Florida High Schools Model United Nations

FHSMUN GULF COAST 7

UNITED NATIONS OFFICE ON DRUGS AND CRIME

CYBERCRIME AND THE RIGHT TO PRIVACY IN THE DIGITAL

Author: Sasha Ahles & Brian D. Sutliff

Cybercrime has become an established threat to the security of States and individuals alike.
- Loide Lungameni, Chief of the Organized Crime and Illicit Trafficking Branch, UNODC

Introduction

"Cybercrime is an emerging form of transnational crime. The complex nature of the crime as one that takes place in the border less realm of cyberspace is compounded by the increasing involvement of organized crime groups."[1] A growing problem for everyone, it is critical to be able to identify what constitutes a cybercrime. "Cybercrime exists in many forms, the most common being identity-related offenses. This occurs by 'phishing' (deceiving Internet users into giving their personal information), the dissemination of 'malware' (software that disrupts computer systems and collects personal or sensitive information), and hacking (illegally accessing someone's computer remotely)."[2] These methods are frequently used for stealing credit card information and money.[3] Tragically, more serious and advanced offenses have begun to emerge. "The Internet has become a breeding ground for criminal activity related to copyright and intellectual property rights, as well as offenses such as child pornography and abuse material."[4]

Questions about an individual's right to privacy have also become paramount in recent years. In the aftermath of the September 11, 2001 attacks on New York City and Washington DC, the US Congress passed the USA Patriot Act that dramatically expanded the government's ability to obtain data about individuals' call records, medical histories, financial information, and internet search queries. Legal challenges to the USA Patriot Act were swift[5], although the ultimate resolution of the US government's ability to investigate peoples' digital footprints without first obtaining a warrant remains an open question. The United States is only one of dozens of countries that is currently grappling with balancing peoples' right to privacy and the emphasis of law enforcement officials on obtaining information related to potential criminal, and even terrorist, actions. In December 2015, the European Union (EU) approved new legislation

[1] *Emerging Crimes*, UNODC, 2015

[2] *DOHA: UN Conference weighs efforts to combat cybercrime, create safer digital world*, UN News Centre, 17 April 2015

[3] The recent high-profile hacks of Capital One, Equifax, and Marriott are frequently cited examples, but there are many other instances within the United States and around the world.

[4] *DOHA: UN Conference weighs efforts to combat cybercrime, create safer digital world*, UN News Centre, 17 April 2015

[5] Susan Jo Keller, "Judge Rules Provisions in Patriot Act to be Illegal", *New York Times*, September 27, 2007.

aimed at clarifying and strengthening important provisions about an individual's right to privacy, including the so-called "right to be forgotten,"[6] a relatively recent provision in European law where individuals may request that digital records and references from beyond a certain number of years may be erased. While the "right to be forgotten" has been applauded by digital privacy advocates, other observers have voiced concerns about individuals potentially expunging relevant, albeit embarrassing, information, such as criminal histories[7], particularly when seeking employment, business and personal loans or even public office.

Scale of the Problem

"Computer related crime is a long established phenomenon, but the growth of global connectivity is inseparably tied to the development of contemporary crime."[78] Cyberspace has become an ideal space for criminals due to the enormous victim pool (about 2 billion users worldwide), as well as the ability to maintain anonymity while gaining access to information that is often knowingly, but also quite frequently unwittingly, stored online.[9] Because of this not only has the number of cyber criminals gone up, but so has the number of their victims. In July 2019, the global total of "active internet users" was estimated at approximately 4.33 billion unique internet users, accounting for more than 50% of the world's population.[9] More than 60% of users are in developing countries and 45% of users are 25 years old or younger.[1011] According to figures published by the United Nations Information Service (UNIS) in 2015, the reach of cybercrime is even greater. There are about 431 million people that have been affected by cybercrime, equating to about 1 daily million victims and 14 adult victims every second. Automated hacking increased to 80 million attacks per day. All of these attacks occur in the rapid growth of a business that may exceed $3 trillion per year[12]; the most widely accepted estimates at this time as to the monetary damages caused by cybercrime and intellectual property theft are approximately $445 billion USD[12], with 2019 estimates of individual and business spending on information security products and services approximating $125 billion USD.[13]

As technology and its availability continues to grow, so does the reach of cybercrime. By 2017, mobile broadband subscriptions approached 70% of the total population with the number of networked devices outnumbering the number of people by six to one[15]; by 2018, more than half of all internet access originated on mobile phones.[14] This growth creates a pressing need to

---

[6] Mark Scott, "Europe Approves Tough New Data Protection Rules" *New York Times* December 15, 2015. [7] Dominique Mosbergen, "Some Criminals Have A 'Right to be Forgotten' on Google, UK High Court Rules", *Huff Post*, April 13, 2018.

