Forum: Economic and Social Council

Issue: Addressing the role of the internet in international crime

Student Officer: Seung Yon Kim

Position: Chair of Economic and Social Council

Introduction

With over 4 billion internet users in our current world, the internet is becoming a more and more popular platform worldwide. There are a little less than 2 billion websites today and around 100,000 websites are hacked every day. Research from McAfee shows that two-thirds of the people online have had their personal information stolen or compromised.

Examples of international cybercrime include online organ trade, which is advertised on the internet and may risk people's lives, state sponsorship of international cybercrime in countries such as North Korea and Russia, and arms trafficking. Additionally, international crimes such as terrorism can also be impacted by the use of the internet. A growing number of terrorists are starting to use the internet as their platform to recruit members and threaten others.

Domestic and international law enforcement regarding international cybercrimes in countries are less effective than they should, this leads to many criminals using the internet to take advantage of the less serious punishments and difficulties of being traced. The difficulty and complexity of the different cybercrimes makes it harder for governments to fight back against the issue at hand. However, countries are starting to realise the threats the internet and cybercrime pose to them and are beginning to work together to enforce stronger laws.

Definition of Key Terms

Cybercrime

This refers to the illegal internet-mediated activities that take place on global internet platforms.

Organ Trade

This is the trade of human organs, tissues or other body parts, usually for transplantation. Trade in human organs is illegal in all countries except for Iran, which therefore leads to the growth of various online organ black markets.

State Sponsorship

This refers to the government support of a type of action. For example, 'state sponsorship of international cybercrime' would refer to the government's support of international cybercrime.

Transplant Tourism

Transplant tourism is when the recipient of the organ travels abroad to purchase the organ and receive the transplant. This is the most common way in which organs are traded across national borders.

Arms Trafficking

It refers to the trafficking of contraband weapons and ammunitions.

Phishing

It refers to sending emails or calling people pretending to be from reputable companies in order to get those people to reveal their personal information such as passwords.

Dark Web

It refers to websites that exist on an encrypted network and cannot be found by using a traditional search engine or visited by using traditional browsers.

General Overview

International organ trade

The trading of human organs is illegal in all the countries except for Iran. There are around 100,000 people on the kidney transplant waiting list alone, and the waiting list has doubled in size over the past decade. In addition, people wait 5 to 10 years to receive a kidney transplant from a deceased donor and 13 people die every day whilst waiting for a kidney transplant. With so many people in desperate need of organ transplants, many have turned to the illegal organ black market to save their lives. International organ trade comes in various forms, such as transplant tourism. The internet is being used to trade organs online and to attract patients from all over the world.

Transplant tourism

Nowadays, the internet is often being used to attract foreign patients for transplant tourism. There are quite a few websites online which offer not only one organ but also ‘full packages’ of transplant organs.

Main routes of the organ trade

Transplant tourism risks the lives of the recipients. Research from China’s department of health shows that out of the 118 patients who received organ transplants from transplant tourism, only 69

transplantations were performed by doctors.

South Africa

In South Africa, less than 2% of the country's population is on the organ donor list, meaning that many people are desperate for organs. With advertisements plastered all over the internet, those who are in need for money sign themselves up to become an organ donor. These people will then receive a medical exam from unqualified doctors. They will then obtain passports and airplane tickets to travel to South Africa, where they will donate their organs. At the same time, the recipient will travel to South Africa. The recipient and donor would then meet at a hospital, where they exchange their organs. Using this method, in which both the recipient and donor travel to a third country, there have been over 100 illegal kidney transplants that were performed in St. Augustine's Hospital, South Africa, between the years 2001 and 2002. In addition, there have been over 220 illegal transplants that have took place across the hospitals Charlotte Maxeke and Garden City Hospitals in Johannesburg, and Christian Barnard Memorial Hospital in Cape Town.

State sponsorship of international cybercrime

Criminals of cybercrimes are becoming more and more sophisticated, and now with the use of bitcoins, it is very hard to catch these criminals. Some cybercriminals may be able to make millions of US dollars without getting caught at all. Some cybercriminals are supported by the government, meaning that the criminals are backed by government resources, therefore the crimes can be very dangerous. Below are a few examples of major cybercrimes that have happened around the world.

