UNODC

Cybercrime and the Dark Web

UCIMUN 2020

Welcome Delegates,

We are Hana Schlosser and Angie Lo, and we are the Secretaries-General for the UCI Model United Nations 2019-2020 school year. We are honored to serve as part of your Secretariat this year and are excited for everything we have planned for the conference. We truly hope you find our conference to be enjoyable as well as engaging and educational in nature.

Hana is a 4th year Biomedical Engineering major with passions in both biology and politics. This is her fourth year participating as part of the UCIMUN Conference Staff, previously serving as Assistant Director of Ad Hoc on Terror, Director of SOCHUM, and Director-General. She originally joined UCI's MUN program because she wanted to continue intellectual discussions outside of STEM after participating in Speech and Debate throughout high school. Hana truly loves the MUN program at UCI because it allows her to improve upon skills such as public speaking and diplomacy while also providing her a family at UCI. Outside of her studies and MUN, Hana enjoys playing music, cooking, and playing basketball.

Angie is a 3rd year Sociology and Political Science double major. She has been involved in MUN since freshman year of high school, and loved her experiences there so much she wanted to continue it onto college. She served as Secretary-General of her high school MUN club in her senior year and as a part of UCIMUN, has been an Assistant Director and a Director for General Assembly, and Under-Secretary-General of Mains. When not busy with her school, UCIMUN and work, she likes drawing, playing video games and doting on her pet fish.

This year, we really hope for you all to take to heart the paramount nature of coming up with solutions to the topics we have chosen. Our theme this year, "*addressing global human security and its impacts",* was carefully selected because we would like to emphasize the number and severity of global issues which affect everyday people. With your research and your resolutions, we would like you all to delve into ways to benefit as many people as possible, because global issues go beyond nations and governments—they affect all of us.

Our staff's goal, as always, is to provide delegates with high quality debate and an opportunity to immerse themselves in an intellectual discussion of issues that are relevant to the community around them. Please feel free to reach out to us, our USGs, or our Directors anytime between now and our conference. We are here to help you in any way we can.
Thank you for your time, and we look forward to seeing you in the Spring!

Sincerely,
Hana Schlosser and Angie Lo
Secretaries-General
UCIMUN Secretariat 2019-20
ucimunsg@gmail.com

Greetings Delegates,

A very warm welcome to the 28th Annual UCI Model United Nations High School Conference! My name is Ashima Seth, and I am looking forward to serving as your Under-Secretary-General for Specialized Agencies. Like you, I have been an active participant in the MUN tradition since high school, with this conference marking eight years of experience attending and organizing conferences. The time spent with my fellow delegation members, delegates and dais members has helped me forge lasting bonds and gain invaluable experience and skills. It gives me great pleasure to have the opportunity to be a part of your MUN experience and to, hopefully, make it as rewarding as my own has been.

For the last year, I have been working tirelessly with your Secretaries-General, Hana Schlosser and Angie Lo, and the Under-Secretary-General of Mains Committees, Kyle Petersen, in addition to the Directors, Assistant-Directors, and Administrative staff in researching, organizing and preparing all the material you will be seeing in the coming two days of the conference. The theme of this year's conference is "Addressing Global Human Security and its Impacts". I hope to see this theme reflected in the debate as delegates come together in crafting solutions to the topics being discussed in their respective committees. Our committee topics for this year aim to challenge you and your fellow delegates' problem-resolution skills in areas that have either been a source of dissension in international politics in the past or present (Security Council and Concert of Europe, respectively), that have impacted those who are more vulnerable (the United Nations High Commissioner for Refugees and the United Nations Entity for Gender Equality and the Empowerment of Women), and that have become increasingly worrisome due to their critical nature (United Nations Office on Drugs and Crime).

