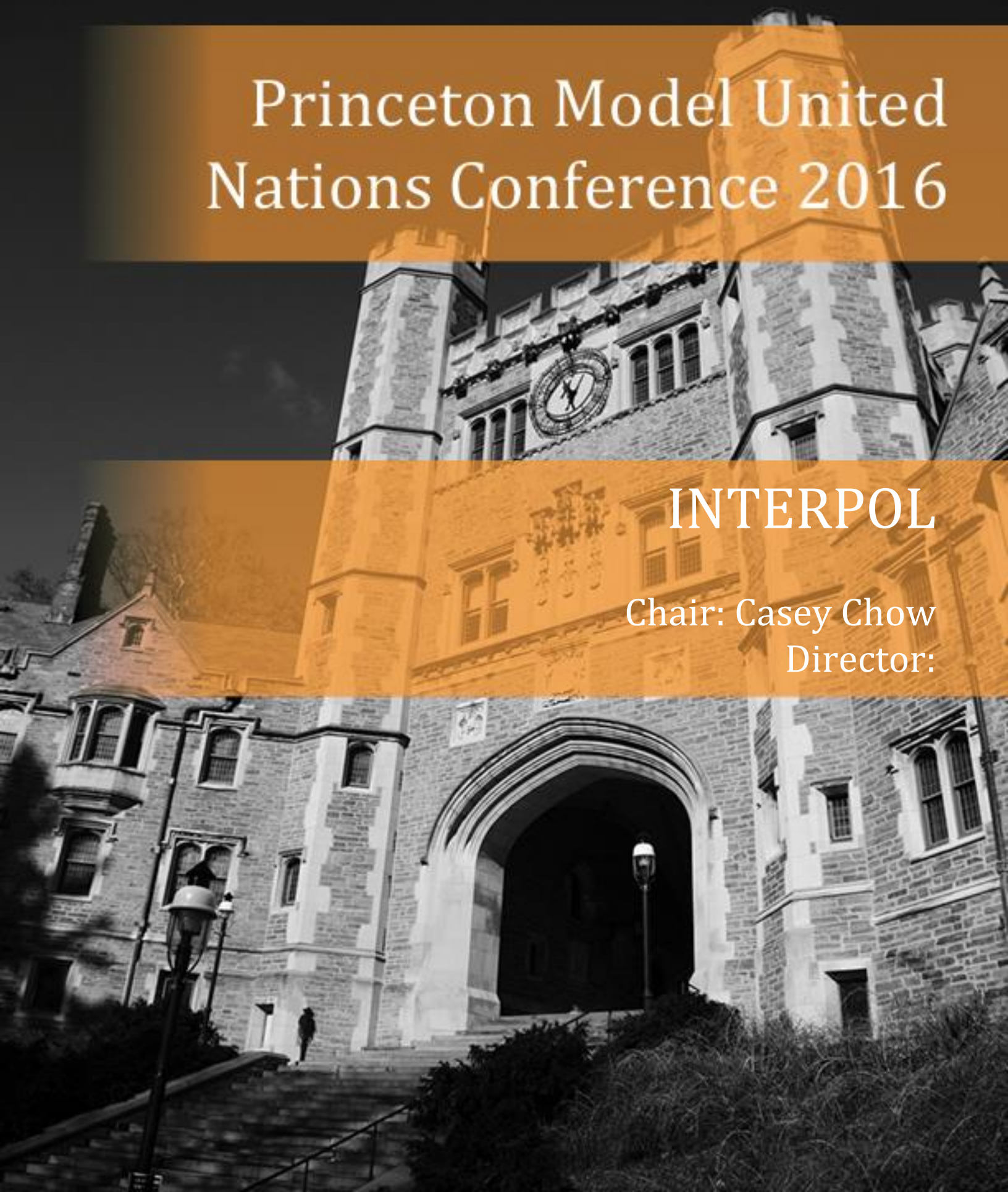
Princeton Model United Nations Conference 2016



INTERPOL

Chair: Casey Chow
Director:

Contents

Letter from the Chair

Dear Delegates,

Congratulations on the concern and care for international affairs that have brought you here today. My name is Casey Chow, and I have the distinct pleasure of chairing INTERPOL for PMUNC 2016. I am currently pursuing studies in Computer Science and pursuing certificates in Technology & Society and Statistics and Machine Learning. I've been involved with Model UN since my freshman year of high school, ultimately serving as a General Assembly Chair for Y-MUN in 2015, although sadly I had never attended PMUNC as a high school student. Last year, I served as Director for WHO, so I'm looking forward to see what incredible ideas a smaller committee will produce in comparison! Besides helping out with PMUNC, I serve on the board of Innovation Magazine, Princeton's Science Writing Journal, as well as a Director for Entrepreneurship Club and Vice President of an a cappella group on campus. I spent my time last summer studying Chinese in Beijing in a program called, fittingly, Princeton in Beijing. In my free time, I play a lot more Super Smash Bros than I really should, and occasionally go outside.

I look forward to serving you as your Chair for PMUNC 2016!

Best,

Casey Chow

Introduction

The original incarnation of INTERPOL, the International Criminal Police Commission, was first established in 1923 by the Vienna Police with the goal of facilitating cooperation among police forces, ultimately allowing for more effective prevention, investigation, and punishment of crimes across borders. However, the ICPC was effectively disbanded in 1938 due to Nazi control until the end of WWII, when the Belgian government spearheaded its revival, renaming the inter-police organization the International Criminal Police Organization, ICPO, or INTERPOL.[1]

The principles governing INTERPOL largely stem from a 1914 memorandum, known as the 12 Wishes, describing the goals of police cooperation. Among these wishes are, among other things, calls for the sharing of criminal profiles and forensic techniques, the centralization of such information, and greater facilitation of criminal extradition, all to "facilitate the action of criminal justice."[2] INTERPOL is governed by its General Assembly, composed of appointed delegates from all member nations, with one vote per nation.

Legally, INTERPOL is governed by its Constitution, and in turn, the General Assembly is authorized to perform the following actions, as per Articles 8 and 11:[3]

1. Determine principles for the Organization and/or member states to follow,
2. Make recommendations to the Organization and/or member states relating to law enforcement practices and policies,

[1] INTERPOL. "INTERPOL 1914-2014." INTERPOL. Accessed June 20, 2016. http://www.interpol.int/About-INTERPOL/History/1914-2014/INTERPOL-1914-2014/INTERPOL-1914-2014.

[2] 1st International Police Congress, Monaco. *Summary of the Wishes Expressed at the Sessions or Assemblies Held on 15, 16, and 18 April 1914*. PDF. INTERPOL.

[3] INTERPOL. "Constitution of the ICPO-INTERPOL." INTERPOL. Accessed June 20, 2016. http://www.interpol.int/About-INTERPOL/Legal-materials/The-Constitution.

3. Authorize and direct the actions of the Executive Committee (which, broadly speaking, oversees implementation of GA resolutions) and the General Secretariat (which oversee all other functions of INTERPOL),
4. Set INTERPOL's budget and direct related financial policies,
5. Authorize agreements between INTERPOL and other organizations,
6. Establish specialized subcommittees for specific topics, and
7. Sponsor regional conferences for matters of localized interest.

For the purposes of the Princeton Model United Nations Competition, all substantive decisions made by the General Assembly are by simple majority. It is of note that no political, military, or religious or racial actions may be taken by INTERPOL—for example, INTERPOL may not intervene in national politics.

INTERPOL agents are not police officers, and have no law enforcement jurisdiction in their own right. However, INTERPOL can organize a number of services to member nations, including:

1. Training of high ranking police officers in law enforcement best practices,[4]
2. National Central Bureaus, appointed by member nations to act as liaisons between domestic and foreign law enforcement efforts,
3. A set of law enforcement databases, including criminal profiles (fingerprints, photos, DNA samples, etc.), examples of counterfeit documents, and missing property records,[5]
4. Incident Response Teams (IRTs), which provide specialized assistance to broad emergencies and highly impactful crimes,[6] and

[4] [4] INTERPOL. "Training and capacity building." INTERPOL. Accessed June 20, 2016. http://www.interpol.int/INTERPOL-expertise/Training-and-capacity-building

[5] INTERPOL. "Databases." INTERPOL. Accessed June 20, 2016. http://www.interpol.int/INTERPOL-expertise/Databases.

