Forum: Commission on Crime Prevention and Criminal Justice (CCPCJ)

Issue #1: The Question of Cybersecurity to Tackle Doxxing and Information Insecurity

Student Officer: Ana Queen

Position: Chair of the Commission on Crime Prevention and Criminal Justice (CCPCJ)

Introduction

In the 21st century, technology has resulted in strong 'interconnectedness' between individuals from all across the globe. This can give rise to many challenges regarding a person's personal and information security: It can be alarmingly easy to find the personal information of online figures, like influencers, celebrities, or anyone on any social media platform. Because of this, people can access all kinds of information about an individual, even if that person did not consent to this possession of their information or if they haven't posted anything about themselves. According to a 2020 survey by the Pew Research Center, roughly 4 in 10 Americans have experienced some form of online harassment abuse: Even without somebody having any social media, another person can non-consensually publish their information online, exposing them to cyber insecurity. In light of this escalating, severe conflict, there are thousands of people affected every year. Addressing the threat of document dropping (or "doxxing") and information insecurity has become essential in ensuring the protection of personal, government, and corporate data.

As stated by the Identity Theft Resource Center (ITRC), the number of reported U.S. data compromises in 2023 has surpassed the previous annual record by 14%, totaling 2,116 incidents. This includes 733 compromises reported in the third quarter alone, exceeding the previous annual record of 1,862 events in 2021, impacting 353 million total victims. The repercussions of these incidents can affect a wider scope beyond the individual victim, but impact governments and large organizations alike. While there are many ways to enforce cybersecurity, such as multifactor authentication measures or implementing robust encryption, people will still go out of their way to find loopholes around any laws that may be imposed against them. A collaboration between countries, international organizations, governments, and IT companies is essential to establish worldwide agreements on cybersecurity standards and protocols to keep these corporations safe and any individual part of this collective society. Although this conflict parallels today's rapidly evolving technology, it also grows alongside the domain of possible solutions.

Definition of Key Terms

Technology: The functional application of scientific knowledge for practical purposes, mainly in the industry.

Cybersecurity: The practice of protecting systems, networks, and programs from any form of digital attacks

Cyber Aggression: Any conduct aimed to intentionally harm people online/digitally who perceive such acts as offensive, derogatory, or dangerous.

Cybercrime: Criminal activities are carried out through computers or the Internet.

Data Breaches/Leakages: A security incident in which unauthorized parties gain unwanted access to sensitive, personal, or confidential information.

Dropping Documents (or "Doxxing"): To search for and publish personal or confidential information about a specific person or group of people online without their consent.

Identity Theft: the fraudulent claim and use of a person's private identifying information, including the acquisition of their name, social security number, or credit card number.

Personal Information: Unique and exclusive information used to identify, locate, or contact an individual.

Harassment: Any unwanted behavior that makes an individual feel uncomfortable, humiliated, or distressed.

General Overview

The ongoing issue of cyber information insecurity can be measured and examined through multiple perspectives and instances. One of the primary triggers for information insecurity is the rapid advancement of digital technologies, online programs, and services. As individuals and organizations have become more dependent on these tools, cybercriminals have found new ways to gain unauthorized access to sensitive information. This has led to a surge in high-profile data breaches, identity thefts, and other forms of cyberattacks that have shaken the security of internet users everywhere. Especially in recent years, the rise in cybercrime has been exacerbated due to growing technologies and digital programs. According to a report by the Center for Strategic and International Studies (CSIS), cybercrime costs the global economy an estimated $1 trillion annually. The impact of cyber information insecurity extends beyond the financial aspect, as it can also inflict psychological and emotional harm on victims. Instances of doxxing, where personal information is maliciously disclosed online, can lead to stalking, harassment, and even physical threats, leaving individuals feeling vulnerable and unsafe in their own digital spaces. These occurrences have the potential to shatter lives, disrupt families, and undermine the fundamental rights and freedoms that individuals should enjoy in the digital age. This highlights the significant financial burden and societal impact of instances such as data breaches, doxxing, and cyberattacks.