MUN affords a unique format of debate that not only helps you develop and showcase your skills in research and public speaking but which also facilitates a dialogue that unites us all in the quest to find effective solutions. To me, a successful committee is comprised of delegates who are well-versed in the subject matter, who have opinions on the said matter, and who voice these opinions in a diplomatic manner, engaging in teamwork to come up with solutions that are in the best interests of everyone involved. I strongly believe that all of you will more than rise to the challenge. I eagerly anticipate seeing you all during the conference and hope that it will be a pleasant and enriching experience for you!

Sincerely,
Ashima Seth
Under-Secretary-General of Specialized Agencies
UCIMUN Secretariat 2019-20
usgspecials@gmail.com

Hello Delegates,

My name is Lindsay Neighbors and I will be your Co-Director for the United Nations Office on Drugs and Crime. This is my third year in UCIMUN, having been a member of Crisis Staff for the previous two. My high school did not have a MUN program, which leads me to feel especially grateful to be able to participate in the UCIMUN's Annual Conference. As a member of the Crisis Staff, I worked to make the conference experience more interesting for all delegates. I found that working in a position that allowed me to read committee directives was one of the primary reasons I enjoyed being a part of the Crisis Staff, since they served to show me the dedication and energy put into the conference by all the delegates. I hope to see that same passion in this year's conference!

I am a double major in International Studies and Political Science, and am also pursuing a minor in Philosophy. My involvement in MUN stems from my two majors, which I chose due to my avid interest in post-colonial studies, with a focus on Latin America and international law. As such, the MUN program is very important to me because it aligns well with my studies, and also matches up well with other programs that I am involved in on campus; one of these being focused on teaching middle schoolers basic topics in international relations, such as human rights and trade. Thus, my college career is focused on not only expanding my own knowledge, but also trying to help others in that same endeavor.

The topic for this year's UNODC committee is Cybercrime and the Dark Web. The reason why we chose this topic is that it has become increasingly important in the modern age as technology continues to spread to every corner of the globe. As such, cyberspace has provided the perfect breeding ground for a new kind of crime group, one that does not function within recognized state borders and is thus able to have far-reaching consequences for the entire international community. When we look to the theme of this year's conference, *"addressing global human security and its impacts"*, the connection to cybercrime and the dark web is clear--states have to work together to address the issue, as crimes in cyberspace can have perpetrators and victims on two different continents. Therefore, addressing cybercrime not only helps to prevent a wide range of individual crimes, but also helps countries come together to strengthen our global community.

As a reminder, this topic synopsis serves as an overview of the committee's agenda, and should not be the end of your research into this issue. I and my fellow Co-Director would like to encourage you to continue your research into this topic so that you can bring your own unique viewpoint to the debate.

Lastly, I would just like to say how excited I am to be your Co-Director this year. I am sincerely looking forward to meeting and working with you all, and to making this experience the best that I possibly can. As a reminder, you should receive a receipt of your submission soon after submitting your position paper. Please do not hesitate to send me an email if you have any questions or concerns. Good luck with your research, and I'll see you at the conference!

Sincerely,
Lindsay Neighbors
Director
United Nations Office on Drugs and Crime
ucimunodc@gmail.com

Hello Delegates

My name is Hari Ajith and I will be your Co-Director for the United Nations Office on Drugs and Crime. I'm very excited to be co-directing this committee, seeing that we have a particularly intriguing topic to discuss and debate. This will be my second year as part of UCIMUN, and my sixth year participating in Model United Nations overall. Having been a part of Model United Nations for quite some time now, I know what it's like to experience committee as a delegate and how fun and interesting it can be. As such, I am looking forward to ensuring that you have the best possible experience at UCIMUN.

I am double majoring in Business Administration and International Studies. International relations has fascinated me since a young age, and I have been actively participating in Model United Nations since the beginning of high school. To me, in a world of rapid globalization, awareness of global affairs is not only important, but essential to successfully navigating the changing world. During my free time, I enjoy traveling to new countries, skydiving, learning new languages, and learning more about the world. I look forward to continuing my MUN journey as one of the Co-Directors for UNODC this year.