5. Command and Coordination Centers (CCCs), accessible 24/7/365 by member nations, that assist in urgent law enforcement matters.[7]

Given the increasingly technical nature of INTERPOL's work, and key stipulations on its powers, a thorough understanding of INTERPOL's directives and jurisdiction is vital to developing viable means of addressing contemporary crime patterns.

[6] INTERPOL. "Response Teams." INTERPOL. Accessed June 20, 2016. http://www.interpol.int/INTERPOL-expertise/Response-teams.
[7] INTERPOL. "Command and Coordination Centres." INTERPOL. Accessed June 20, 2016. http://www.interpol.int/INTERPOL-expertise/Command-Coordination-Centre.

Topic A: Organized Crime

It would seem that the impressive development of modern society is necessarily accompanied by an equally cunning, and frighteningly prescient illicit underbelly. Organized crime, often defined as a highly connected, profit-driven network of individuals working to make money illegally, has only grown with the rising demands of a globalizing society.

However, the days of the Mafia and the highly-structured systems associated with traditional organized crime have given way to a new reality. The mobs, the cartels, the gangs all remain at large; but nowadays, one can no longer make the assumption that organized crime is hierarchical. The transnational element, as well as the streamlining of the supply chain has allowed markets to grow where monopolies once thrived, and as a result the concept of taking down a "crime boss" to keep organized crime off the streets no longer applies—nowadays, these organizations are informal, flexible, and are not dependent on a coordinating head to slither through society's shadows.[8]

The world is depending on its police to develop new means to prevent and prosecute the common enemy of mankind; the world's professional criminals cannot be allowed to continue developing new markets that harm lives, question the rule of law and create disorder where development should stand.

[8] Sacco, Vincent F. "Organized Crime." *Encyclopedia of Crime and Justice*. 2002. *Encyclopedia.com.* (September 4, 2016). http://www.encyclopedia.com/doc/1G2-3403000179.html

History

The origin of organized crime proves difficult to pinpoint, to say the least; for the purposes of this debate, organized crime in its modern form began around the end of World War I, with the rise of an international world order and governmental cooperation. The American Prohibition of the 1920s led to an unprecedented growth in the reach, power, and wealth of black market operators, especially the American Mafia; in that time, such groups grew increasingly talented in the illicit manufacture, smuggling, and distribution of alcohol throughout the country. These trust and power structures remained even as Prohibition ended in 1933; crime families simply switched to alternative revenue streams such as narcotics, loan-sharking, and racketeering in place of alcohol sales.[9] Indeed, the Mafia's policies of avoiding police interaction at all costs allowed them to stay under the radar of the FBI and other American authorities for nearly 30 years; it was only in the 1960s when the government began to acknowledge the existence of and investigate the operations of organized crime groups.[10]

Soon, similar developments began to occur in the backdrop of international development and evolving political systems. The disorder of the Chinese Civil War allowed for groups like the Triads to recruit members, which after the 1949 founding of the People's Republic of China and subsequent crackdown against organized crime, fled to non-PRC controlled localities such as Macao, Hong Kong, and Taiwan.[11] At the end of World War II, the Japanese Yakuza, which had existed since the 1700s but saw membership decline as the war effort swelled, began to remise recruiting efforts to widespread success among a nuclear war-torn nation. In the political turmoil after Josef Stalin's death, nearly 1.5 million criminals previously imprisoned in Gulags (about 60% of Gulag

[9] Ibid.
[10] History.com Staff. "Mafia in the United States." History.com. 2009. Accessed August 04, 2016. http://www.history.com/topics/mafia-in-the-united-states.
[11] Lo, T. Wing, and Sharon Ingrid Kwok. "Chinese Triad Society." Chinese Triad Society. January 13, 2014. Accessed August 28, 2016. http://www.oxfordbibliographies.com/view/document/obo-9780195396607/obo-9780195396607-0115.xml.

inhabitants) were released into the Soviet Union as an act of "amnesty,"[12] leading to a marked increase in crime throughout the Communist state and sowing the seeds of the Russian Mafia. Corruption began to soar throughout the '70s and '80s, "the result of an economy where the government could not provide people with the basic necessities, and the elite and loyal Communist Party members were lavishly rewarded."[13] In the Ural mountains, in fact, a career as a professional criminal proved extremely attractive, because "crime and its practitioners … were seen as less hypocritical, and in many ways more honest, than working with corrupt bureaucrats and officials."[14]

By the 1980s, globalization as a phenomenon had taken root, and organized crime groups, like virtually all major enterprises, rode along in establishing themselves among the growing interconnection and infrastructure. Drug trafficking began to take off despite, or perhaps because of Nixon's "War on Drugs," and Pablo Escobar's Medellín cartel began to sell considerable amounts of cocaine to European and American consumers.[15] After the collapse of the Soviet Union, organized crime soared in Eastern Europe; having lost work and State support, "hundreds of ex-KGB men and veterans of the Afghan war veterans [sic] offered their skills to the crime bosses."[16] The Russian Mob, now free to join the world economy and global community, began to expand into Europe and America to establish the lucrative global crime networks apparent today.[17] Consequently, targeting these enterprises was and remains most police forces' primary means of targeting organized crime.

After the turn of the millennium, however, organized crime began to evolve more quickly. As early as 2001, Europol noted that "traditional hierarchical structures are being replaced by loose

[12] Tikhonov, Aleksei. "The End of the Gulag." The Hoover Institute. Accessed August 2, 2016. http://www.hoover.org/sites/default/files/uploads/documents/0817939423_67.pdf.
[13] Pike, John. "Soviet Organized Crime." GlobalSecurity.org. February 25, 2016. Accessed September 01, 2016. http://www.globalsecurity.org/military/world/para/soviet-organized-crime.htm.
[14] Ibid.
[15] "Timeline: America's War on Drugs." NPR. April 2, 2007. Accessed August 12, 2016. http://www.npr.org/templates/story/story.php?storyId=9252490.
[16] "The Rise and Rise of the Russian Mafia." BBC News. November 21, 1998. Accessed September 1, 2016. http://news.bbc.co.uk/2/hi/special_report/1998/03/98/russian_mafia/70095.stm.
[17] Ibid.

networks of criminals,"[18] a trend that has only continued as increasing infrastructure decreases the economies of scale of criminal empires. As a result, taking down any individual organized crime ring has decreased in value, as the competitive market will easily adjust to that ring's absence. Enterprises lose the monopolistic power, and thus the overwhelming brand identity, they once had, and as a result return to the invisibility of the American mob in the early 20th century.

[18] United Nations. Office on Drugs and Crime. "The Globalization of Crime: A Transnational Organized Crime Threat Assessment." UNODC. 2010. Accessed August 25, 2016. https://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf.

Relevant International Law and UN Actions

United Nations Millennium Development Goal 1 (2000)

Sustainable Development Goal 16 (2015)

The Millennium Development Goals were originally established in 2000 to promote and target global development. Among them, MDG 1, the eradication of extreme poverty and hunger, applies to organized crime because of the devastating effects of the phenomenon on developing societies. Yury Fedotov, Executive Director of the UN Office on Drugs and Crime, noted that when "organized crime flourishes, successes in development are reversed, opportunities for social and economic advancement are lost."[19]

As a result, the Sustainable Development Goals, which were created at the close of the Millennium Development Goals' deadline, further recognizes organized crime as an inhibitor to social and economic development; the tagline for SDG 16 is to "promote just, peaceful and inclusive societies" and lists the following relevant targets:[20]

- By 2030, significantly reduce illicit financial and arms flows, strengthen the recovery and return of stolen assets and combat all forms of organized crime (16.4)
- End abuse, exploitation, trafficking and all forms of violence against and torture of children (16.2)
- Substantially reduce corruption and bribery in all their forms (16.5)

[19] "United Nations Office on Drugs and Crime." UNODC. April 23, 2012. Accessed August 12, 2016. https://www.unodc.org/unodc/en/press/releases/2012/April/transnational-crime-threatens-millennium-development-goals.html.