[7] *Comprehensive Study on Cybercrime*, UNODC, February 2013

[8 th] *United Nations Congress on Crime Prevention and Criminal Justice, Doha, 12-19 April 2015 | Cybercrime*, UNIS Vienna, 2015

[9] *Statista*, "Global digital population as of July 2019 (in millions)", 2019. Found at: https://www.statista.com/statistics/617136/digital-population-worldwide/

[10] *Comprehensive Study on Cybercrime*, UNODC, February 2013

[11 th] *United Nations Congress on Crime Prevention and Criminal Justice, Doha, 12-19 April 2015 | Cybercrime*, UNIS Vienna, 2015

[12] *The Economist*, "Defending the digital frontier" July 12, 2014.

[13] Steve Morgan, ed., & Cybersecurity Ventures, "2019 Official Annual Cybercrime Report", 2019, p. 6. Found at: https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

[15] *Comprehensive Study on Cybercrime*, UNODC, February 2013

[14] *Statista*, "Percentage of all global web pages served to mobile phone from 2009 to 2018", 2018. Found at: https://www.statista.com/statistics/241462/global-mobile-phone-website-traffic-share/

[17] *Emerging Crimes*, UNODC, 2015

address the issue as soon as possible. Perpetrators of cybercrime and their victims can be located in different regions and its effect can ripple through societies around the world, highlighting the need to mount an urgent, dynamic, and international response.[17] While advertising and news stories frequently focus on the problems to consumers posed by cybercrime, large-scale institutions[15], both public and private, are also frequently targeted, particularly because of the enormous monetary and informational resources at risk.

Cyberterrorism and the Threat to States

Acts of terror have long since been a threat to countries across the globe. However, advancement in technologies has given a whole new aspect to terrorism that was not previously existent or focused on. The September 11, 2001 attacks "prompted the start of an intensive discussion about the use of information and communication technologies (ICTs) by terrorists," with reports showing that the offenders used the Internet in preparation of the attacks.[16] A recent UNODC publication, *the use of Internet for terrorist purposes*, observes that "computer systems may be used for a range of acts that promote and support terrorism,"[17] including propaganda (recruitment, radicalization and incitement to terrorism); financing; training; planning (through secret communication and open source information); execution; and cyberattacks.[18]

A recent example of how terrorists can use the Internet to plan, coordinate and commit their crimes, can be seen in Western Europe. "In May 2012, a Western European court sentenced one of its nationals to five years imprisonment for participation of a terrorist act. At trial, the prosecution presented dozens of decrypted email communications of jihadist content, which were, among others, sent to the website of the President of the country, and traced back to a member of a globally operating extremist group. A preservation order enabled the authorities to identify communication between the extremist group's member and extremist websites, including a website with the stated goal of hosting and disseminating the extremist group's documents, audio and video recordings, statements from warlords and suicide attackers, and the materials of other extremist groups. This indicated that the defendant actively performed, inter alia, the translation, encryption, compression and password protection of pro-jihadist materials, which he then uploaded and circulated via the Internet; and taking concrete steps to provide financial support to extremist groups, including the attempted use of PayPal and other virtual payment systems. The court found the required sufficient evidence to demonstrate that the defendant had provided not merely intellectual support, but also direct logistical support to a clearly identified terrorist plan."[19]

The planning and organization of a terrorist attack over the Internet is not the only threat to a state as a result of the growth of the cyberspace, but rather actual attacks committed by terrorist groups themselves being carried out online as well. Attacks against critical information infrastructures have widely been recognized as potential targets for terrorist attacks. As reliance on information technology grows, so does the vulnerability of these critical information structures; particularly interconnected systems that are linked by computer and communication

---

[15] Liz Moyer, "Prosecutors Announce More Charges in Hacking of JPMorgan Chase" *New York Times* November 10, 2015.