The topic for this year's UNODC committee is Cybercrime and the Dark Web. With the rapid advancement of technology and its integration into nearly aspect of the modern world, cybercrime has become a vitally important issue for the UNODC to tackle. The issue of cybercrime and its extensive geopolitical repercussions represents not only a threat to the safety of citizens around the world, but also a threat to the social coexistence, economic development, and political stability of the international community. As technology develops, so to must the international community's response to these developing threats.

As a reminder, this topic synopsis serves as an overview of the committee's topic, and should not be the end of your research into this issue. In this committee, delegates are expected to engage in professional discourse about the issues at hand as well as utilize credible external resources to substantiate your position papers and solutions. We are looking for well-thought out, expansive, and innovative solutions to the topic, while also maintaining integrity to your country's foreign policy. Adherence to country values and policy is integral to UNODC topics.

Overall, I hope that everyone has fun and can engage in meaningful discourse. I can always be reached by email if you have any questions. I'm looking forward to meeting and working with you all, and ensuring that you have the best possible experience in committee!

Best regards,

Hari Ajith
Director
United Nations Office on Drugs and Crime
ucimunodc@gmail.com

Topic A: Cybercrime and the Dark Web

Introduction

The United Nations Office on Drugs and Crime (UNODC) has worked to address cybercrime in the past years through multilateral programs, largely focused on education, and through the creation of a Cybercrime Repository database. The Global Programme on Cybercrime (GPC) focuses on technical assistance in various methods of cybercrime prevention and response, and works under the UNODC Organized Crime Branch. A subsidiary of the GPC is the Cybercrime Repository, which is a database for participating countries to share cybercrime legislation and strategy in the interest of transparency and coordination. The UNODC has also formed an Open-Ended Intergovernmental Expert Group Meeting, which is meant to function as a review board for larger, comprehensive draft studies on cybercrime responses.

All of these efforts are based on criminal activity conducted using the internet, which, at its base, is a networking infrastructure through which all computers connected to the system can communicate. A large portion of internet traffic, but not all, comes from the World Wide Web (WWW), an information-sharing model that uses the medium of the internet. The parts of the internet that most concern the UNODC are the deep web and dark web. The deep web is a part of the WWW that is not accessible through normal means, and is instead hidden from view. It is estimated that the deep web is around five hundred-fold bigger than the WWW that one can access through normal search engines. The dark web is a portion of the deep web that has been intentionally hidden, and is only accessible through specialized, anonymous browsing systems that are encrypted, such as Tor or I2P (Chertoff 2015).

The major cases that prompted action on the part of the UN include international espionage, human trafficking, drug trafficking, financial fraud, identity theft, and cyberterrorism. Most notably, it is cases such as the cyberattacks on Estonia and Georgia in the late 2000s along with the Stuxnet virus used against Iran in 2010, that have inspired UN involvement in the world of cybercrime. In the cases of Estonia and Georgia, distributed denial of service (DDoS) attacks were conducted to restrict the flow of information between the government and the people. Specifically, hackers allegedly working for Russia conducted DDoS attacks that shut down civilian access to the internet in its entirety in Estonia, and further DDoS attacks were conducted on government websites that coincided with increased ground troop movements and conflict with the Russian Federation (McGuiness 2017). Stuxnet was a virus allegedly created by the United States and Israel that destroyed approximately 1000 nuclear centrifuges and infected over 60,000 computers working on the Iranian nuclear program (Britannica).

Both of these examples show how countries can use cybercrime as a way to undermine other governments and push their own advantages on an international scale. However, the impacts of cybercrime are also felt on a smaller scale, whether it be ransomware, phishing, data alteration in hospitals or official government sites, and malware that is almost impossible to properly respond to as it has been integrated with AIs. In all these cases, what becomes clear is that cybercrime is increasingly difficult to respond to without the help of other countries. Whether it be a case of ransomware or international sabotage, the culprits behind cyberattacks are notoriously hard to find as cyberattacks will often occur across national borders. Thus, when preparing to properly address this topic, one must look to maintaining cooperation and transparency, which are the themes that the previously mentioned UNODC programs depend on.

