas. Due to this lack of openness for Russia, many attacks from Russian hackers have been allegedly

supported by the Russian government. In most recent times, during the 2016 American presidential election, Russia has been accused by the US of 'meddling' with the votes, bringing President Donald Trump to power. There have been multiple accusations from the American government at which Russia has neither denied or confirm to this date. This has further driven a wedge between the relationship between the two nations.

International Police Organization (INTERPOL)

INTERPOL has taken an active role as being the global mediator between conflicting sides in order to remove cybercrime from our shared society. It has a facility in Singapore called the INTERPOL Global Complex for Innovation (IGCI) which opened in 2014 and contains cutting-edge technology that can aid research and development of techniques and methods to shut down cybercriminals. INTERPOL has aimed to be the driving force that will take digital law enforcement to a new era where cybercrime is non-existent. They work around three main initiatives; harmonization, capacity building and operational and forensic support. Harmonization is when INTERPOL frequently pushes and encourages member nationals to purse international cooperation by facilitating experts to share their vast knowledge on the subject. This is also done in partnership with regular reviews of national cybercrime reviews, where experts examine the abilities of a nations cybercrime unit and helps it improve areas where lacking is found. Secondly, capacity building is the training of law enforcements officers and governmental employees to understand and identify cybercrimes if they happen. They cover a wide range of topics from investigation techniques to trends in cybercrime. Finally, operational and forensic support entitles INTERPOL operatives and agents with proficient knowledge of the field of cybercrime assisting and supporting member states in finding a cybercriminal. They also often act as the intermediary between nations if the cybercrime is transnational.

Timeline of Events

Date	Description of event
1973	The US Defense Advanced Research Projects initiates a program that monitors and regulates devices that link computer networks
1997	Representatives from Britain, Canada, France, Germany, Italy, Japan, Russia and the United States (G8) have a meeting in Washington D.C, to start a foundation against cybercrime, establishing a group called the Subgroup of High-Tech Crime.
February 1998	The first major cyber-attack occurs on a governmental website. The US Department of Defense has sensitive information from over 500 systems is stolen from locations all across the world by 3 teenagers in California.

2001	The Budapest Convention of Crime is drafted and ratified by the Council of Europe.
2003	The Additional Protocol is added to the Convention of Crime.
2006	The Federal Bureau of Investigation (FBI) shares multiple initiatives at the RSA Security conference.
2013	The European Cybercrime Centre begins operations.
2014	China releases the policy paper where it shows its willingness to cooperate with the EU on the issue of cybercrime and start strategizing plans to abolish it.
2016	The most prominent cybercrime scandal of whether the American Presidential Election was hacked by Russia occurs.

Relevant UN Treaties and Events

- The Budapest Convention of Cybercrime, effective 1 July 2004
- Prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children, 28 July 2011, **(E/2011/30)**
- Twelfth United Nations Congress on Crime Prevention and Criminal Justice, 1 April 2011, **(A/RES/65/230)**
- Strengthening the United Nations crime prevention and criminal justice programme, 27 March 2013, **(A/RES/67/189)**
- Strengthening international cooperation to combat cybercrime, 2013 **(Resolution 22/7)**
- Doha Declaration, April 2015
- Comprehensive Study on Cybercrime, February 2013
- Promoting technical assistance and capacity-building to strengthen national measures and international cooperation against cybercrime, 2013 **(Resolution 22/8)**

Previous Attempts to solve the Issue

The formation of the G8 group consisting of Britain, Canada, France, Germany, Italy, Japan, Russia and the United States can be considered as one of the first multi-national attempts to stop cybercrime. They came together and decided to focus on many different types of cybercrimes from electronic fraud to corporate espionage. The most important measure that was established was the training of local law enforcement officers to deal with cybercrimes and prepare them for a range of cybercrimes. This was also paired with the co-ordination of prosecution efforts so that countries

understand how to try a cybercriminal with maximum efficiency. The availability of 24 hours-a-day contact service to help national police was also created. This would aid police to respond to cybercrimes more quickly and give them advice on how to catch a moving criminal in a concise manner. In later meetings, the aim of quick cooperation on Internet-related investigations and rapid intervention were focused upon. Unfortunately, the G8 initial plan to get other countries involved fell through mainly because of LEDCs unwilling to divert its national resources to meet the demands and standards set up by the G8.