[16] *Cybersecurity | Understanding cybercrime: Phenomena, Challenges and Legal Response*, ITU Telecommunication Development Sector, November 2014

[17] *Comprehensive Study on Cybercrime*, UNODC, February 2013

[18] *The Use of the Internet for Terrorist Purposes*, UNODC, 2012

[19] *Comprehensive Study on Cybercrime*, UNODC, February 2015

networks.[20] "An infrastructure is considered to be critical if its incapacity or destruction would have a debilitating impact on the defense or economic security of a state," such as: electrical power systems, telecommunication systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, and emergency services.[21]

Huge disruptions to systems are not necessary in order to achieve catastrophic results. Disruptions caused by a network-based attack goes further than the failure of a single system; as even short interruptions to services can cause huge financial damage to e-commerce business for civil services and military infrastructure and services, alike.[22] Ransomware attacks, in which individuals and criminal syndicates demand payment to unlock infected computers, against local, regional, and national governments are also increasing in frequency, in large part because many governments have ultimately acceded to these ransom demands.[23] An attack on any one of these critical information structures can prove to be an incredibly dangerous threat to a state, not only due to the consequences of the attack itself, but additionally due to the fact that it makes the person(s) or group behind the crime all the more elusive. Cyber-attacks allow perpetrators to be absent from "the scene of the crime" as they use anonymous communication and encryption technology to conceal their identity while carrying out the attack.

Security firms around the world have been researching endlessly in order to quickly identify and combat these attacks. Several different ones have been found and identified, while others still remain elusive. In 2004, a computer worm, Sasser, was found to be infecting millions of computers around the world. Its reach included many of the major airlines, causing forced cancellation of flights as their computer systems went down. VirusBlokAda, an internet security firm in Belarus, discovered a new, then un-named, malicious software in 2010; this particular software would subsequently become known as Stuxnet, believed to be a joint American Israeli venture that targeted Iranian nuclear enrichment centrifuges. Far more complex than many others, this has more than 4,000 functions. It has been found to target industrial control systems (ICS), particularly those produced by technology company, Siemens, and is distributed through removable drives. It used four zero-day exploits in order to infect the computer systems, primarily located in Iran, Indonesia and Pakistan, with some reports of the software being found in the US and European countries. This software in particular not only highlights the vulnerability of these critical infrastructures as they rely so heavily on computer technology, but also that merely disconnecting a computer or system does not necessarily protect it from attacks, as they can be plugged in.[24]

Who's in your wallet? The financial impacts of cybercrime

Cybercrime is a rapidly rising threat to citizens of the global community. With techniques and methods constantly growing and evolving, it becomes riskier to trudge through the potential

---

[20] *Cybersecurity | Understanding cybercrime: Phenomena, Challenges and Legal Response*, ITU Telecommunication Sector, November 2014

[21] *Cybersecurity | Understanding cybercrime: Phenomena, Challenges and Legal Response*, ITU Telecommunication Sector, November 2014

[22] *Cybersecurity | Understanding cybercrime: Phenomena, Challenges and Legal Response*, ITU Telecommunication Sector, November 2014

[23] Manny Fernandez, David E. Sanger & Mariana Trahan Martinez, "Ransomware Attacks Are Testing Resolve of Cities Across America", *New York Times*, August 22, 2019.

[24] *Cybersecurity | Understanding cybercrime: Phenomena, Challenges and Legal Response*, ITU Telecommunication Sector, November 2014

threats to one's personal data. According to security expert Eugene Kaspersky, more than 49 million cyber-attacks took place in the first quarter of 2014.[25] While the growing number of cyber-attacks is occurring globally, certain areas of the world such as Africa and Brazil[26] seem to be experiencing the growth more than ever.