Description

Human Trafficking

The UNODC defines human trafficking as: “the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs." (UNODC). While human trafficking is a multi-billion dollar industry with victims across the globe, a common thread that can often be found between individual cases is the use of the internet for advertisement, organization, and payment. While human trafficking does occur on the dark web, it also occurs on non-encrypted, easily acceptable sites.

A study done by the University of Portsmouth gathered data on the number of hidden Tor services available online, and found that while only 2% of traffic was dedicated to sites linked to child abuse, 83% of the visits to hidden service sites were to sites linked to child abuse (Finklea 2017). Therefore, while the number of websites advertising the trafficking of minors is limited, most of the actual web traffic to dark web sites are to those few sites that do contain information regarding this trafficking. A further study done by the NGO Thorn surveyed victims of human trafficking and found that 63% of respondents reported being sold online. Many victims of human trafficking are advertised online, often using false identities and photos to hide age

exploitation (Rhodes 2016). Thus, the internet is used heavily when it comes to identifying, kidnapping, transporting, and advertising the victims of human trafficking.

A recently published survey shows that a majority of the general public recognizes that human trafficking is an issue in their country, and that human trafficking utilizes the internet for different purposes (Mendel and Sharapov 2014). Governments have also begun to recognize this link, and organizations such as Interpol, Europol, and the European Cybercrime Center have recognized cybercrimes in regards to human trafficking as both “borderless” and as having striking “scalability.” (Mendel and Sharapov 2014). It is with this basic idea that the UN itself has attempted to address human trafficking, as the focus of much of the UN’s efforts are geared towards created a basis of knowledge so that countries can coordinate their efforts to address the issue. Most UNODC efforts are geared towards creating standards for data collection and facilitating inter-institutional cooperation. The UN also looks to non-governmental organizations and other UN agencies to aid countries in their efforts, and works to establish relationships between these organizations and individual countries as a method of response. Therefore, the UN approach to human trafficking as a branch of cybercrime looks to coordination and cooperation in their efforts to address human trafficking.

Cyberwarfare and Cyberterrorism

According to the United States Federal Bureau of Investigation, cyberterrorism is any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents" (FBI Cybercrime). Nation-states have increasingly been engaging in long-term cyberattacks and other such offensive cyber operations in order to support their

strategic and geopolitical policy initiatives. A large number of countries have increased their technological capabilities so as to conduct cyberattacks, including military-style, destructive cyber attacks. According to 2018 intelligence reports from the US Intelligence Community, there are currently more than thirty nation-states with the capability to conduct a military-grade destructive cyber attack. According to Siemens AG, a German multinational conglomerate that provides services to industries and governments globally, "Where past attacks primarily targeted data theft, current and future attacks can hijack control systems and logic controllers that operate critical infrastructure with the intent to cause physical damage and outages" (Siemens Cybersecurity). This type of cyberattack could cause major public health crises, endanger the safety of millions of individuals, as well as cause mass panic and fatalities.

One of the most prime examples of the chilling destructive effects that cyberterrorism can have upon a state is the example of the June 2017 Notpetya attack on Ukraine (WIRED). According to classified reports cited by US intelligence officials, the Russian GRU military spy agency was responsible for the creation of Notpetya, in an effort to disrupt Ukraine's financial system. The cyberattack resulted in over $10 billion in damages (Washington Post). The WannaCry ransomware cryptoworm released by North Korean hackers in May 2017, is estimated to have cost between $4 billion and $8 billion in damages as it wreaked havoc across the National Hospital Service in the United Kingdom. According to former Homeland Security Advisor, Tom Bossert, "While there was no loss of life, it was the equivalent of using a nuclear bomb to achieve a small tactical victory," (Washington Post)