Data Breaches

Data breaches involve unauthorized access to sensitive information stored on computer systems, leading to the exposure of personal or corporate data. They should be accounted for due to their potential to cause financial loss and violate individuals' privacy rights. According to the 2022 IBM Cost of a Data Breach Report, the average cost of a data breach reached a record high of $4.35 million globally in 2022, a 2.6% increase from the previous year. The report also found that the United States experienced the highest average cost of a data breach at $9.44 million. Globally, the healthcare industry suffered the highest average cost of a data breach at $10.1 million (IBM, 2022). Moreover, a study by Risk Based Security revealed that in 2021, there were 5,258 publicly reported data breaches, exposing over 22 billion records, a 68% increase from 2020 (Risk Based Security, 2022). These trends show the growing conflict of data breaches and shine light on the prioritization of enforcing and improving cybersecurity measures to protect sensitive information to prevent fines, lawsuits, reputation, and unemployment.

Dropping Documents ("Doxxing")

Doxxing has become a growing concern in the digital age, especially since anyone at any time can obtain information on an online figure(s). Occasionally, it can involve citizen detectives taking the law into their own hands. In other, worse instances, however, the attacks can be more severe; including identity theft, the sharing of intimate images, or the practice known as "SWATting":

where perpetrators report made-up crimes, hoping to have a target's home raided by armed police. A study by the Anti-Defamation League found that in 2021, 44% of Americans reported experiencing some form of online harassment, with doxxing being one of the most common tactics used (Anti-Defamation League, 2022). Furthermore, a survey by the Pew Research Center revealed that 25% of young adults aged 18-29 have been doxxed, with women and marginalized groups disproportionately targeted (Pew Research Center, 2021). This form of online harassment amplifies the room for mistreatment and prejudice against marginalized groups, including women and other minorities. Some of the many consequences of doxxing can be severe and disproportionately long-term, ranging from reputational damage and financial loss to persisting threats and safety risks.

Cybercrime & Cyberattacks

Cyberattacks refer to assaults launched using computers against single or multiple computers or networks. Cybercrime, on the other hand, generally encompasses a wide range of criminal activities that are carried out using digital devices and/or networks. Both cybercrime and cyberattacks have become very prevalent in recent years, causing economic and societal harm. As opposed to doxxing, cybercrime affects a wider scope and demographic of people, usually organizations, firms, and companies as opposed to individuals or particular groups. According to a report by Cybersecurity Ventures, global cybercrime costs are projected to reach $10.5 trillion annually by 2025, a 300% increase from 2015 (Cybersecurity Ventures, 2020). Additionally, a study by the Center for Strategic and International Studies revealed that the Asia-Pacific region experienced the highest number of cyberattacks, accounting for 45% of global incidents (CSIS, 2021), showing the scale to which this conflict is extensive in present time.

Major Parties Involved and Their Views

United States

In January 2024, SafeHome.org conducted an online survey of 1,003 adult American internet users, which emphasized the repercussions of doxxing attacks and the large shadow or fear they cast over many Americans. While four percent of the participants have been doxxed, 93 percent are concerned it might happen to them. Nearly half of the adults expressed extreme concern about the negative consequences of doxxing. The U.S. has been at the forefront of global cybersecurity efforts, given its technological prowess and a significant stake in internet governance. For example, some states have anti-doxxing laws, such as Illinois' law, focusing on civil liability. The country has taken various measures to ensure the safety of its citizens.

Russia

Russia was found to have accidentally doxxed its secret military bases and spies. On one hand, the country has been accused of engaging in cyberattacks that were possibly funded by the state and disinformation campaigns. For example, anonymous hackers have amassed vast amounts of data on Russian assets, spreading propaganda and targeting important state institutions. However, Russia has also experienced incidents where its own sensitive information has been exposed by accident: A noteworthy example is the extensive report that detailed a 434-page document containing the addresses of Russia's military bases, which was accidentally leaked online. This report uncovered how Russia's secretive military and intelligence sites were exposed through public electricity consumer lists, notably on Moscow City Hall's website.