Another key attempt was the Budapest Convention. There is no denying that it provided the world with the perfect stepping stone to propel it to global cooperation against cybercrime. However, due to some issues, its effects have been limited. Due to the guideline being drafted by the Council of Europe, non- EU like India refused to ratify as it wasn't involved in the process of drafting. This with countries who simply refuse to ratify it like Russia hampered the guideline of its full potential.

Possible Solutions

It is first and foremost essential to make all countries aware of the severity of cybercrime has on the world. Therefore, through international workshops were all member nations are invited to participate should be implemented. At these workshops, experts from organizations that have researched the effects and the financial threat that cybercrime imposes can inform these representatives about the situation. This will help lead to a global understanding that regardless of whether you are a More Economically Developed Nation (MEDC) or a Less Economically Developed Nation (LEDC), ensuring citizens have a secure connection to a pool of beneficial information is essential. Citizens are the building blocks of a nations development therefore digital networks need to regulate to the extent where people they have the right to access the information they need in a legal manner.

An international body designed to combat cybercrime has already been created in the form of INTERPOL however some countries may feel unease to co-operate them. This makes moving forward in the ongoing conflict difficult to deescalate a bit difficult. Nations within the UN must be able to trust INTERPOL. Since this trust cannot be earned in one day, a viable idea would be getting INTERPOL to train national law enforcement with basic training in dealing with cybercrime. Once this trust can be fully earned, INTERPOL could assist with major attacks. Also, in cases where the cybercrime is transnational, INTERPOL would be the ideal agency to oversee the peaceful collaboration between the 2 countries.

A major setback is that certain nations do not have the capabilities to make cybercrime a high priority issue on the government's agenda. Therefore, the UN could offer incentives and benefits to these countries in return the country would pass these basic global cybercrime laws like in the Budapest Convection of Cyber Crime.

Bibliography

"Countries Collaborate To Counter Cybercrime." *SIGNAL Magazine*, 16 Jan. 2015, www.afcea.org/content/countries-collaborate-counter-cybercrime.

Li, Xingan. "International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene." *Webology*, Webology, www.webology.org/2007/v4n3/a45.html.

Tripwire Guest AuthorsOct 12, 2017Featured Articles. "Will the World Really Cooperate in Curbing Cybercrime?" *The State of Security*, 13 Oct. 2017, www.tripwire.com/state-of-security/featured/will-world-really-cooperate-curbing-cybercrime/.

"Cyber Crime: Reported Damage to the IC3 2016 | Statistic." *Statista*, www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/. Accessed 27 Oct. 2017.

"Budapest Convention and Related Standards." *Cybercrime*, www.coe.int/en/web/cybercrime/the-budapest-convention. Accessed 27 Oct. 2017.

"Cybercrime." *Cybercrime / Cybercrime / Crime Areas / Internet / Home - INTERPOL*, www.interpol.int/Crime-areas/Cybercrime/Cybercrime. Accessed 27 Oct. 2017.

"International Cooperation against Cybercrime." *Cybercrime*, www.coe.int/en/web/cybercrime/international-cooperation. Accessed 27 Oct. 2017.

"Internet Users." *Number of Internet Users (2016) - Internet Live Stats*, www.internetlivestats.com/internet-users/ . Accessed 27 Oct. 2017.

IOCTA 2016, www.europol.europa.eu/iocta/2016/distribution.html. Accessed 27 Oct. 2017.

Malakata, Michael. "Africa's Effort to Tackle Cybercrime Gains Momentum." *PCWorld*, IDG News Service, 8 Sept. 2015, www.pcworld.com/article/2981739/africas-effort-to-tackle-cybercrime-gains-momentum.html. Accessed 27 Oct. 2017.

"Malware." *What Is A Computer Virus?,* www.us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html. Accessed 27 Oct. 2017.