While cyberattacks tend to lack the obvious physical devastation and damage as traditional firearms and military attacks, they can be the source of immense internal havoc, and

as such raise a new set of problems. Their effects tend to be economic and political in nature rather than lethal. As such, state actors in the modern world struggle to find appropriate non-violent responses to such acts. In 2018, the UN called for global rules to minimize the damage of cyberattacks in the wake of several attacks from state-sponsored groups on multinational firms, ports, and public services (Khalip 2018). In the case of cyberwarfare, what has become of particular interest is the debate over whether the Geneva Convention or international humanitarian law applies to these attacks. Fear of misuse has thus led the UN to push for rules that would ensure a "more humane character" of cyberwarfare, and more generally to ensure that the internet remains "in the service of good" (Khalip 2018). Therefore, the interest of the international community is currently focused on creating an evolving framework that allows for an environment better suited for maintaining stability and accountability in cyberspace.

Illicit Firearm and Explosive Trafficking on the Dark Web

One of the most rapidly growing dangerous and damaging activities conducted on the Dark Web is the illegal trafficking of firearms and explosives around the world. Every year, illegal trafficking in small arms and light weapons is estimated to be worth $1.7 to $3.5 billion, equivalent to around 10 to 20 percent of the legal arms trade (Forbes).

Despite efforts to regulate and limit illegal firearm trafficking, the Dark Web has provided multiple avenues for technologically-savvy criminals to circumvent controls and transport weapons across international borders. Through the Dark Web, criminals and terrorist groups are able to access a worldwide market where it's possible to procure or sell a wide range of weapons and associated products through encrypted marketplaces and vendor shops.

Moreover, due to the anonymity it provides, the darknet is presenting a new and extremely difficult challenge for governments and law enforcement agencies across the globe.

Research conducted by RAND indicates that while the United States accounts for nearly 60% of firearm listings on the darknet, Europe as a whole serves as the largest international market for illicit firearms. Europe's darknet market for firearms generates nearly five times the revenue of the United States (RAND). Weapons traffickers in the Middle East and Africa have established regional firearm and explosive-focused marketplaces on the darknet, advertising weapons that range from simple handguns to anti-tank and anti-aircraft missiles (RAND). The Dark Web has increased the availability of more powerful and more dangerous weapons for purchase, with prices that are comparable, if not lower, than those that would be available on the street.

Of particular concern is the illicit proliferation of files for making weapons with 3D printers and other production technologies, such as computer numerically controlled (CNC) milling machines (Carnegie Endowment). While current evidence suggests that only a minor percentage of illegal firearms are currently made with these technologies, as technology rapidly develops and printers improve in quality and decrease in price, they pose a particularly dangerous concern for the international community (Carnegie Endowment). 3D printed weapons have become more and more available in the public sphere, and cases of their usage in terrorist attacks has increased due to their lethality and because they are hard to trace (Hoffman 2019).

Many high-profile shootings have been conducted using weapons purchased online, such as the Charlie Hebdo attacks in 2015 and the Munich shooting in 2016 (Hoffman 2019). The UN had previously created the Global Firearms Programme, which was created in order to foster

information sharing and cooperation in the interest of identifying and preventing cases of firearms trafficking. The program attempts to foster legislative and policy development, implement preventive and security measures, and strengthen criminal justice response. UNODC also mandates the collection of basic data for firearms, and is currently working towards (GFP). The Cybercrime Programme is working in conjunction with the Global Firearms Programme, in the capacity of gathering digital evidence and providing training for the tracking of cryptocurrencies frequently used in the purchase of firearms on the dark web (GFP).

Bloc Positions

North America:

The United States and Canada both have individual government sectors dedicated to cybercrime response, but prosecutions still remain low, with the majority of cybercrime cases remaining unsolved (McMillian 2019). The countries have fairly robust cybercrime laws that correspond with a similarly robust cyber-warfare and cybersecurity government divisions. The main concern for these countries in regards to international legislation is maintaining informational freedom while also curbing the negative economic and political impacts (Nakashima 2019).