Internet usage is rising rapidly in Africa, and with it, cybercrime.[27] The growth has been giving criminals incredible ease when attacking users, "creating a new pool of potential victims."[28] Cybercrime has not only grown in number, but it has grown in its means of attack. Cybercrime on the African continent has moved far beyond the notorious 419 email scam, which promised riches in exchange for cash and/or bank details, "with gangs embracing more sophisticated ways to use technology, such as malware and bonnets, to get what they want".[29]

This has made just logging onto the Internet an increasingly perilous task for many, as noted by most of the top security firms worldwide. Security firm Norton has said that 70% of South Africans have fallen victim to cybercrime, compared to 50% worldwide.[30] McAfee, a cyber security firm, reported that cybercrime has cost South African companies more than $500 million USD in 2014.[31] US firms spent an estimated $2 billion USD in 2014 in cybercrime insurance.[35] With the rates for cyber-attacks on the rise, and along with it the cost to users and companies, the need for a solution has never been greater.

The African Union (AU) has approved a convention on cyber security and data protection, in June of 2014, "that could see many countries enact personal protection laws for the first time."[32] A convention such as this could be the starting point that Africa needs in order to protect its citizens from cyber criminals, a protection that they have lacked for some time. However, it has yet to be passed. 15 of the 54 AU member states will need to ratify the text for it to be implemented. Of which none have done so, in over a year since the convention was first introduced. Nevertheless, there is hope that it will happen in the next three to five years.[33]

It is important for it to be ratified sooner rather than later. However, extra care must be taken to make sure no basic human rights, including a prospective right to privacy, are violated in the process. Human rights organization Access, has called on member states "to ratify the convention as soon as possible." Junior policy counsel at Access, Drew Mitnick said "it is critical for countries to adopt cyber security policies that better protect users while respecting their privacy and other human rights."[34] There is a concern that an effort to provide security from cyber-attacks can and will violate a person's rights. Access believes that legislation "would either fail to provide basic protection for user data or allows the government to violate the rights

---

[25] Tom Jackson, *Can Africa fight cybercrime and preserve human rights?*, BBC News, 10 April 2015
[26] Robert Muggah & Nathan Thompson, "Brazil's Cybercrime Problem" *Foreign Affairs* September 17, 2015.
[27] Tom Jackson, *Can Africa fight cybercrime and preserve human rights?*, BBC News, 10 April 2015
[28] Tom Jackson, *Can Africa fight cybercrime and preserve human rights?*, BBC News, 10 April 2015
[29] Tom Jackson, *Can Africa fight cybercrime and preserve human rights?*, BBC News, 10 April 2015
[30] Tom Jackson, *Can Africa fight cybercrime and preserve human rights?*, BBC News, 10 April 2015
[31] Tom Jackson, *Can Africa fight cybercrime and preserve human rights?*, BBC News, 10 April 2015
[35] *The Economist*, "Think of a number and double it" January 17, 2015.
[32] Tom Jackson, *Can Africa fight cybercrime and preserve human rights?*, BBC News, 10 April 2015
[33] Tom Jackson, *Can Africa fight cybercrime and preserve human rights?*, BBC News, 10 April 2015
[34] Tom Jackson, *Can Africa fight cybercrime and preserve human rights?*, BBC News, 10 April 2015

if privacy, expression, and assembly," according to proposed cyber and data protection laws it has tracked across the continent.[35]

Additionally, the Centre for Intellectual Property and Information Technology Law at Strathmore University, Kenya, "believes the convention could limit freedom of expression and allow authorities to intercept private data too easily", which they say could have "substantial negative effects on online economies and social cultures across Africa"[40] Not everyone has such a bleak view on the outcome of the convention. Mitnick, in particular, has applauded the protection of human rights. According to him, "the convention contains a data protection provision covering control of personal data, with a large part of it mirroring the data protection framework and language developed by the European Union."[36]

Nevertheless, the need for legislation that both protects its users while bearing in mind the inherent risk to basic human rights has become a pressing issue. Beza Belaynen, managing director of the African Cyber Risk Institute (ACRI) has expressed such concerns. "Cyber security and cybercrime need a multi sectional approach - cyber security educators, researchers, NGOs, vendors, ethical hackers were supposed to be involved so they could present a multidimensional framework instead of a legal paper."[37]

Combating Cybercrime and the Threat to Privacy

Combating crime in all its forms comes with its own set of challenges. However, the concerns that face those looking to combat cybercrime are particularly unique. International human rights law has a specific concern for the manner in which the state achieves its crime prevention and criminal justice goals. All aspects of the investigation have the potential to engage human rights standards and criminal prosecute law and practice and therefore come under scrutiny from international human rights law.[38]