[20] United Nations. "Peace, Justice and Strong Institutions - United Nations Sustainable Development." UN. Accessed August 13, 2016. http://www.un.org/sustainabledevelopment/peace-justice/.

United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988)[21]

Primarily used to combat organized crime by combating one of its major revenue sources, the UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances provides for a wide range of standardized protocols in dealing with the drug trafficking industry, especially with regard to seizure, investigation and prosecution of drug traffickers. Notably, it requires all nations to allow police and judicial bodies to seize illegal substances. There are currently 189 countries party to the treaty.

United Nations Convention against Transnational Organized Crime (2000)[22]

The Palermo Protocols (2000/2001)

The UNTOC, also known as the Palermo Convention, serves as the primary international law against organized crime. There are currently 187 states party to the convention, an obligation that involves the creation of domestic laws that prohibit common organized criminal activity, such as money laundering and corruption, the establishment of extradition protocols, and upgrading domestic police forces to adequately handle organized crime.[23] The UNTOC is further empowered through The Palermo Protocols, three supplementary treaties that specify how a state must respond to human trafficking, migrant smuggling, and arms trafficking respectively. The Protocols provide complementary provisions on what laws a state must enact and how it must act in the international community with respect to such crimes.[24]

[21] United Nations. World Summit on the Information Society. "The Geneva Declaration of Principles and Plan of Action." UN. December 2013. Accessed August 23, 2016. https://www.itu.int/net/wsis/docs/promotional/brochure-dop-poa.pdf.

[22] "Convention on Cybercrime." Treaty Office. September 23, 2001. Accessed August 16, 2016. https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

[23] "Convention on Transnational Organized Crime." United Nations Office on Drugs and Crime. Accessed August 26, 2016. http://www.unodc.org/unodc/en/treaties/CTOC/index.html.

[24] Ibid.

Current Status

Despite technological and procedural advances, organized crime has become increasingly difficult to investigate and prosecute due to globalization. To avoid the suspicions of (non-corrupt) law enforcement, organized crime groups have developed into a wide array of organizational structures, no longer a simple hierarchy. Moreover, the densely interconnected supply chains and networks of these groups make them increasingly harder to dig out of the woodwork. Globalization has transformed the field of organized crime into a 2.1 trillion USD industry,[25] and the organizations that power this revenue are constantly searching for new ways to exploit others to make make even more money.

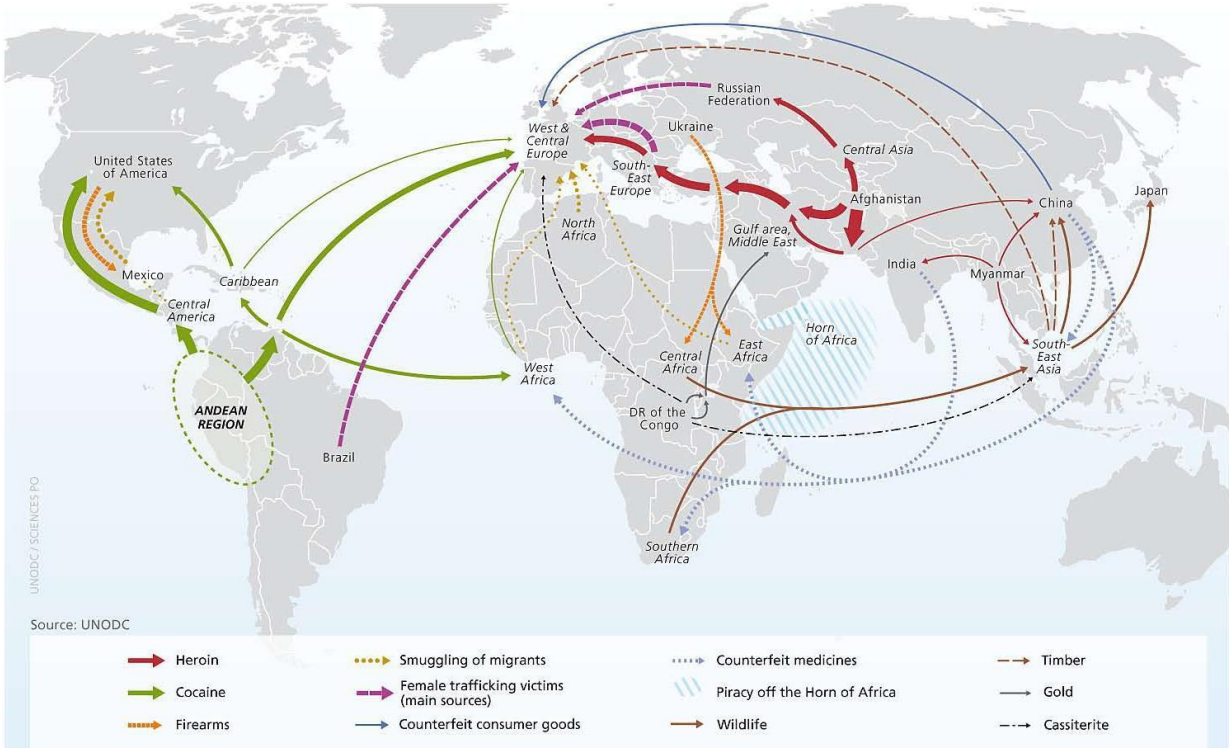


Figure 1 Global trade routes for illicit goods by industry, source UNODC.

[25] United Nations. Office on Drugs and Crime. "Illicit Money: How Much Is out There?" United Nations Office on Drugs and Crime. October 25, 2011. Accessed August 1, 2016. https://www.unodc.org/unodc/en/frontpage/2011/October/illicit-money_-how-much-is-out-there.html.

At the same time, international efforts to combat organized crime appear to be underfunded; the Council for Foreign Relations, a U.S.-based think tank, noted in 2013 that that the "UNODC is 91 percent funded by voluntary contributions and suffers from chronic funding shortages and understaffing. These resource constraints continue to limit the agency's effectiveness."[26] INTERPOL is under similar constraints.[27] As a result, the fight against organized crime rests primarily on limited coordination among individual nations' police and investigative forces rather than a centralized pool of international resources.

Key Issues

Trafficking of Drugs, Persons, Organs, and Firearms

The illegal drug trade remains one of the largest black markets in the world today, accounting for nearly 1% of total global trade. According to the 2011 UN World Drug Report, 315 million people aged 15-64, or roughly 7% of the global population, had used an illegal substance that year[28]. Due to the prevalence of these drugs, this $321 billion industry has an influence on nearly every UN nation. Plans to resolve drug trafficking are vital yet difficult to enforce, primarily because countries have differing viewpoints on the legality of these substances. That is, while one country may declare a certain substance illegal, another may impose no legal restrictions on that same substance.

One of the most commonly smuggled goods is human beings; trafficked humans are frequently exploited for labor, whether for clam picking in the United Kingdom, construction work in the Middle East, military service for ISIS and other terrorist groups, or perhaps most notoriously, as sex slaves. The International Labor Organization notes that the illicit trafficking of persons had led

[26] "The Global Regime for Transnational Crime." Council on Foreign Relations. June 25, 2013. Accessed August 13, 2016. http://www.cfr.org/transnational-crime/global-regime-transnational-crime/p28656.
[27] Ibid.
[28] "World Drug Report 2011." United Nations Office on Drugs and Crime. 2011. Accessed September 04, 2016. https://www.unodc.org/unodc/en/data-and-analysis/WDR-2011.html.

to a nearly $32 billion USD profit for criminal enterprises worldwide in 2005,[29] but this estimate is made in the backdrop of inconsistent definitions of human trafficking and imperfect reporting—the actual number is likely to be distressingly higher.