South America

Many South American countries have had cybercrime legislation in effect since the early 2000s, but much of that legislation has not had necessary updates since the 2010s, thereby creating significant issues with prevention and prosecution (Glickhouse 2013). Cybercrime in the public and private sector cost Latin American countries over $90 billion in 2018 (Egusa 2018).

The most common type of attack is malware attacks, with 50% of Latin American businesses suffering malware attacks in 2013 (Clavel 2016).

Western Europe

Much of the European legislation on cybercrime focuses on the dissemination of information and training for government officials (Council of Europe). However, in some European countries, cybercrime still makes up around half of all crimes committed (Council of Europe). Western European countries broadly accept previous UN resolutions on cybercrime, and are some of the main participants in the Global Programme on Cybercrime (Council of Europe).

Eastern Europe

The region has large amounts of cybercriminal rings, with highly sophisticated fraud and extortion programs, and much of the cybercriminals in the region focus more on stealing financial information because it can be quickly monetized (Kshetri 2013 (1)). Further many of the attacks by Eastern European cybercriminals occur in other countries, mostly in North America and Western Europe, which makes accountability difficult (Wagner 2013). On the governmental level, there is a lack of sufficiently high penalties and generally weak legislation (Kshetri 2013 (1)).

Northern Africa

According to a 2017 report, four of the world's top 25 countries where computers are the most vulnerable to cyber-attacks are in the Northern Africa region (Enact Africa 2019). Northern African countries have generally weak IT infrastructures (Enact Africa 2019). Further, much of

the legislation that is currently in place is too broad in scope, and is defined in terms that allow for state control of information (Enact Africa 2019).

Sub-Saharan Africa

African countries have been increasingly targeted by cyber attacks, as cybercriminals often target emerging economies as their legislation against cybercrime is typically more lax; Sub-Saharan African countries are at a particular risk, because the number of individuals with mobile phone subscriptions and access to e-banking is expected to increase drastically (Kshetri 2019). A limited number of Sub-Saharan African countries have enacted information sharing institutions in the hope of expanding cybercrime legislation and response, while the majority of the region continues to have fairly weak and ineffective legislation (ISS 2019).

Central and Western Asia

The central and western Asiatic regions do not face as much threat domestically from cybercrime as opposed to central or eastern Europe, but nonetheless have been the subject of various high profile cyber-attacks, many of which are politically motivated (Kshetri 2013 (2)). Generally, the region has underdeveloped regulatory framework and enforcement mechanisms, which creates an environment that allows for large cyberattacks against various governments (Kshetri 2013 (2)). Therefore, the main concern for this region moving forward is national security, as harsher regulations have been passed across the region in recent years (Kshetri 2013 (2)).

Eastern and Southeastern Asia

Cybercrime attacks in eastern and southeastern Asia have increased dramatically since 2015 (Lin et al 2017). Due to the political, cultural, and economic diversity in this area, it has

been difficult for the countries in this region to create avenues for communication with regards to cybercrime, therefore limiting the ability of law enforcement to properly respond to cyber threats within their own countries (Lin et al 2017). Although many heads of states within the region have announced the intention of cross-border communication for the purpose of coordinating cybercrime responses and legislation, very little consistent action has been taken (Lin et al 2017). However, there have been some cases of cooperation in cybercrime cases, mainly with regards to attacks that have been politically motivated, and a few nations have undertaken cybercrime training programs launched by the UNODC (Lin et al 2017).

Southern Asia

Although some of the countries within Southern Asia have established cybersecurity divisions for their government, comprehensive legislation is lacking across the region (Tufail 2018). This is despite an increase in politically motivated attacks on government websites and programs, often perpetrated by other countries within the region, north America, or eastern Asia (Tufail 2018). The legislation within these countries that is currently enacted has a focus on preventing certain kinds of cyberattacks, such as ones that are politically motivated or attack businesses, and usually contain sections that allow for censorship in regards to politically motivated content and general surveillance (India Times 2015).