North Korea

North Korea is one of the two 'cybercrime centres' alongside Russia. Most of the time, the cybercriminals in North Korea are state sponsored, due to the fact that the criminals have government support, this protects them from investigation and punishment. In North Korea, these hackers and criminals mostly work for the General Bureau of Reconnaissance or the General Staff Department of the Korean People's Army.

In 2016, cybercriminals in North Korea nearly stole $951 million from the Bangladesh Central Bank and North Korea has been accused of hacking emails at Sony Pictures in 2014. Furthermore, they have also been accused of attempting to break into Lockheed Martin, the American defence contractor that built an anti-missile defence system which is currently deployed in South Korea.

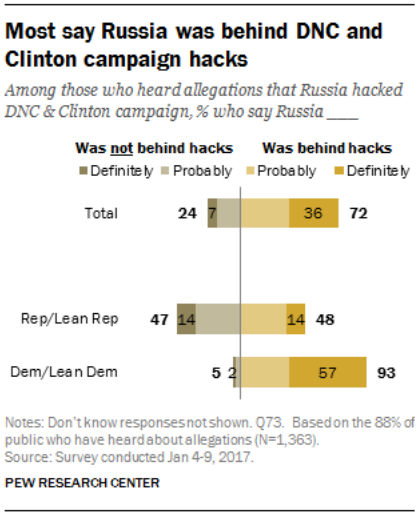
Russia

With many Russian university departments in maths, engineering, and computer science that have been ranked as one of the world's best for decades, Russia has many citizens with highly developed technical skills. This is all due to the literacy campaigns in 1917, which boosted the literacy rate of 22% to full literacy by the time the Soviet Union collapsed. As the 21st century rolled in, several hundreds of Russians began to participate in the many Russian hacking competitions. In 2014, the Russian cybersecurity company, Group-IB, estimated that the size of the Russian cybercrime market was $2.3 billion.

Moscow's military intelligence has been accused by other European governments for attempting to hack into the world's chemical watchdog and several other European institutions.

2016 U.S. Presidential Election Campaign

In September 2015, the Federal Bureau of Investigation (FBI) contacted the Democratic National Committee's (DNC) help desk, they warned the IT department that at least one computer was compromised by Russian hackers. During November of the same year, the FBI contacted the DNC once again, claiming that one of their computers were transmitting information back to Russia.



Survey on the U.S. Presidential Campaign

On March 19, 2016, chairman of the Clinton campaign, John Podesta, received a phishing email masked as an alert from Google, the email alerted him saying that someone had tried to access to account. Podesta then shared the email with a staff member from the help desk. The staff member was supposed to reply with 'This is an illegitimate email' but accidentally sent 'This is a legitimate email', causing Podesta to change his password using the link that was sent to him by the phisher, this allowed the hackers to access his emails.

In June 2016, WikiLeaks announced that they had managed to obtain Clinton's emails and would publish them for the public to see. Nearly 20,000 emails hacked from the DNC server is published by WikiLeaks on the 22nd of July 2016. The FBI then conducted an investigation as to who hacked the DNC server, the US officials then told CNN that the cyberattack is linked to Russia.

During the October of 2016, DCLeaks, a group of hackers seeking to expose officials, published a batch of stolen documents from Hillary Clinton's ally, Capricia Marshall. DCLeaks was later revealed to be a front for the Russian military intelligence.

The Central Intelligence Agency (CIA) reportedly determined that the Russian hacking was done to boost Donald Trump and hurt Hillary Clinton during the presidential campaign, according to the Washington Post in December 2016. Former president, Barack Obama, requests the United States intelligence agencies to look at the hacking incidents in 2016 and incidents on the presidential campaign that go back to 2008. Meanwhile, a Russian foreign minister shows scepticism on the review and asked the intelligence agencies for their evidence of state sponsored cyber-attacks.

In June 2017, Russian president, Vladimir Putin, stated that the hacking during the presidential election campaign may have been conducted by patriotic Russians, who felt threatened by the perceived slights against Russia from the United States. Additionally, during the same month, a Department of Homeland Security official stated that hackers linked to the Russian government targeted voting systems in around 21 states.

Though it is still unclear whether or not the Russian government rigged the U.S. presidential election, this situation shows the damaging and lethal threats state sponsored cybercrimes pose to other governments.