If the person is not being sold, then oftentimes, their organs are. Desperate recipients facing organ failure will often pay for organs from equally desperate youth from developing countries, usually leading to a massive payout on the order of tens of thousands of US dollars per transplant. The World Health Organization estimates that there are about 10,000 organ sales annually and approximately 1.14 illegal transplants per hour.[30]

Corruption

UN and international rhetoric often portrays corruption as having a symbiotic relationship with organized crime—corruption enables organized crime to proliferate; organized crime makes corruption profitable. Police officers especially are often paid to ignore, if not outright facilitate, illegal operations and smuggling within their jurisdiction, while public officials will favor using government money to purchase criminal enterprise-owned goods and services in exchange for a cut of the margin. This cycle ultimately feeds into the governments of developing nations diverting resources "from sectors of vital importance such as health, education and development" into criminal enterprises, thus economically harming some of the most impoverished in the world.[31] In extreme cases, such as the Russian Federation, corruption is not only pervasive, but accepted; to

[29] United Nations. Office on Drugs and Crime. "The Globalization of Crime: A Transnational Organized Crime Threat Assessment." UNODC. 2010. Accessed August 25, 2016. https://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf.

[30] Campbell, Denis, and Nicola Davison. "Illegal Kidney Trade Booms as New Organ Is 'sold Every Hour'" The Guardian. May 27, 2012. Accessed August 04, 2016. https://www.theguardian.com/world/2012/may/27/kidney-trade-illegal-operations-who.

[31] United Nations. UNICRI. "Organized Crime and Corruption." UNICRI. Accessed September 04, 2016. http://www.unicri.it/topics/organized_crime_corruption/.

many citizens in such countries, corruption is so embedded in government that it is no more than a way of life.[32]

International Cooperation in Investigation

On the enforcement side, widely varying definitions of organized crime and enforcement practices again prove to be extremely counterproductive to the effective punishment of such activities. While the United Nations Convention against Transnational Organized Crime calls for all countries to extradite criminals suspected of participating in organized crime,[33] the lack of a formal definition for organized crime is quite apparent, and cited as merely a means to allow for broader application of the Convention. Yet, this underscores the fundamental jurisdictional issues present in prosecuting complex and rapidly evolving networks of criminals—cooperation can prove difficult among police agencies that enforce significantly different laws, especially under a legal framework with little to no mechanism for implementation.[34] One case study following the Crown Police in several financial investigations noted that the formal procedures for police cooperation, a formal letter requesting information, proved too burdensome, and reverted to informal means of requesting, such as emails or phone calls.[35] While largely successful, this pattern of cooperation also indicates that the international framework for dealing with organized crime is excessively burdensome to police forces and may be preventing them from investigating effectively.

[32] Friedman, Misha. "For Russians, Corruption Is Just a Way of Life." The New York Times. August 18, 2012. Accessed September 04, 2016. http://www.nytimes.com/2012/08/19/opinion/sunday/for-russians-corruption-is-just-a-way-of-life.html.

[33] "Convention on Cybercrime." Treaty Office. September 23, 2001. Accessed August 16, 2016. https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

[34] "The Global Regime for Transnational Crime." Council on Foreign Relations. June 25, 2013. Accessed August 13, 2016. http://www.cfr.org/transnational-crime/global-regime-transnational-crime/p28656.

[35] Brown, Rick and Samantha Gillespie. 2015. "Overseas Financial Investigation of Organised Crime." *Journal of Money Laundering Control* 18 (3): 371-381. http://search.proquest.com/docview/1690364767?accountid=13314.

Country Policy

Market Nations

The majority of UN member nations are committed to reducing and fighting organized crime, but their ability to do so often is controlled by their socioeconomic status and the strength of the central government. The overwhelming majority of western nations in the UN affected by crimes such as human trafficking, and the illicit narcotics trade, such as the United States and western Europe are what would be considered "market nations," or nations in which the largest consumer demand for organized illegal activities exists. Put simply, market nations are generally the nations in which illicit goods are trafficked in and sold. These nations are often very powerful and affluent, and have extremely strict stances in regards to the regulation of and possession of these narcotics. These nations are usually the most committed to reducing organized crime, and are willing to spend large amounts of capital to reduce organized crime first within their borders, and then in other places throughout the world.

Supply Nations

Whereas market nations largely receive illicit goods for sale and consumption, supply nations are nations in which organized crimes (i.e., illicit goods) originate. In some cases, the governments of these nations do not support the manufacture or trade of such goods, but are powerless to stop them due to the large amount of power the leaders of the various criminal groups have, for example, the production of cocaine in Columbia by FARC. In other cases, these nations will publicly decry organized crime, but put in little effort, if any, to reduce production domestically. These nations are often extremely poor, with rampant corruption within the government and military and at large, and with a relatively uneducated and underprivileged population. Some prominent examples include Colombia and Myanmar.[36]

Transit Nations

[36] United States. Office of the Press Secretary. "Presidential Determination -- Major Drug Transit or Major Illicit Drug Producing Countries for Fiscal Year 2016." The White House. September 14, 2015. Accessed September 04, 2016. https://www.whitehouse.gov/the-press-office/2015/09/14/presidential-determination-major-drug-transit-or-major-illicit-drug.

The third and final nation type is the transit nations, countries that do not explicitly participate in the organized illegal activities, and are not the end goal of the cartels and various crime-focused organizations. These nations are also relatively poor, but have stronger governments than those that serve as points of origin for illicit activities such as the drug trade, or do not have a suitable social or political landscape for cartels or other organized crime groups to take hold. They are nations that have relaxed regulations and laws, and serve as transportation hubs for the organized crime rings. Oftentimes these nations border or are relatively close to market nations. Two examples of transit nations are Afghanistan and Costa Rica.[37]

[37] Ibid

Keywords

corruption	the act of an official or fiduciary person who unlawfully and wrongfully uses his station or character to procure some benefit for himself or for another person, contrary to duty and the rights of others[38]
organized crime	crime committed by groups engaged in planned and sustained criminal activities[39] (NB: In order to allow for greater coverage among differing legal regimes, no formal definition of organized crime exists in international law.)
human trafficking	the illegal sale of human beings as slaves, often for purposes of sexual or labor exploitation

[38] "Corruption." The Law Dictionary. Accessed September 04, 2016. http://thelawdictionary.org/corruption/.
[39] American Heritage® Dictionary of the English Language, Fifth Edition. S.v. "organized crime." Retrieved September 4 2016 from http://www.thefreedictionary.com/organized+crime

Questions

When formulating policy for your country, consider the following questions:

- How does your country define organized crime and related topics, and how do these definitions differ from surrounding countries, allies, and the rest of the international community's definitions?
- Is your country primarily used as a supply, transport, or market for illicit goods and services?
- How does your country's police and investigative forces currently address this organized crime market? How effective are its policies and practices? What can international cooperation do to assist in improving this effectiveness?

When formulating resolutions, please consider the following questions:

- Do countries need to standardize or harmonize their organized crime laws and practices in order to effectively investigate and prosecute organized crime? If so, what can INTERPOL do to encourage such harmonization? If not, what workarounds can be implemented?
- How can police forces, within the framework of existing policy, begin shifting away from an attitude of targeting individuals and groups and towards targeting the organized crime market as a whole? Should they?

Topic B: Cybercrime

In the days when all roads led to Rome, the over 52,000 miles of road that emitted from the city was at first seen as a demonstration of the empire's strength and infrastructural prowess. But as Rome's conquerors soon realized, it also enabled anyone to march troops straight to the city limits with unprecedented ease, such was the downfall of a great empire.[40]

Federal Bureau of Investigation Director Robert Mueller points out that history may soon repeat itself[41] as the Internet starts to look less like humankind's panacea and more like Rome's fateful roads. The world's interconnection infrastructure, in the words of Steven Chabinsky of the FBI, "offers the chance of a lifetime to cheat, steal, and strike from afar with little money, covered tracks, and enormous real world impact." Cybercrime has fast become a way of life for professional hackers, criminal masterminds, legitimate businesses, and everyday consumers alike; breaches of celebrity Twitter accounts, sensitive government documents, and credit card numbers have faded into the banal drone of the 5 o'clock news. The other side of cybercrime, known as cyber-enabled crime, is even harder to see, since offenses such as child pornography and online harassment are almost never reported and even less commonly investigated. Child porn site boylover.net had amassed over 70,000 members before even coming to the attention of the international police community.[42] INTERPOL delegates are tasked today with creating the necessary practices, infrastructure, and member state recommendations to facilitate the prevention, detection, investigation, and prosecution of cybercrimes of all flavors and varieties.