Committee Goals

For this committee, we hope to see a lot of negotiation and compromise. As the information this summary has provided suggests, much of the worldwide efforts towards stopping cybercrime of all kinds is in the sharing of information and technology. With this in mind, we hope to see countries working together to find solutions to common problems, and

using systems already established by the United Nations for this purpose either as inspiration, or as a starting point for something different. This brings us to the second thing we are looking for in this committee, which is creativity. The main reason criminals and countries have been able to gain such assets and power through cybercrime is because their approaches are increasingly creative and hard to predict. In order to properly address this issue, therefore, your solutions should be just as creative.

Research Questions

1. What are the most important pieces of legislation on cybercrime your country has passed individually, and what does that tell you about the most relevant cybercrime issues they are facing?
2. Are there other countries, in the same geographic area or otherwise, that are facing similar issues in the field of cybercrime? If so, what are those issues, and how could they benefit from a multilateral approach?
3. What are some relevant treaties that your country has entered, and how have they affected cybercrime rates? If your country has not entered into any cybercrime treaties, why do you think that is? How could they benefit or be disadvantaged by entering into cybercrime treaties?
4. How has cybercrime affected warfare between countries? On the other side, how has it also affected the formation of alliances between countries?
5. What is the extent of damage that a cyber attack can have on individual cities, such as in the case of utilities like the electricity grid or water sanitation plants? What does this

mean for the future of national defense systems, and how does that change the willingness of countries to work together?

References

Clavel, T. (2016, September 26). Can Latin American Governments Keep Up With Cyber Criminals? InSight Crime. Retrieved December 5, 2019, from https://www.insightcrime.org/news/analysis/can-latin-american-govt-keep-up-with-cybe-criminals/

Chertoff, M., & Simon, T. (2015). The impact of the dark web on internet governance and cyber security. *Global Commission on Internet Governance.* Retrieved October 29, 2019 from https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf

Council of Europe action against Cybercrime. (n.d.). Council of Europe. Retrieved November 26, 2019, from https://www.coe.int/en/web/portal/coe-action-against-cybercrime

Cyber attacks on India mostly from Pakistan, China: Government. (2015, August 7). India Times. Retrieved December 7, 2019, from https://economictimes.indiatimes.com/news/defence/cyber-attacks-on-india-mostly-from-pkistan-china-government/articleshow/48392113.cms

Egusa, C. (2018, July 31). Five Measures Latin America Must Take To Get Up To Snuff On Cybersecurity. Forbes. Retrieved November 26, 2019, from https://www.forbes.com/sites/forbesagencycouncil/2018/07/31/five-measures-latin-america-must-take-to-get-up-to-snuff-on-cybersecurity/

ENACTAfrica.org. (2019, April 24). North Africa should fight online crime the right way. ENACT Africa Retrieved December 5, 2019, from https://enactafrica.org/enact-observer/north-africa-should-fight-online-crime-the-right-way

Finklea, K. (2017, March 10). Dark Web. Congressional Research Service 7-5700. Retrieved October 30 from https://aquadoc.typepad.com/files/crs_dark_web_10march2017.pdf

Glickhouse, R. (2013, October 21). Explainer: Cybercrime in Latin America. Council of the Americas. Retrieved November 26, 2019, from https://www.as-coa.org/articles/explainer-cybercrime-latin-america

Global Firearms Programme (GFP). (n.d.) A Global Problem : Illicit Trafficking and Misuse of Firearms as a Threat to Global Security. United Nations Office on Drugs and Crime. Retrieved November 14, 2019, from https://www.unodc.org/unodc/en/firearms-protocol/index.html

Hoffman, B. & Ware, J. (2019 October 25). Is 3-D Printing the Future of Terrorism? - WSJ. Retrieved December 20, 2019, from https://www.wsj.com/articles/is-3-d-printing-the-future-of-terrorism-11572019769

