The Question of Cybercrime

Topic Background

Every year, billions of dollars in capital are illegally stolen directly from the pockets of some of society's most vulnerable individuals, but without the victim ever even physically interacting with the perpetrator of their robbery. Norton estimates that over $15 billion U.S. dollars were lost in 2017 to online identity theft incidents alone (a fourfold annual increase), with billions more being lost as a result corporate cybercrime, hacking incidents, and data breaches.[1] In this regard, the global cybercrime industry can amount to a theft of larger proportions than the GDP of a middle-sized economy.

The definitions and boundaries of cybercrime vary across jurisdictions - some organizations tend to treat it as encompassing purely-software based crimes that are carried out completely by means of a computer, i.e. online information theft, malware, or blackmail. However, in recent years, many governments and agencies have expanded their definition of cybercrime to include physical, often violent crimes that involve technology and the internet more broadly. The Canadian government, for example, has expanded how they define cybercrimes to also include crimes wherein there is "usage of computers as a tool used to commit a material component of the offence."[2]

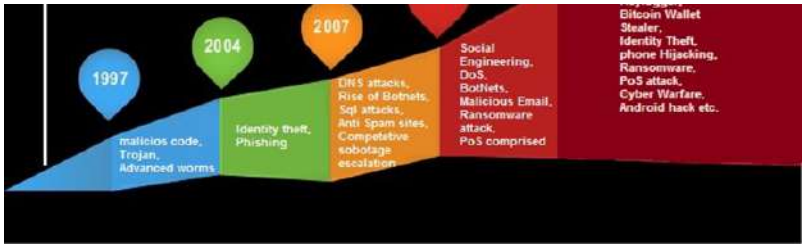
Conceptions and limits of the cybercrime industry have also changed with the waves of technological progress and innovation. The first instance of a "cybercrime", for example, was relatively harmless. It occurred in the early 1980s, when the original cybercriminals were able to use computers to illegally harness telephone networks to make free long distance calls using what was known as a "creeper" virus.[3] Soon after, the first more tangibly harmful virus was (albeit

[1] "10 cyber security facts and statistics for 2018". Norton. https://nr.tn/2pHuWs5
[2] "Cybercrime overview". Global Affairs Canada. https://bit.ly/2Tzsbr0
[3] "Evolution in the world of cybercrime". The Infosec Institute. https://bit.ly/302DpXf

accidentally) sent out in the form of the "Morris worm", which capitalized on flaws in coding and weak passwords to such an extent that a computer could shut itself down. By the 2000s, identity theft, phishing, malicious email scams, and ransomware were on the rise; today, data leaks, online currency theft and manipulation, and DDOS attacks dominate news cycles, signalling how far cybercrime has come in a rapid time frame.

From an expanded perspective, cybercrime can also directly physically impact victims in ways that transcend the internet itself. Thousands of young boys and girls under the age of 18 are trafficked into child pornography rings each year by means of the illicit "dark web", where images of them can be published online for illegal purchase and viewing; the University of Massachusetts Amherst estimated that there were over 840,000 unique downloads of this content between 2011 and 2014.[4]

Source: Infosec Institute.



Another form of cybercrime that can have tangible impacts on the health and well-being of victims is the issue of identity theft. The Identity Theft Resource Center (ITRC) reports that of each of the estimated fifteen million individual instances of identity theft that occur annually, an average of $500 is lost.[5] In the worst instances of identity theft, however, entire livelihoods can be jeopardized, especially if the crime is not realized or reported immediately by the consumer.

Data breaches and the illegal accessing of private consumer information are another dimension of cybercrime that have undergone a strong insurgence in recent years. Notably, numerous social media companies have experienced major data breaches, putting sensitive consumer information such as email passwords, browsing histories, and potentially even payment information in the hands of third-party cybercriminals or organizations. A key example of this is the Yahoo! data breaches between 2014 and 2016, in which thousands of passwords were illegally leaked, resulting in millions of dollars in damages.[6] One different, yet equally - if not more - impactful information leak involved the Facebook Cambridge Analytica scandal, wherein the non-consensual harvesting

[4] "The scourge of child pornography". Federal Bureau of Investigation. https://bit.ly/2KzDPzj
[5] "The 2018 impact of data breaches and cybercrime". Identity Theft Resource Center. https://bit.ly/2KAlCkU
[6] "Yahoo! must pay 50m in damages for security breach". Cnet.com. https://cnet.co/2yvnTYm

of millions of users' data over the course of years by the firm Cambridge Analytica for non-transparent political purposes.[7]

Lastly, another major dimension of cybercrime involves corporate crimes committed against organizations, institutions, and companies, as opposed to individuals. These crimes can often have the most widespread impacts on societies, as companies providing key services can be brought to a standstill. One contemporary example of such an attack occurred in Spain in 2018, when the Bank of Spain's online servers were intermittently downed after a series of "distributed denial of service" (DDOS) attacks, wherein their systems were flooded with traffic beyond their bandwidth capacity.[8] These kinds of attacks exemplify the societal, broader-scale threats that exist in the realm of cybercrime; delegates ought to consider their prevention, in addition to other forms of cybercrime previously mentioned, when crafting their resolutions.

Past International Actions

The question of cybercrime is in many ways interconnected with SDG 9: Industry, Innovation, and Infrastructure, which seeks to "build resilient infrastructure, promote inclusive and sustainable industrialization, and foster innovation" for all. Cybercrime challenges the resiliency of an oft-forgotten, yet crucial form of infrastructure: online infrastructure and data security. International efforts undertaken in recent years have focused on ensuring the most cost-effective cybersecurity measures possible are enacted in order to achieve sustainable development.