[40] Mueller, Robert S. "Major Executive Speeches." Federal Bureau of Investigation. November 6, 2007. Accessed August 1, 2016. https://web.archive.org/web/20090902233652/http://www.fbi.gov/pressrel/speeches/mueller110607.htm.

[41] Ibid.

[42] Europol. "More than 200 Children Identified and Rescued in Worldwide Police Operation." Europol. March 16, 2011. Accessed August 1, 2016. https://www.europol.europa.eu/content/more-200-children-identified-and-rescued-worldwide-police-operation.

History

To understand the history of cybercrime, one must first understand the potential and possibilities discovered in the early days of computing. Such potential proved huge; as early as July of 1966, the US House of Representatives began holding hearings on the nature and usage of this new technology. In those days, computers were still the size of entire rooms; the worst thing that could happen, in the eyes of the American government, was a Communist saboteur taking the trouble to *physically* breach their computers. (This did in fact happen in 1968, when an East German spy was discovered and captured in IBM's West Germany offices.[43]) Still, the American military took a bleak outlook; one de-classified report commissioned by the Defense Science Board admitted, "Contemporary technology cannot provide a secure system in a [sic] open environment," so "[it] is unwise to incorporate classified or sensitive information in a system functioning in an open environment unless a significant risk of accidental disclosure can be accepted."[44] While this sounds perfectly obvious today, it revealed something indisputably profound to contemporaries: that despite the computer's power to solve virtually any problem, computer security itself can never be solved, only addressed.

Fast forward a couple decades, and the root of the cybersecurity issue begins to manifest: that computer systems are not secure by default. Lt. Col. Roger, from the US Air Force, noted the extraordinary risk of such vulnerabilities, let alone maliciously-inserted back doors, yet "most military systems include programs not developed in a secure environment, and some are even developed abroad."[45] This would become increasingly important as wars become won and lost not with guns

[43] Warner, Michael. "Cybersecurity: A Pre-history." Intelligence and National Security 27, no. 5 (2012): 781-99. Accessed July 20, 2016. doi:10.1080/02684527.2012.708530.

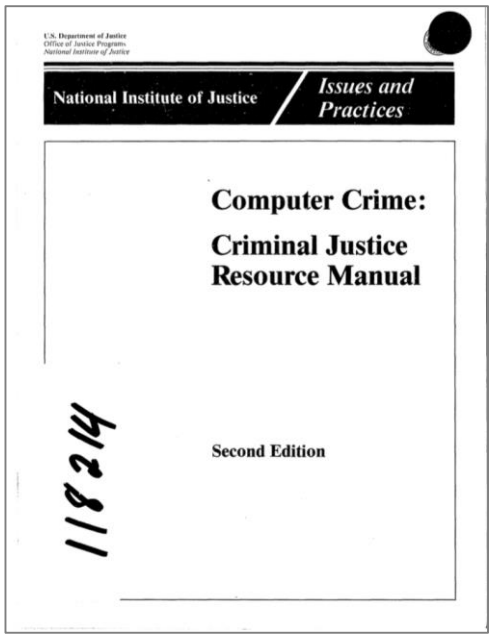
[44] Ware, Willis H. Security and Privacy in Computer Systems. Report. Santa Monica, CA: RAND Corporation, 1967. Accessed July 23, 2016. http://www.rand.org/content/dam/rand/pubs/ papers/2005/P3544.pdf.

[45] Schell, Roger R. "Computer Security: The Achilles' Heel of the Electronic Air Force?" Computer Security: The Achilles' Heel of the Electronic Air Force? Accessed July 24, 2016. http://www.airpower.maxwell.af.mil/ airchronicles/aureview/1979/jan-feb/schell.html.

Also of note is that the USSR has historically accused the US of doing just, in 1990 positing that US-made computers were capable of stealing Russian state secrets: Nikolai Brusnitsin, Openness and Espionage

but with keyboards. In a joint statement after the Gulf War, the Air Force Chief of Staff and Secretary noted that by hacking into enemy refineries, they discovered "the means of affecting the refineries' operations at a time of our choosing," that is to say, they developed a huge strategic advantage through what they would later term "information warfare" or less ominously, "information operations." In a sense, the weaknesses found in computing since the 1960s had not only become well known, but strategic, and soon a wide variety of countries would follow in developing advanced cyber warfare techniques.

Cybercrime as a phenomenon developed parallel to the rise of the personal computer, which empowered cybercriminals to begin appearing out of virtually nowhere and gain traction and power.



In the early 1970s, researchers had concluded that cybercrime was not worth discussing as its own issue; this proved, needless to say, completely false. Certainly, the publication of the Computer Crime Criminal Justice Resource Manual[46], authored by SRI International in 1979, could not have arrived quickly enough; just two years later, the first hacker declared a felon, Ian Murphy a.k.a. Captain Zap, was convicted of illegally tampering with AT&T's phone billing system. Of course, he would not be the last, as such infrastructure attacks became increasingly common and high-profile. Despite security advances, by the early 1990s, an acute awareness of the dangers of computing had begun to penetrate the public consciousness. The 1986 blockbuster *War Games*, depicting a hacker accidentally triggering US supercomputers into triggering a nuclear war, made sure of that. The more

(Moscow: Military Publishing House 1990), pp.28–9.

[46] SRI International. Computer Crime: Criminal Justice Resource Manual. Washington, D.C.: National Criminal Justice Information and Statistics Service, Law Enforcement Assistance Administration, U.S. Dept. of Justice, 1979. Accessed July 20, 2016. https://babel.hathitrust.org/cgi/pt?id=pur1.32754078042987.

banal attacks on infrastructure, of course, would prove more frequent. The 1988 Morris Worm, meant as an academic exercise to determine the size of ARPANet (the precursor to our modern Internet), instead slowed it down to a crawl for not only military users, but also Universities nationwide, costing its victims approximately $98 million in total.[47] In one of the earliest known cases of electronic theft, the First Bank of Chicago lost almost $70 million in a 1988 computer attack[48]—of course, also dragging down the bank's patrons into the fray. Cybersecurity had left the confines of military theory and entered the lives of everyday citizens.

Concurrently, the late 1980s and early 1990s brought about an awareness of cybercrime among the international community. The Council of Europe, for one, had begun to develop recommendations for cybercrime laws around the late 1980s, publishing its first report in 1989, and its second in 1995.[49] (These recommendations, with help from the US, Japan, Canada and South Africa, would later form the basis for the Council of Europe Convention on Cybercrime, discussed in the next section.) Russia and the PRC had begun to notice the information warfare infrastructure America had been developing since the 1960s as well; Chinese Major General Wang Pufeng noted that "the people's war of the past was conducted in tangible space, but information warfare…is conducted even more in intangible space."[50] Soon enough, virtually every country sought to develop

[47] Lee, Timothy B. "How a Grad Student Trying to Build the First Botnet Brought the Internet to Its Knees." Washington Post. November 1, 2013. Accessed August 27, 2016. https://www.washingtonpost.com/news/the-switch/wp/2013/11/01/how-a-grad-student-trying-to-build-the-first-botnet-brought-the-internet-to-its-knees/.
University Alliance. "A Brief History of Cyber Crime." Florida Tech. Accessed August 27, 2016. http://www.floridatechonline.com/resources/cybersecurity-information-assurance/a-brief-history-of-cyber-crime/.

[48] Specter, Bob. "7 Charged in $70-Million Chicago Bank Embezzlement Scheme." Los Angeles Times. 1988. Accessed July 23, 2016. http://articles.latimes.com/1988-05-19/news/mn-4838_1_embezzlement-scheme.

[49] Wills, John. "Cybercrime: Is the Internet Outside the Law." In *History behind the Headlines: The Origins of Conflicts Worldwide*, 86-97. Vol. 6. Detroit: Gale Group, 2003. Accessed August 23, 2016. http://go.galegroup.com/ps/i.do?id=GALE|CX3410600217&v=2.1&u=someco_main&it=r&sw=w&asid=b0a8deebdedefac0254f6e31bd28d9c4.