ISSAfrica.org. (2019, June 26). Is Africa cybercrime-savvy? Institute for Security Studies. Retrieved December 5, 2019, from https://issafrica.org/iss-today/is-africa-cybercrime-savvy

Khalip, A. (2018 February 19), U.N. chief urges global rules for cyber warfare - Reuters. Retrieved November 12, 2019, from https://www.reuters.com/article/us-un-guterres-cyber/u-n-chief-urges-global-rules-for-cybe-warfare-idUSKCN1G31Q4

Kshetri, N. (1) (2013). Cybercrime and Cybersecurity in the Former Soviet Union and Central and Eastern Europe. In N. Kshetri (Ed.), *Cybercrime and Cybersecurity in the Global*

South (pp. 51–76). London: Palgrave Macmillan UK. https://doi.org/10.1057/9781137021946_3

Kshetri, N. (2) (2013). Cybercrime and Cybersecurity in the Middle East and North African Economies. In N. Kshetri (Ed.), Cybercrime and Cybersecurity in the Global South (pp. 119–134). London: Palgrave Macmillan UK. https://doi.org/10.1057/9781137021946_6

Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. Journal of Global Information Technology Management, 22(2), 77–81. https://doi.org/10.1080/1097198X.2019.1603527

Lin, L. S. F., & Nomikos, J. (2017). Cybercrime in East and Southeast Asia: The Case of Taiwan. In A. J. Masys & L. S. F. Lin (Eds.), Asia-Pacific Security Challenges: Managing Black Swans and Persistent Threats (pp. 65–84). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-61729-9_4

McGuinness, D. (2017, April 27). How a cyber attack transformed Estonia. *BBC News*. Retrieved from https://www.bbc.com/news/39655415

McMillian, E. (2019, July 25). Cybercrime is going up across Canada and most cases remain unsolved | CBC News. Retrieved November 26, 2019, from https://www.cbc.ca/news/canada/nova-scotia/cyber-crime-rising-across-canada-1.522130

Mendel, J., & Sharapov, K. (2014). Human trafficking and online networks. *policy briefing. CEU Center for Policy Studies*. Retrieved October 30, 2019 from https://discovery.dundee.ac.uk/ws/files/7689615/Trafficking_paper_final_deanonymised_fr_Antipode.pdf

Nakashima, E. (2019, November 16). The U.S. is urging a no vote on a Russian-led U.N. resolution calling for a global cybercrime treaty. Washington Post. Retrieved November 26, 2019, from https://www.washingtonpost.com/national-security/the-us-is-urging-a-no-vote-on-a-russianled-un-resolution-calling-for-a-global-cybercrime-treaty/2019/11/16/b4895e76-075e-11e-18c-fcc65139e8c2_story.html

Rhodes, L. M. (2016). Human Trafficking as Cybercrime. *Agora International Journal of Administration Sciences*, *1*(1), 23-29. Retrieved October 30, 2019 from http://univagora.ro/jour/index.php/aijas/article/download/2992/1138

Stuxnet | computer worm | Britannica. (n.d.). Retrieved October 29, 2019, from https://www.britannica.com/technology/Stuxnet

Tufail, T. (2018, January 5). Comparing the National Security Framework of Pakistan and India with the United Kingdom. Tallinn University of Technology. Retrieved November 26, 2019 from https://digi.lib.ttu.ee/i/file.php?DLID=10767&t=1

Wagner, D. (2013, January 23). Inside the Eastern European Cybercrime Network That Brought Down NASA - The Atlantic. Retrieved December 5, 2019, from https://www.theatlantic.com/technology/archive/2013/01/inside-eastern-european-cybercrme-network-brought-down-nasa/319150/

What is Human Trafficking. (n.d.) United Nations Office on Drugs and Crime. Retrieved October 31, 2019 from https://www.unodc.org/unodc/en/human-trafficking/what-is-human-trafficking.html