Challenges that law enforcement confront are frequently founded on privacy-based protections within international and national law. The International Covenant on Civil and Political Rights (ICCPR), the European Convention for Protection of Human Rights and Fundamental Freedoms (ECHR) among others, all have "prohibitions on arbitrary interference with privacy, family, home and correspondence."[39] Privacy rights in international law are not absolute and are therefore subject to limitations. For example, in the ECHR, specifically for "the prevention of disorder or crime," the definition of conditions and circumstances under which investigative powers can be used; the identity of authorizing officials; and the length of time investigative measures may be applied are all critical to the human rights assessment of whether or not criminal investigations that infringe privacy are acceptable as lawful and necessary.[40]

In all parts of the world, in order to determine whether the interference with the privacy, family, home or correspondence is justified, "each investigative measure must be assessed in its own legal and practical context."[41]. This can become problematic to law enforcement and

---

[35] Tom Jackson, *Can Africa fight cybercrime and preserve human rights?*, BBC News, 10 April 2015
[40] Tom Jackson, *Can Africa fight cybercrime and preserve human rights?*, BBC News, 10 April 2015
[36] Tom Jackson, *Can Africa fight cybercrime and preserve human rights?*, BBC News, 10 April 2015
[37] Tom Jackson, *Can Africa fight cybercrime and preserve human rights?*, BBC News, 10 April 2015
[38] *Comprehensive Study on Cybercrime*, UNODC, February 2013
[39] *Comprehensive Study on Cybercrime*, UNODC, February 2013
[40] *Comprehensive Study on Cybercrime*, UNODC, February 2013
[41] *Comprehensive Study on Cybercrime*, UNODC, February 2013

actually impede on their ability to conduct investigations on cybercrime as they tip-toe around privacy-based protections. "Case law from international human rights courts and tribunal emphasizes that procedural protections are critical to respecting privacy in the context of law enforcement investigations."[42] These challenges grow exponentially when the crimes cross borders. "Divergent national privacy approaches will become an increasing challenge in the context of trans-national law enforcement investigations and developments."[43]

Cybercrime frequently crosses borders and thus creates a whole new element to the problem. Terrorist use of the internet is a transnational problem, requiring an integrated response across borders and among national criminal justice systems. This means that in order to effectively investigate instances of cybercrime, a "combination of traditional investigative methods, knowledge of the tools available to conduct illicit activity via the Internet, and the development of practices targeted to identify, apprehend, and prosecute the perpetrators of such acts."[44] Challenges begin to occur when detailing out exactly what those best practices might entail. The investigation and prosecution of cases involving digital evidence require specialist criminal investigation skills, as well at the expertise, knowledge and experience to apply those skills in a virtual environment. "A sound knowledge of the required applicable rules of evidence, and in particular with respect to digital evidence, promotes the collection of sufficient admissible evidence by investigators to support the successful prosecution of a case."[45] This poses a challenge for many states as they may not have the resources required available to them. Governments are also seeking to improve their bilateral and multilateral efforts at cooperation in the fight against cybercrime; in September 2015, China and the United States announced that they would cooperate more closely to prevent and punish cybercrime.[46] This announcement was met with both muted fanfare and considerable skepticism as the US government and businesses have routinely accused China's government of turning a blind eye to, if not directly encouraging and/or sponsoring, daily hacking of US business and government websites.[47]

With all this in mind, there are "a number of challenges and good practices related to the use of investigative measures and cybercrime investigations in general.[48] The starting point for successful investigations is ensuring the capability for timely obtaining subscriber information, such as an IP address, as well as the importance of the careful organization and ordering of investigations have been regarded as good practices. The current investigative challenges, on the other hand, greatly outweigh those good practices. There is a growing need for law enforcement investigations to 'keep up' with cybercrime perpetrators, as well as an increasing level of criminal sophistication: locating electronic evidence, obfuscation techniques, large volumes of data in need of analysis, obtaining data from service providers, etcetera.[49]

In order to assist states in combating instances of cybercrime, the International Multilateral Partnership Against Cyber Threats (IMPACT) provides the needed resources to