[50] Schell, Roger R. "Computer Security: The Achilles' Heel of the Electronic Air Force?" Computer Security: The Achilles' Heel of the Electronic Air Force? Accessed July 24, 2016. http://www.airpower.maxwell.af.mil/ airchronicles/aureview/1979/jan-feb/schell.html.

protection against the cybercrimes, and some, like China and Russia, raced to develop offensive capability as well.

It would seem, however, that such efforts nonetheless were unable to keep up with the rapid advances of both technology and its adoption. With British Computer Scientist Sir Tim Berners-Lee's 1989 invention, the World Wide Web, criminals were able to move beyond the traditional cybercrimes of merely "hacking" computers. The most notable and pervasive of these new "cyber-enabled crimes" proved to be child pornography. The International Tribunal of Children's Rights pointed out in the aftermath of the World Wide Web, "more and more children are being raped and tortured as fixed images give way to live shows on computers."[51] To close down a popular pedophile forum from the late 1990s, the "Wonderland" chat room, US and European customs and police departments carried out over 100 raids in 12 countries to achieve this feat, indicating the sheer difficulty of targeting cyber-enabled crime even before computers reached the scale and penetration the technology enjoys today. The rise of Napster, a popular music service that allowed users to illegally download music free of charge, created panic among the music industry, who feared a loss of sales from music piracy. (While groups like the Recording Industry Association of America and the often exaggerate the amount of potential sales they lost, that number is undoubtedly large; in 2001 Napster users downloaded approximately 2.7 billion songs in a single month.[52])

Cybercriminals today continue to innovate, finding new ways to profit off illegal activities online. The most recent innovation is perhaps the most sophisticated: the dark net market. While networks have been used as early as 1970 by MIT and Stanford students to purchase marijuana,[53] recent technologies, most notably Tor and Bitcoin, have enabled virtually untraceable purchases of anything from LSD to AK-47s. Most famously, the 2011 Gawker exposé of the Silk Road dark net

[51] Wills, John. "Cybercrime: Is the Internet Outside the Law." In *History behind the Headlines: The Origins of Conflicts Worldwide*, 86-97. Vol. 6. Detroit: Gale Group, 2003. Accessed August 23, 2016. http://go.galegroup.com/ps/i.do?id=GALE|CX3410600217&v=2.1&u=someco_main&it=r&sw=w&asid=b0a8deebdedefac0254f6e31bd28d9c4.

[52] Ibid.

[53] Power, Mike. "Online Highs Are Old as the Net: The First E-commerce Was a Drugs Deal." The Guardian. 2013. Accessed August 27, 2016. https://www.theguardian.com/science/2013/apr/19/ online-high-net-drugs-deal.

market[54] and consequent 2013 arrest of Silk Road creator Ross Ulbricht[55] has revealed not only the staggering potential of the Internet to create such markets, but the rising priority of police to destroy such markets. After all, Silk Road processed nearly $22 million in drug sales annually until its seizure. More commonplace, the development of the BitTorrent protocol and subsequently torrenting sites like The Pirate Bay have enabled copyright infringement on a massive scale. Cybercrime, as a result, has become commonplace, more present than ever, and with an ever increasing need to address.

[54] Chen, Adrian. "The Underground Website Where You Can Buy Any Drug Imaginable." Gawker. 2011. Accessed August 27, 2016. http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160.

[55] McCormick, Ty. "The Darknet: A Short History." Foreign Policy. December 9, 2013. Accessed August 27, 2016. http://foreignpolicy.com/2013/12/09/the-darknet-a-short-history/.

Relevant International Law and UN Actions

Universal Declaration of Human Rights, esp. Article 19 (1948)[56]

The fight against cybercrime, as with many crimes, derives from the desire to protect people, specifically their rights as humans. Articles of the UDHR that can apply to cybercrime include Article 3, establishing life, liberty and security of person, and Article 19, which establishes freedom of expression in the media.

General Assembly Resolutions 55/63 (2001), 56/121 (2002)

These two resolutions jointly outline and affirm the United Nations' broad framework for dealing with cybercrime, noting not only that police among nations should cooperate on these efforts, but also that the "fight against the criminal misuse of information technologies requires…both the protection of individual freedoms and privacy and the preservation of the capacity of Governments to fight such criminal misuse," importantly noting that citizen privacy must also be protected in investigation practices. The resolutions largely step away from recommending any specific policy, of course, but do indicate several bodies that are permitted to represent the General Assembly in its dealings with cybercrime.

Council of Europe Convention on Cybercrime (2001)[57]

This treaty is one of the first international steps towards harmonization, that is, the unification of policies and integration of constituent police bodies, on the topic of cybercrime. Under this treaty, each state needs to adopt laws outlawing the following actions: unauthorized access of devices, unauthorized interception of information, interference or misuse of devices, computer-related forgery and fraud, child pornography, and intellectual property infringement. It also provides for standardized methods to allow police bodies to quickly and easily share evidence, findings,

[56] United Nations. "Universal Declaration of Human Rights." Refworld. Accessed August 27, 2016. http://www.refworld.org/docid/3ae6b3712c.html.

[57] Council of Europe. *Convention on Cybercrime*. Strasbourg: Council of Europe, 2002. Accessed August 20, 2016. https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

training, and methods across state lines, as well as jurisdictional guidelines and limits on police power in cyberspace.

Geneva Declaration of Principles and Plan of Action (2003)[58]

Tunis Commitment and Tunis Agenda (2005)[59][60]

The Geneva Declaration of Principles and Plan of Action are the output of the World Summit on the Information Society, which met in Geneva in 2003, and among broad goals regarding the state of media, telecommunications, etc. in the international community discusses the prevention and punishment of cybercrime as a means of ensuring that people feel confident in using the latest technologies in advancing the world.

The World Summit on the Information Society met again in 2005 in Tunis, which ultimately led to the creation of the Tunis Commitment and Tunis Agenda. Like the Geneva Declaration and Plan of Action, the Commitment would re-establish the broad goals for Internet governance the international community agreed upon, while the Agenda would go into more specifics. Of note in the Agenda is operative clauses 37-40, which deal specifically with cybercrime, and operative clause 72, which establishes the Internet Governance Forum. The Tunis Commitment and Agenda prove important in a discussion of cybersecurity as it describes the principles by which governments, and thus police forces, must abide by in any policy or implementation.

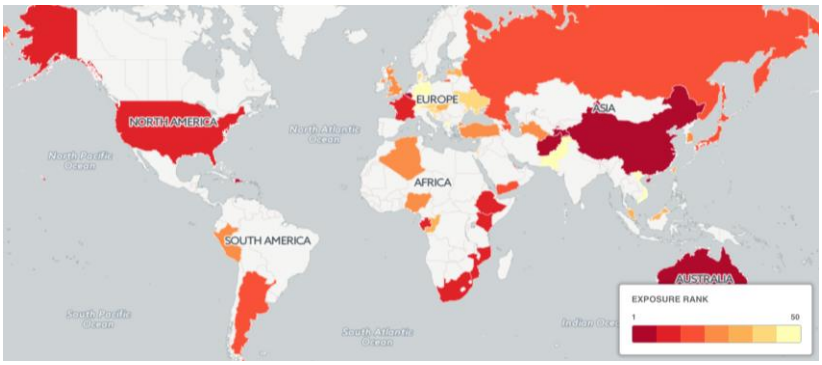
[58] United Nations. International Telecommunications Union. "The Geneva Declaration of Principles and Plan of Action." *ITU*, Accessed July 25, 2016. https://www.itu.int/net/wsis/docs/promotional/brochure-dop-poa.pdf.

[59] United Nations. International Telecommunications Union. *Tunis Commitment*. November 18, 2015. Accessed July 28, 2016. http://www.itu.int/net/wsis/docs2/tunis/off/7.html.

[60] United Nations. International Telecommunications Union. *Tunis Agenda for the Information Society*. Geneva: United Nations, 2005.