S, Shalini. "Budapest Convention on Cybercrime – An Overview." *The CCG Blog*, 8 Sept. 2016, www.ccgnludelhi.wordpress.com/2016/03/03/budapest-convention-on-cybercrime-an-overview.html. Accessed 27 Oct. 2017.

"Sci/Tech | G8 Wages War on Cyber-Crime." *BBC News*, BBC, 11 Dec. 1997, www.news.bbc.co.uk/2/hi/science/nature/38009.stm. Accessed 27 Oct. 2017.

Selyukh, Alina, and Doina Chiacu. "China Cyber Crime Cooperation Stalls after U.S. Hacking Charges." *Reuters*, Thomson Reuters, 26 June 2014, www.reuters.com/article/us-usa-cybersecurity-

china/china-cyber-crime-cooperation-stalls-after-u-s-hacking-charges-idUSKBN0F12OJ20140626. Accessed 27 Oct. 2017.

"A Timeline of Cyberwar and Cybercrime." *Hazlitt*, 8 Aug. 2014, hazlitt.net/blog/timeline-cyberwar-and-cybercrime. Accessed 27 Oct. 2017.

"What Is Cryptography? - Definition from WhatIs.com." *SearchSoftwareQuality*, www.searchsoftwarequality.techtarget.com/definition/cryptography. Accessed 27 Oct. 2017.

"What Is Cybercriminal? - Definition from Techopedia." *Techopedia.com*, www.techopedia.com/definition/27435/cybercriminal. Accessed 27 Oct. 2017.

"What Is Email Spoofing? - Definition from WhatIs.com." *SearchSecurity*, www.searchsecurity.techtarget.com/definition/email-spoofing . Accessed 27 Oct. 2017.

"What Is Firewall? - Definition from WhatIs.com." *SearchSecurity*, www.searchsecurity.techtarget.com/definition/firewall. Accessed 27 Oct. 2017.

"International Cooperation against Cybercrime." *Cybercrime*. N.p., n.d. Web. 27 Oct. 2017. https://www.coe.int/en/web/cybercrime/international-cooperation.

"The Effectiveness of International Co-operation against Cybercrime." N.p., n.d. Web. https://rm.coe.int/16802fa3a2

Sidley Austin LLP -Colleen Theresa Brown, Edward R. McNicholas, Alan Charles Raul and Anna L.Spencer. "Data Security and Cybercrime in USA." *Lexology*. N.p., n.d. Web. 27 Oct. 2017. https://www.lexology.com/library/detail.aspx?g=769815b3-3087-4030-a469-e7c319970d8c.

Nancy Cao. "United Nations Office on Drugs and Crime." *Sustainable Development Goals*, www.unodc.org/unodc/en/about-unodc/sustainable-development-goals/sdgs-index.html.

Akara Umapornsakula. "United Nations Office on Drugs and Crime." *Cybercrime*, www.unodc.org/southeastasiaandpacific/en/what-we-do/toc/cyber-overview.html.

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

Agustina Diaz-Rhein. "United Nations Office on Drugs and Crime." *Cybercrime Repository*, www.unodc.org/unodc/en/cybercrime/cybercrime-repository.html.

Cybercrime Repository, www.unodc.org/cld/v3/sherloc/index.jspx?tmpl=cybrepo.

Carlos Gomez del Campo. "United Nations Office on Drugs and Crime." *Crime Congress 2015: A Focus on Cybercrime*, www.unodc.org/unodc/en/frontpage/2015/March/focus_its-a-crime_-cybercrime.html.

Doris Resch. *Thirteenth United Nations Congress on Crime Prevention and Criminal Justice*, www.unodc.org/congress/index.html.

Carlos Gomez del Campo. "United Nations Office on Drugs and Crime." *UNODC and Japan Strengthen Cooperation with Eye on Security and Development, 2020 Crime Congress*, www.unodc.org/unodc/en/frontpage/2016/March/unodc-and-japan-strengthen-cooperation-with-eye-on-security-and-development--2020-crime-congress.html