The principal United Nations Agency combating the growth of cybercrime is the United Nations Office on Drugs and Crime (UNODC). As cybercrime rates have risen, the UNODC has committed more resources in turn to innovation and prevention initiatives in this realm: it operates the United Nations Global Programme on Cybercrime, whose mandate is to "assist member states in their cyber-related crimes through capacity building and technical assistance".[9] The programme also includes the UNODC Cybercrime Repository, which serves as a central database for cybercrime laws, capabilities, and assessments.[10]

One of the most essential international agreements on the subject of cybercrime comes in the form of a document passed by the United Nations General Assembly itself: UNGA Resolution 65/230 was adopted on 21 December of 2010, and recommended a framework for states to make use of increased technical assistance and training from resources in the private sector in order to increase the prevention capacities of state and national authorities.[11] The resolution also successfully called

---

[7] "The Facebook and Cambridge Analytica scandal, explained with a simple diagram". Vox. https://bit.ly/2pCFpEJ

[8] "Bank of Spain hit by DDOS attack". Bankinfosecurity.com. https://bit.ly/2wveXQT

[9] "UNODC Global Programme on Cybercrime". UNODC. https://bit.ly/2AN6DvP

[10] United Nations Office on Drugs and Crime Cybercrime Repository. https://sherloc.unodc.org/cld/v3/cybrepo/

[11] General Assembly Resolution 65/230, "Twelfth United Nations Congress on Crime Prevention and Criminal Justice". https://bit.ly/2KAt6Vl

for the establishment of the Open-ended Intergovernmental Expert Group, which organizes semi-regular Expert Group Meetings (EGMs) aimed at facilitating the sharing of studies, counter-strategies, and information relating to the problem of cybercrime itself.[12]

One major civil society organization that is also active in the fight against cybercrime is the Cyber Peace Foundation (CPF), which incorporates more than 12,000 expert members who constitute a grassroots network advocates for the promotion of cyber-peace and software resiliency online.[13] They do so by operating a "Cyber Peace Corps", which involves members serving as points of contact for governments to reach out to as mediators in solving complex online cybercrimes and cyber-disputes.

Possible Solutions

Efforts to bridge the gap between the high internet accessibility of the developed world and the low to non-existent rates of access throughout the developing world are valiant and will come with an abundance of positive effects, but will also inevitably be accompanied by new challenges in the form of expanded avenues for potential cybercrimes. Delegates should seek to understand this delicate balance between a distinct need for cybersecurity, and a simultaneous goal to expand online networks to developing regions in ways which must necessarily be cost-effective and potentially less secure relative to existing networks; such a balance must be at the forefront of all potential solutions.

When drafting potential solutions, it is also important to consider the disproportionate ways in which cybercrime can impact the most vulnerable sectors of society. Globally, the elderly have been identified as the demographic group most likely to be worst impacted by cybercrimes, particularly in the form of identity theft and user-driven account breaches.[14] In addition to the challenges of senility, this vulnerability stems from a root underlying cause of a lack of education, which can be attributed to generational differences in quality of education when it comes to online safety. Delegates should therefore consider the merits of a "bottom-up" approach to mitigating cybercrime rates through education initiatives, as well as ponder how the link between quality education and likelihood of cybercrime could impact developing nations undergoing emergent processes of online economic integration. How should cybercrime protections accommodate the differing needs of the West and the global south?

Another key dynamic of cybercrime which requires addressing is the issue of child pornography and other forms of violence facilitated by means of the internet. Civil society actors such as the Innocent Justice Foundation have documented that there are direct correlations between the

---

[12] "Open-ended Intergovernmental Expert Group Meeting on Cybercrime". UNODC. https://bit.ly/31GIF3n
[13] "About us". Cyberpeace. https://www.cyberpeace.org/about-us/
[14] "The eldery most at risk from cyber-crime". E&T: Engineering and Technology. https://bit.ly/2NeGX5x

presence of anti-crime task forces within a jurisdiction and the number of cybercrimes which trace back to that same area. Despite this, online child crime task forces are relatively rare outside of the continental United States and Western Europe, and are chronically underfunded where they are present.[15]

The role played by corporations in the growing cybercrime industry should also not be neglected. Many argue that corporations such as Yahoo! and Facebook which were found to cut corners in terms of assuring data security need to be continuously sure to have both politico-economic incentives for implementing cyber-secure protection mechanisms, as well as internationally consistent consequences for failing to do so if meaningful progress is to be achieved. Such incentives and consequences must be further balanced to account for the diversity of country policies, as certain states may be more or less content to commit to concrete sanction and incentivization targets for often influential, multinational corporations.

On the whole, cybersecurity is an increasingly relevant concern that transcends national borders and requires immediate addressing by means of an approach which is both consistent and holistic in addressing all aspects of cybercrime. Delegates should strive to be inclusive and considerate in drafting any such approach.

Further Research

- United Nations Office on Drugs and Crime: Topic of Cybercrime
- Sustainable Development Goal #9: Industry, Innovation, and Infrastructure
- UNGA Resolution 65/230: Crime Prevention and Criminal Justice
- Website of the Cyber Peace Foundation

Worksheet Questions

1. What is one definition of cybercrime?
2. According to historians, was the first ever 'cybercrime' to be committed?
3. What does "DDOS" mean?
4. What is the Cyber Peace Corps and how does it work?
5. Which demographic group was mentioned as having a higher risk of being cybercrime victims?

[15] "What we can do to stop it". The Innocent Justice Foundation. https://bit.ly/2MifaRX