Current Status

Cybercrime is becoming more profitable, and thus more commonplace, by the day. While accurate statistics on the exact impact of cybercrime are rare to find, one report from McAfee places the global damage at $400 billion USD per year.[61] While governments are beginning to converge on uniform principles and policies to address cybercrime, there is much left wanting of the way the world's governments address this issue. In 2013, an expert committee, commissioned by the General Assembly to conduct a Comprehensive Study on Cybercrime, noted that cybercrime laws and practices are diverse to the point that the committee feared "the emergence of country cooperation 'clusters,'" or blocs of countries that would only cooperate amongst themselves in investigations, ultimately undermining the effectiveness of international police operations.[62] In particular, the United States and China have major issues with cybercrime, collectively responsible for over half of the world's attack traffic,[63] but vulnerability to cybercrime is almost universal; security research firm Rapid7 found that the countries most vulnerable to hacking have little geographical commonality.[64]



Heat map of countries' National Exposure Index, a metric created by security research firm Rapid7.

[61] *Net Losses: Estimating the Global Cost of Cybercrime.* Publication. Center for Strategic and International Studies, McAfee. June 2014. Accessed July 26, 2016. http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

[62] United Nations. Office of Drugs and Crime. Comprehensive Study of the Problem of Cybercrime and Responses to It by Member States, the International Community and the Private Sector. January 23, 2013. Accessed July 23, 2016. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/ UNODC_CCPCJ_EG4_2013_2_E.pdf.

[63] Milian, Mark. "Top Ten Hacking Countries: Red Alert." Bloomberg. April 23, 2013. Accessed August 28, 2016. http://web.archive.org/web/20160414060803/http://www.bloomberg.com/slideshow/2013-04-23/top-ten-hacking-countries.html.

[64] Titcomb, James. "Mapped: The Countries Most Vulnerable to Cyber-attacks." The Telegraph. June 10, 2016. Accessed August 1, 2016. http://www.telegraph.co.uk/technology/2016/06/10/mapped-the-countries-most-vulnerable-to-cyber-attacks/.

Key Issues

International Cooperation

At the root of the issues INTERPOL will be facing is the lack of standardization among regimes regarding cybercrime. As previously mentioned, the UN is deeply concerned that States will not be able to cooperate in investigations and prosecutions due to the lack of a standardized cybersecurity regime. In some states, for example, unauthorized access to a computer system is considered distinct from unauthorized access to the data within it, and in many countries, the use of hacking tools is not even illegal, thereby restricting prosecution possibilities for cybercriminals.

Furthermore, even if these legal regimes are in alignment, there are often barriers to passing along vital evidence and insights. These barriers, of course, are at times necessary, as the gratuitous sharing of information should be prevented, but such barriers are proving excessive in the high-pace scene of modern cybercrime. As the Comprehensive Study on Cybercrime concludes, "Reliance on traditional means of formal international cooperation" as applied to cybercrime investigations "is not currently able to offer the timely response needed for obtaining volatile electronic evidence."[65] Indeed, many police forces nowadays do unwittingly infringe on other countries' electronic jurisdiction, "due to cloud computing technologies which involve data storage at multiple data centres in different geographic locations," making it difficult to know where the data they're accessing is actually, physically situated.[66]

[65] United Nations. Office of Drugs and Crime. Comprehensive Study of the Problem of Cybercrime and Responses to It by Member States, the International Community and the Private Sector. January 23, 2013. Accessed July 23, 2016. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/ UNODC_CCPCJ_EG4_2013_2_E.pdf.

[66] Ibid.

Malware and Fraud

Malware and fraud are the two most consumer-visible forms of cybercrime, directly infecting end user machines or stealing money. While viruses, worms, ad-ware, phishing, etc. have existed for quite some time, they are constantly evolving, and automated tools like anti-virus prove of limited use in protecting users, with new viruses being discovered every week. Today's viruses have taken on a particularly frightening new face: ransomware, which discreetly encrypts a user's files and then holds the password up for ransom. This has proven massively profitable for attackers; the ransomware Cryptolocker has amassed an estimated $3 million for its creators.[67] In fact, the FBI reportedly has no recourse against ransomware; Joseph Bonavolonta, Assistant Special Agent in Charge of the Cyber and Counterintelligence Program at the FBI is quoted saying of the ransomware Cryptolocker, "The ransomware is that good…. To be honest, we often advise people just to pay the ransom."[68] On the other hand, Europol has set up an advisory website, called No More Ransom, with guidelines on preventing and removing ransomware without forfeiting money.[69] The effect of this measure has yet to be seen, but offers a possible starting point for further preventative and investigative measures.

Cyber-enabled Crime: Child Pornography, Darknet Markets

Cyber-enabled crime, or illicit actions facilitated by the Internet, prove to be the most common form of cybercrime present today. As stated before, the most sophisticated cybercrime phenomenon in recent history is the Darknet Market, an online site that allows one to buy illegal drugs, arms, and other goods with about the same convenience as buying a book off Amazon. Today, using such markets makes the use of Tor, a tool meant to make it impossible to trace a single

[67] Shahani, Aarti. "Ransomware: When Hackers Lock Your Files, To Pay Or Not To Pay?" NPR. December 8, 2014. Accessed August 28, 2016. http://www.npr.org/sections/alltechconsidered/2014/12/08/366849122/ransomware-when-hackers-lock-your-files-to-pay-or-not-to-pay.

[68] Zorabedian, John. "Did the FBI Really Say "pay Up" for Ransomware? Here's What to Do…." Naked Security. October 28, 2015. Accessed August 28, 2016. https://nakedsecurity.sophos.com/2015/10/28/did-the-fbi-really-say-pay-up-for-ransomware-heres-what-to-do/.

[69] "Ransomware Advice Service to Tackle Extortion Gangs." BBC. July 25, 2016. Accessed August 1, 2016. http://www.bbc.com/news/technology-36883056.

computer's web traffic, as well as Bitcoin or related cryptocurrency, which allows for the anonymous and secure transfer of money. The first popular Darknet Market to use these technologies was Silk Road, which was made known to the public at large by Gawker in 2011 and shut down in 2013 by the FBI. Since then, Darknet Markets have increased in number, selection, and security, making it harder for police forces to investigate and shut them down. In the meantime, purchasing illegal goods has become easier and safer than ever, with no apparent end in sight.

Even before Darknet Markets appeared, the production and distribution of child pornography has long been the most publicly-feared cyber-enabled crime in recent memory. Today, the producers and consumers of such content number in the hundreds of thousands, with techniques that the framers of many child pornography laws could even begin to fathom. One case involved an unsuspecting victim being arrested for the possession of child pornography because hackers had been using his computer to store their files, so as to avoid arrest themselves. Between 1997 and 2005, child pornography sites are estimated to have increased by over 1500%, and the problems associated with this increase are clear: the market for this illicit content creates pressure to abuse, exploit, and torture children, the 4 out of 5 of which were under the age of 10, and 1 out of 25 of which were not even old enough to walk at the time of filming.[70] However, many states have conflicting laws regarding such content, complicating international cooperation in investigating and prosecuting pornographers. While 83 countries do have sufficient legislation to combat child pornography, according to the International Centre for Missing and Exploited Children, 35 countries today still have no legislation targeting child pornography.[71]

[70] "Child Pornography: Model Legislation and Global Review." International Centre for Missing & Exploited Children. 2016. Accessed August 1, 2016. http://www.icmec.org/wp-content/uploads/2016/02/Child-Pornography-Model-Law-8th-Ed-Final-linked.pdf.

[71] Ibid.

Country Policy

OECD Countries

Generally the nations with the closest historical and economic ties with the Internet, members of the OECD have enjoyed ubiquitous Internet access from early on, and as a result, their citizens' economic, social, and political lives depend the most heavily on its unfettered usage. At the same time, these countries have also had the most experience combating cybercrime, the United States having written the Computer Crime Criminal Justice Resource Manual as early as 1978. This experience, in addition to the general lack of strong government controls (i.e. censorship) of Internet access, has led to the OECD leading the world in the development of public-private partnerships for dealing with cybercrime.[72] The OECD also places a strong emphasis on the protection of human rights when implementing security,[73] namely "the freedom of expression, the freedom of information, the confidentiality of information and communication, the protection of privacy and personal data, openness and fair process."[74] (Of course, in practice those rights are not as well-respected as the OECD's principled statements, but comparatively speaking, OECD nations tend toward more Internet freedom than less.)