Dark Web

The United States Justice Department arrested Ross Ulbricht, the founder of a large online black market on the dark web, the 'Silk Road'. The Silk Road, where drugs and other illicit items were traded, was the 'most sophisticated and extensive criminal marketplace on the Internet'.

Arms trafficking

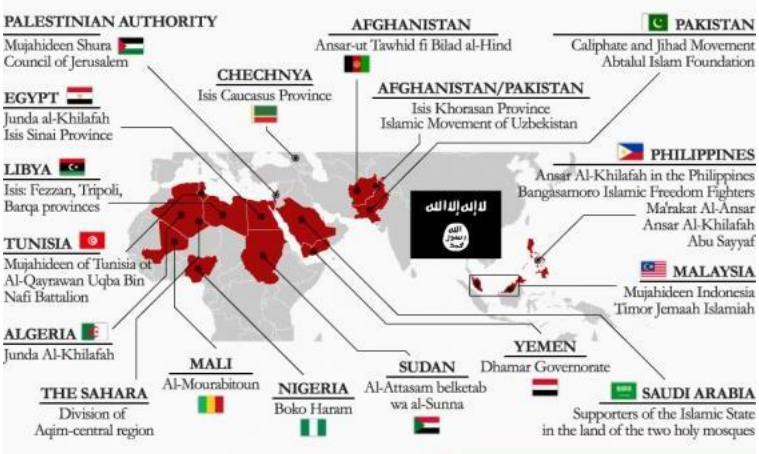
The internet plays a large role in the trafficking of weapons. People may reach out towards potential clients on social media, and they may also obtain weapons and ammunition from online sellers. Technological advancements, for example 3D printing, can cause the trade of arms to be entirely online, however, due to the fact that weapons are physical items, very few cases of arms trafficking happen completely online.

According to a survey, traffickers in the United States have shipped hundreds of weapons to consumers they met through social media. In addition, traffickers in the Middle East and Africa have set up regional arms trafficking markets on social media too.

Online arms trafficking makes it very difficult to catch the traffickers as the internet allows them to minimise their footprint. Furthermore, most traffickers use online payment services and cryptocurrencies, such as Bitcoins, making it even harder for officials to trace back and catch the trafficker.

Terrorism

Terrorist groups have started to promote their organisations by using their internet as their platform to promote their ideas and recruit members. The Islamic State of Iraq and the Levant (ISIL) is one of the examples of terrorist groups that use the internet to promote their ideologies. With such terrorist groups becoming larger and larger, it is important to lessen the number of people that are getting recruited through the internet.



Militant Groups That Have Pledged Allegiance to ISIL

ISIL

ISIL is well-known for their use of the internet to spread their ideologies and recruit members. They mostly use Twitter to spread its propaganda. Although Twitter shut down 125,000 accounts linked to ISIL in 2016, the social media influence ISIL has is still extremely strong. A defector of ISIL has said that those who work with the internet and media in ISIL have a much higher income than the soldiers.

UN Involvement, Relevant Resolutions, Treaties and Events

The United Nations office, United Nations Office on Drugs and Crime (UNODC), promotes long-term and sustainable capacity building in the fight against cybercrime by supporting national laws and actions. The UNODC uses its specialised expertise on criminal justice systems response to provide technical assistance during capacity building, prevention and awareness raising, international cooperation, and data collection, research and analysis on cybercrime. The UNODC has a global programme on cybercrime called 'The UNODC Global Programme on Cybercrime'. This programme is aimed to respond flexibly to the needs of developing countries to combat cybercrime. Furthermore, the UNODC has a protocol called The Protocol against Illicit Manufacturing of and Trafficking in Firearms, their parts and Components and Ammunition. This protocol was first signed by 52 parties and as of October 2018, it is signed by 116 parties. There have also been multiple resolutions on the issue of cybercrime.

Timeline of Events

Date	Description of event

1997	Formation of the United Nations Office on Drugs and Crime, formerly the Office for Drug Control and Crime Prevention.
July 11th, 2001	The Protocol against Illicit Manufacturing of and Trafficking in Firearms, their parts and Components and Ammunition, supplementing the United Nations Convention against Transnational Organised Crime signed, previously adopted by the United Nations General Assembly as Resolution 55/255.
December 21st, 2010	Resolution 65/230 adopted by the United Nations General Assembly.
January 1st, 2013	Resolution 22/7 adopted by the Commission on Crime Prevention and Criminal Justice.
May 15th, 2013	Resolution 22/8 adopted by the Commission on Crime Prevention and Criminal Justice.