---

[42] *Comprehensive Study on Cybercrime*, UNODC, February 2013
[43] *Comprehensive Study on Cybercrime*, UNODC, February 2013
[44] *The Use of the Internet for Terrorist Purposes*, UNODC, 2012
[45] *The Use of the Internet for Terrorist Purposes*, UNODC, 2012
[46] Jim Kerstetter, "Daily Report: China Promises to Work with US to Prevent Cybercrime" *New York Times* September 24, 2015.
[47] Elias Groll, "Will China Deliver on its Promise to Stop Hacking American Business" *Foreign Policy* September 25, 2015.
[48] *Comprehensive Study on Cybercrime*, UNODC, February 2013
[49] *Comprehensive Study on Cybercrime*, UNODC, February 2013

states who need it. A key partner of the ITU, IMPACT is modeled after the Centers for Disease Control and Prevention (CDC), Atlanta. It coordinates the resources of governments, industry leaders, and individuals to go beyond political borders. ITU-IMPACT has become the largest cybersecurity alliance of its kind with a total of 152 countries now formally part of the coalition and strong partnership. Through this, it enables "governments and stakeholders with vested interests in cybersecurity to converge, connect, and collaborate for a tighter and a more cohesive move forward in the defense against adversaries online."[50] Efforts such as the one by IMPACT are crucial towards combating cybercrime effectively.

UN System Actions

There are a number of groups working towards combating cybercrime in all its forms. The UNODC, in particular, promotes long-term and substantial capacity building in the fight against cybercrime through supporting national structures and action.[51] "The agency has emphasized that developing countries lack the capacity to combat cyber-attacks and other forms of cybercrime." Under its program for cybercrime, the UNODC "has been delivering technical assistance to law enforcement authorities, prosecutors, and judiciary in three regions of the world:" Eastern Africa, South East Asia, and Central America. Legal loopholes and weak security measure are exploited in such countries of the world perpetuate cybercrimes.[52] The UNODC draws upon specialized expertise on criminal justice systems response to provide technical assistance in capacity building, prevention and awareness raising, international cooperation, and data collection, research and analysis on cybercrime.[53]

According to Lungameni, "the main objective of the programme is to respond to identified needs in developing countries by supporting Member States to prevent and combat cybercrime."[54] It works with international partners in carrying out technical assistance, including the International Telecommunication Union (ITU), the Commonwealth Secretariat, the World Bank, Interpol, and Europol.[55]

Other efforts can be found directed and adopted by many of the UN systems, including the General Assembly and the Security Council. In 2006, the General Assembly unanimously adopted the United Nations Global Counter Terrorism Strategy, "representing a milestone in the domain of multilateral counter-terrorism initiatives."[56] In this, Member States resolved "to work with the United Nations with due regard to confidentiality, respecting human rights and in compliance with other obligations under international law", to explore means to coordinate efforts international and regionally to counter terrorism, in all its forms, and to use the Internet as a tool for countering the spread of terrorism, while recognizing that there are states which may

---

[50] *About Us*, International Multilateral Partnership Against Cyber Threats, 2015
[51] *Emerging Crimes*, UNODC, 2015
[52] *DOHA: UN Conference weighs efforts to combat cybercrime, create safer digital world*, UN News Centre, 17 April 2015
[53] *Emerging Crimes*, UNODC, 2015
[54] *DOHA: UN Conference weighs efforts to combat cybercrime, create safer digital world*, UN News Centre, 17 April 2015
[55] *DOHA: UN Conference weighs efforts to combat cybercrime, create safer digital world*, UN News Centre, 17 April 2015
[56] *The Use of the Internet for Terrorist Purposes*, UNODC, 2012
[62] *The Use of the Internet for Terrorist Purposes*, UNODC, 2012
[63] *The Use of the Internet for Terrorist Purposes*, UNODC, 2012

be in need of assistance in this matter.[62] This helped opened the door to international initiatives in the fight against cybercrimes and terrorism. The Security Council has passed resolutions that not only include cybercrimes and terrorism but actually actively work against it. In its resolution 1963 (2010), the Security Council expressed "concern at the increased use, in a globalized society, by terrorists of new information and communication technology, in particular the Internet, for the purposes of the recruitment and incitement as well as the financing, planning and preparation of their activities." The Security Council also recognized the importance of cooperation among Member States to prevent terrorists from exploiting technology, communications and resources.[63]