Asian Countries

While China is the source of 40% of the world's cyberattacks, all Asian nations largely share a very proactive, if not suppressive, means of preventing and tracking down illegal content. South Korea, for example, starkly differs from other OECD nations in its total ban of pornography.[75] At the same time, such measures have shown limited success in preventing other forms of cybercrime; the ASEAN regional bloc's cybersecurity methods, for example, "are largely ineffective due to the absence of compliance mechanisms and intra-bloc divergences in security priorities and

[72] Kulesza, Joanna, and Roy Balleste. *Cybersecurity and Human Rights in the Age of Cyberveillance*. Accessed July 28, 2016. https://books.google.com.hk/books?id=cDL0CgAAQBAJ.
[73] OECD. *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*. Paris: OECD Publishing. 2015. Accessed August 28, 2016. http://dx.doi.org/10.1787/9789264245471-en.
[74] Ibid.
[75] "South Korea Crusades against Online Pornography." USA Today. December 10, 2012. Accessed August 1, 2016. http://www.usatoday.com/story/news/world/2012/12/10/south-korea-porn/1758277/.

capabilities,"[76] that is to say, the lack of consistent cybercrime laws among Asian nations, that allow the incredibly fluid, rapidly-evolving nature of cybercrime to fester and push through these cracks in international law. In fact, some nations have not even criminalized the consumption or viewing of child pornography.[77] Some efforts have been proposed to address this; reports have recently surfaced that officials in the region are considering the creation of a regional police collaboration body, like Europol, to target their specific issues with cybercrime.[78]

Former Soviet Countries

Cybercrime rings in the former Soviet Union states, particularly Russia, have proven massively lucrative, the Russian cybercrime industry regularly pulling in $2 billion in profits annually.[79] (This is largely due to a lack of well-paying legitimate engineering jobs for Russian graduates and a relaxed enforcement regime of cybercriminals, with the Russian police largely prosecuting violent crimes over electronic theft of non-Russian targets.[80]) In these nations, cybercrime has become a profession to an extend unprecedented anywhere else in the world, developing not only malware markets, but seller reputation management and branding that ensures the quality of the malware toolkit.[81] In fact, one associate of INTERPOL East Europe, Dr. Paolo Sartori, points out, "There is not a culture to consider these guys as criminals, as robbers, as killers. They are considered professionals as others."[82] As a result, these countries' police forces not only

[76] Beyer, Jessica. "ASEAN Cybersecurity Profile: Finding a Path to a Resilient Regime." The Henry M. Jackson School of International Studies. April 4, 2016. Accessed August 1, 2016. https://jsis.washington.edu/news/asean-cybersecurity-profile-finding-path-resilient-regime/.

[77] Song, Janice Kim. "Protecting Children from Cybercrime: Legislative Responses in Asia to Fight Child Pornography, Online Grooming, and Cyberbullying." The Communication Initiative Network. July 12, 2016. Accessed August 20, 2016. http://www.comminit.com/ict-4-development/content/protecting-children-cybercrime-legislative-responses-asia-fight-child-pornography-online.

[78] Pauli, Darren. "Asian Nations Mull Regional 'Europol' in Fight Against Cybercrime." The Register. July 21, 2016. Accessed August 22, 2016. http://www.theregister.co.uk/2016/07/21/asian_nations_mull_regional_europol_in_fight_against_cybercrime/.

[79] Plesser, Ben. "Skilled, Cheap Russian Hackers Power American Cybercrime." NBC News. February 5, 2015. Accessed August 1, 2016. http://www.nbcnews.com/news/world/skilled-cheap-russian-hackers-power-american-cybercrime-n22371.

[80] Ibid.

[81] Gertz, Bill. "Interpol: Cyber Crime from Russia, E. Europe Expands." Washington Free Beacon. October 2, 2015. Accessed July 28, 2016. http://freebeacon.com/national-security/interpol-cyber-crime-from-russia-e-europe-expands/.

[82] Ibid.

have to deal with the rising tide of profit itself, but an increasingly accepting culture that can make it difficult to even justify investigating cybercrimes that occur.

African Nations

The African continent is generally considered to have the least widespread, but also fastest growing Internet infrastructure in the world. As such, the region is in a prime place to avoid the problems encountered by nations whose cybercrime enforcement regimes have struggled to keep up with their citizens' use of the Internet. For example, the infamous "Nigerian Prince Scam" email, promising the recipient of an email great riches if he or she supplies the so-called Nigerian Prince with their bank account numbers, had successfully targeted millions of professionals, especially in developed nations. In the private sector, many companies underemphasize cybersecurity, and the majority of companies that understand the risks do not employ sufficient talent to protect their infrastructure.[83] Fortunately, African nations, especially Nigeria and Kenya,[84] are starting to develop cybercrime laws, which, if formulated and enforced correctly, could nip the cybercrime threat in the bud for the region, and discussing such laws and enforcement practices could greatly benefit this process. This has surmounted in the 2014 African Union Convention on Cyber Security and Personal Data Protection, largely inspired by the Council of Europe Convention discussed above. This proposal, which places emphasis on data protection and human rights, however also leaves several loopholes, such as bans on "insulting" others online and the use of fraudulently-obtained information (i.e., whistleblower documents).[85] It is up to African police forces to set the precedent for the application of this convention for years to come.

[83] Ogundeji, Olusegun Abolaji. "African Organizations Lag in Cybersecurity, Global Survey Says." PCWorld. November 11, 2014. Accessed August 1, 2016. http://www.pcworld.com/article/2846312/african-organizations-lag-in-cybersecurity-global-survey-says.html.

[84] Malakata, Michael. "Africa's Effort to Tackle Cybercrime Gains Momentum." PCWorld. September 8, 2015. Accessed August 1, 2016. http://www.pcworld.com/article/2981739/africas-effort-to-tackle-cybercrime-gains-momentum.html.

[85] "African Union Adopts Framework on Cyber Security and Data Protection." Access Now. August 22, 2014. Accessed July 29, 2016. https://www.accessnow.org/african-union-adopts-framework-on-cyber-security-and-data-protection/.

Keywords

The cybersecurity space is notorious for having a thorough and technical jargon; as such, the key words provided are far from comprehensive of the words you may need to know for debate.

Bitcoin	a "cryptocurrency," or electronic currency governed by no central issuing authority and is entirely anonymous, lending itself to often being used for dark net markets and illicit sales
Bot-Net	a network of computers infected by the same attacker, with functionality that allows the attacker to command all of these computers to do some collective action, i.e. send spam e-mails
Cybercrime	any crime that involves the use of networked computers, including both security breaches of computers and the use of computers to commit otherwise non-virtual crimes
Denial of Service	a form of cyberattack in which the attacker overloads the target computer with phony connections and requests, thus preventing legitimate use
Phishing	a form of fraud in which the attacker convinces the victim to enter his/her credentials into a fake login form, thereby allowing the attacker to log in as the victim
Tor	"The Onion Router," originally created by the US Dept. of State to allow political dissidents to connect to the Internet safely, now allows anyone to use the Internet with virtually no identity exposure, often used for darknet market transactions

Questions

In formulating country policy, you may want to consider the following questions:

- What legislation does your country have regarding the legal status of cybercrime? Police power to investigate such crimes?
- What are your country's police practices in addressing cybercrime? Is there a specialized unit for cybercrime? How and how well are they trained in technical knowledge and best practices? What kinds of cybercrime are prioritized for investigation?
- What efforts does your country currently place into cybersecurity, specifically in prevention, investigation, and prosecution of cybercrime?
- Does your country have a history of cooperating with other countries in cybercrime investigations? What jurisdictional issues has it had?

In formulating resolutions, addressing the following questions would be highly recommended:

- When participating in joint investigations, what rules should police use when determining jurisdiction?
- What best practices exist to address cybercrime? How should INTERPOL train police forces to exude these best practices?
- What goals and benchmarks should be used to measure and motivate the effectiveness of cybersecurity practices?
- Generally speaking, how can INTERPOL act to mitigate the threat of cybercrime for member states?