Possible Solutions

One solution to organ trade could be **increasing the number of registered donors in a country**. Enhancing the number of donors will reduce the number of transplant tourism. The number of donors can be increased in ways such as regulating schemes that will reduce the disincentives of organ donation and ensure the safety of donors. Doing so will be able to ensure the people around them, which may start to increase the number of donors that are registered.

Member states should work together to tackle online arms trafficking by **gradually eliminating websites** on the dark web. Governments should ask for volunteers, who have experience in the field of technology, to get the community aware and involved tacking the issue at hand. Volunteers can then help the government take down websites on the dark web. It is important for the community to work together in situations like these, due to the fact that the dark web is fairly large and can pose as threats to many civilians. There can be incentives offered for the volunteers in case there are not enough volunteers.

Bibliography

"Global Cybercrime Shifts to State-Backed Hackers: Russian Group." *The Japan Times*, 10 Oct. 2018, www.japantimes.co.jp/news/2018/10/10/world/crime-legal-world/global-cybercrime-shifts-state-backed-hackers-russian-group/#.XBG6fRMzbBI.

"How Terrorists Use the Internet." *Operation250*, www.operation250.org/how-terrorists-use-the-internet/.

Jafar, T H. "Organ Trafficking: Global Solutions for a Global Problem." *Current Neurology and Neuroscience Reports.*, U.S. National Library of Medicine, Dec. 2009, www.ncbi.nlm.nih.gov/pubmed/19880230.

Lewis, James. "Economic Impact of Cybercrime – No Slowing Down" *McAfee*, McAfee, Feb. 2018, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf?kab1HywrewRzH17N9wuE24soo1IdhuHd.

Maurer, Tim. "Why the Russian Government Turns a Blind Eye to Cybercriminals." *Slate Magazine*, Slate, 2 Feb. 2018, www.slate.com/technology/2018/02/why-the-russian-government-turns-a-blind-eye-to-cybercriminals.html.

Rohter, Larry. "THE ORGAN TRADE: A Global Black Market; Tracking the Sale of a Kidney On a Path of Poverty and Hope." *The New York Times*, The New York Times, 23 May 2004, www.nytimes.com/2004/05/23/world/organ-trade-global-black-market-tracking-sale-kidney-path-poverty-hope.html.

Sevastopulo, Demetri. "Sevastopulo, Demetri. "US Accuses North Korea over Global Cyber Crime Wave." *Financial Times*, Financial Times, 6 Sept. 2018, www.ft.com/content/91453da8-b1de-11e8-99ca-68cf89602132.

Shimazono, Yosuke. "The State of the International Organ Trade: a Provisional Picture Based on Integration of Available Information." *World Health Organization*, World Health Organization, 4 Mar. 2011, www.who.int/bulletin/volumes/85/12/06-039370/en/.

Survey, Small Arms. "Beyond the Dark Web: Arms Trafficking in the Digital Age." *Medium.com*, Medium, 16 Feb. 2018, medium.com/@SmallArmsSurvey/beyond-the-dark-web-arms-trafficking-in-the-digital-age-56ddd806587a.

Swingler, Shaun. "The Dark World of Internet Kidney Trafficking." *Health24*, 25 Feb. 2015, www.health24.com/Medical/Kidney-and-bladder/News/The-dark-world-of-internet-kidney-trafficking-20150225.

Van Hooijdonk, Richard. "van Hooijdonk, Richard. "Cybercrime May Be the Biggest Global Threat of 2018." *Richard Van Hooijdonk*, 31 Oct. 2018, www.richardvanhooijdonk.com/en/blog/cybercrime-may-be-the-biggest-global-threat-of-2018/.

"United Nations Office on Drugs and Crime." *Integrity in the Criminal Justice System*, www.unodc.org/unodc/en/cybercrime/index.html.

"United Nations Office on Drugs and Crime." *Integrity in the Criminal Justice System*, www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html.

"United Nations Office on Drugs and Crime." *Integrity in the Criminal Justice System*, www.unodc.org/unodc/en/firearms-protocol/the-firearms-protocol.html.

"2016 Presidential Campaign Hacking Fast Facts." *CNN*, Cable News Network, 24 Nov. 2018, www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html.