In May 2015, the UNODC debuted the cybercrime repository[57], "a database of legislation, case law and lessons learned on cybercrime and electronic evidence."[65] The systematic collection and sharing of relevant data about cybercrime will be truly foundational as countries seek to combat a constantly growing and evolving series of digital threats. Delegates to the UNODC may also wish to familiarize themselves with the Global Programme on Cybercrime and their own countries' preparations in advance of the Fourteenth United Nations Congress on Crime Prevention and Criminal Justice in Kyoto, Japan in April 2020.[66]

Conclusion

Technology is making tremendous advances against hunger, disease, and wasteful uses of energy. But it also empowers organized crime and raises the specter of crippling cyber-attacks.

– Jan Eliasson, Deputy Secretary-General

While cybercrime and its prevention is a relatively new and evolving issue, it is not without its own unique challenges. It is important to note that its impact can range from crimes as small as phishing and identity theft all the way to terrorism. Technology will continue to grow, as will the reliance we hold on it; this holds particularly true for information technology and critical infrastructures. Therefore, Internet-related attacks against individuals and States must be included in strategies to prevent and fight cybercrime. According to then UN Secretary-General Ban Ki-moon, "the Internet is a prime example of how terrorists can behave in a truly transnational way; in response, States need to think and function in an equally transnational manner." States must employ cooperative strategies towards the fight against injustice and crime, while maintaining a respect for both the human rights of an individual, and the rule of law. Only through doing so can a true strategy be developed and implemented.

Guiding Questions

1. What are the most important cyber threats facing your country at this time? What legislation and strategies have your government implemented to confront cybercrime and cyber threats? How successful have these initiatives been? What new legislative and security initiatives are your country considering to more effectively deter and/or combat

---

[57] UNODC, "Repository Cybercrime", 2019. Found at: https://sherloc.unodc.org/cld/v3/cybrepo/ [65] UNODC, "Assisting States in their efforts against cybercrime" May 20, 2015. Found at: http://www.unodc.org/unodc/en/frontpage/2015/May/assisting-states-in-their-efforts-against-cybercrime.html [66] UNODC, "14th United Nations Congress on Crime Prevention and Criminal Justice", 2019. Found at:
https://www.unodc.org/congress/

cybercrime? When drafting legislation to combat cybercrime, what privacy safeguards and human rights protections does your government include and/or implement?

2. What efforts have been undertaken regionally and internationally to combat cybercrime and to protect privacy? What steps can be taken to encourage states to cooperate in apprehending and prosecuting international cyber criminals and organized criminal syndicates? How might countries be persuaded to improve cooperation in extraditing cyber criminals?
3. Is existing international law sufficient to address cybercrime? If not, does the UN System need to consider convening an international conference aimed at addressing gaps and/or deficiencies in international law regarding cybercrime? What are the ramifications of state-initiated and/or statesponsored cyber-attacks and cybercrime?
4. How effectively is the Global Programme on Cybercrime being implemented? How might UN member states increase the effectiveness of the Global Programme?
5. What are the appropriate roles for private sector actors and nongovernmental organizations (NGOs) to take in combating cybercrime and cyber-attacks?
6. Do individuals have a right to digital privacy? Has your country passed any recent legislation regarding individuals and digital privacy? If so, are there any generally agreeable international parameters and/or limits to a right to digital privacy? Or are any limits subject strictly to national legislation and jurisdiction?

Resolutions

UN General Assembly (UNGA), "Countering the use of information and communications technologies for criminal purposes", (A/RES/73/186), December 17, 2018.

UN General Assembly (UNGA), "The right to privacy in the digital age" (A/RES/73/179) December 17, 2018.

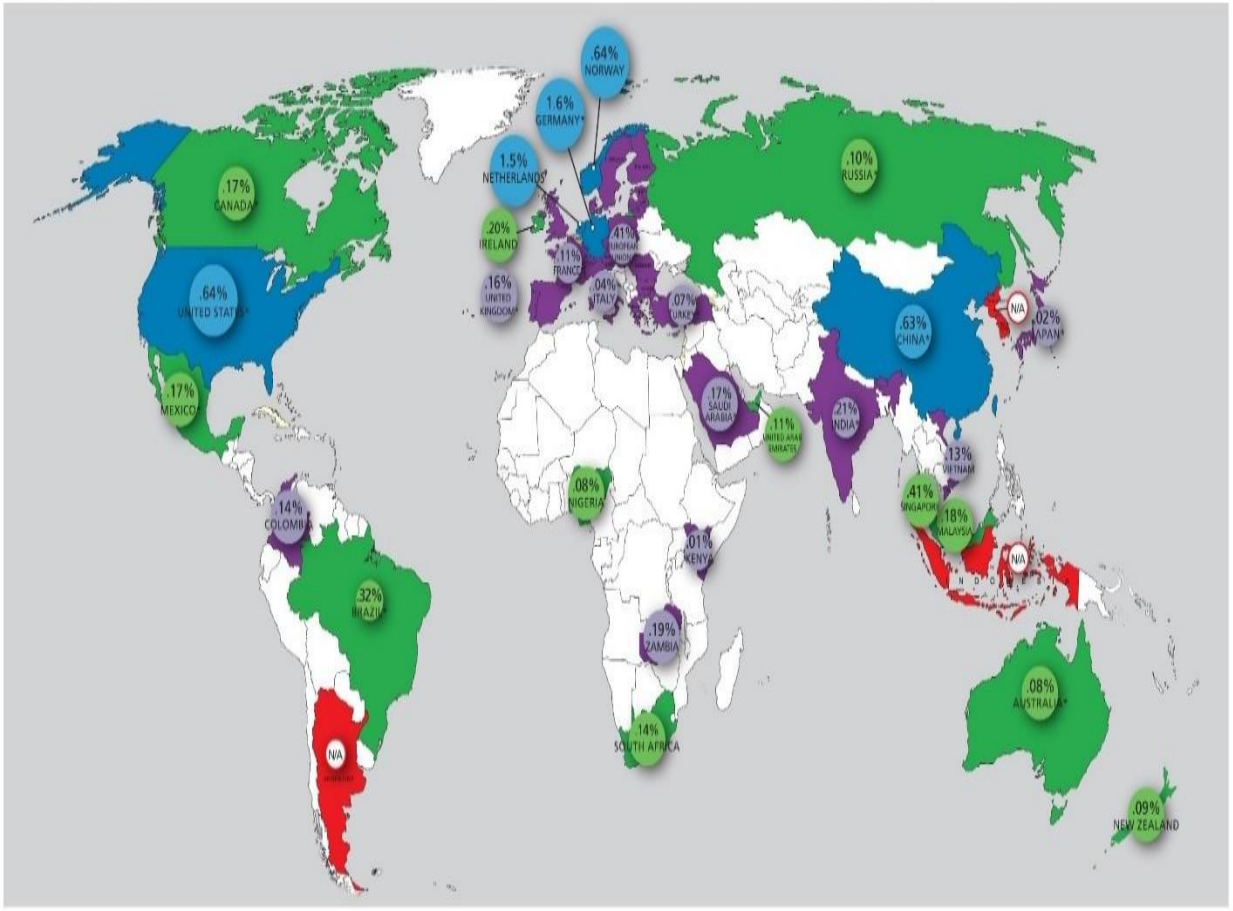
UN General Assembly (UNGA), "Twelfth United Nations Congress on Crime Prevention and Criminal Justice", (A/RES/65/230), December 21, 2010.

UN General Assembly (UNGA), "Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures", (A/RES/64/211), December 21, 2009.

UN Security Council (UNSC), "Threats to international peace and security caused by terrorist acts" (S/RES/1963) December 20, 2010.

McAfee
An Intel Company

CYBERCRIME LOSS AS A PERCENT OF GDP (GROSS DOMESTIC PRODUCT)



Confidence Ranking: Countries Current Tracking of Cybercrime within Their Borders.

- % High Confidence Level
- % Low Confidence Level
- * G-20 Countries
- % Medium Confidence Level
- N/A - Countries currently not measuring cybercrime loss

$445 BILLION
The annual estimated cost to the global economy from cyber crime

200,000+
Jobs lost in the U.S

150,000+
Estimated in Europe