China

China has suffered various cyberattacks that put organizations and citizens at risk. For instance, how a doxxing campaign released the photos, full names, and personal contact details of people who allegedly took part in Hong Kong's 2019 protest movement. This represents a blatant violation of individual privacy and a concerning abuse of power by the Chinese authorities regarding cybersecurity in the country. Additionally, China has implemented a broader system of digital control/surveillance over its citizens, utilizing advanced technologies and measures to monitor online activity and restrict access to information. The government does this mainly for political reasons, such as limiting political opposition and censoring events unfavorable to the CCP, such as the 1989 Tiananmen Square protests and massacre, pro-democracy movements in China, the persecution of Uyghurs in China, and human rights in Tibet. These actions by the Chinese government highlight a relationship between national security, technological advancement, and, arguably, fundamental human rights in the face of these cyber conflicts.

United Kingdom

Laws such as the Protection from Harassment Act and the Malicious Communications Act in the UK offer legal resources to individual victims of cyberattacks, data breaches, and online harassment. Furthermore, the UK's new Online Safety Act empowers victims to seek the removal of posts containing their personal information. These are a few ways in which the government takes a stance to actively enforce cybersecurity. By enacting these comprehensive legal frameworks, the UK government has demonstrated a commitment to stand against the harmful consequences of cyber information insecurity on its citizens.

Israel

Israel has taken a strong approach in addressing the challenges arising from cyber insecurity. The country has established a robust National Cyber Directorate (NCD), which coordinates the government's cybersecurity strategy and works closely with the private sector to develop innovative solutions. One of Israel's key initiatives is the establishment of the National Cyber Security Authority (NCSA), which serves as the national computer emergency response team responsible for monitoring and responding to cyber incidents and providing guidance/support to possible targets and victims. Israel has also engaged in various ‘collateral’ initiatives, such as the Global Cybersecurity Forum, where it has shared its expertise and advocated for the development of common standards and norms for responsible state behavior in cyberspace. However, many citizens are concerned about the use of surveillance technologies and the targeting of opposition groups and human rights activists, both within Israel and, importantly, in the occupied Palestinian territories.

Timeline of Events

Date	Description of event
Late 1990’s	Early doxxing occurred on Usenet forums, including users circulating lists of potential/suspected neo-Nazis.
1998	The “Morris Worm” was when a graduate student in computer science at Cornell launched the world's first computer worm that replicated itself on other internet-connected devices, causing them to shut down.
2002	First recorded data breach; snagging 250,000 social security numbers swiped from a State of California data hub.

2007 TJX Companies reveal 45.6 million card numbers stolen over 18 months, one of the worst-ever data losses at the time.

2013 Target data breach, where cybercriminals stole 40 million credit and debit records and 70 million customer records.

2014 Hackers accessed the credit card information of over 130 million customers of the payment processing company Heartland Payment Systems.

2017 The Charlottesville rally in Virginia, where counter-protesters and activists doxxed and publicly identified several participants.

2021 A ransomware cyberattack on the Colonial Pipeline, a major fuel pipeline in the United States, negatively impacted computerized equipment managing the pipeline.

2023 A massive data breach on Twitch took place, leading to the release of the company's source code and financial information.

2024 Harvard students are doxxed upon writing an anti-Israel letter.

UN Involvement, Relevant Resolutions, Treaties and Events

- Resolution 55/63 “Combating the criminal misuse of information technologies” (2000)
    - This resolution condemned criminal misuse of information technologies and called for international cooperation to address cybercrime, ensuring fostered international cooperation for crime prevention.
- Resolution 57/239 “Creation of a global culture of cybersecurity” (2003)

    - This resolution stresses global cooperation for cybersecurity upon the growing reliance on information technologies, including awareness, responsibility, and responses.
- Resolution 58/199 "Creation of a global culture of cybersecurity and the protection of critical information infrastructures" (2004)
    - This resolution emphasizes the need for cooperation to protect critical information infrastructures, stressing awareness and sharing best practices to bridge the digital division, mitigating unequal access to technology.
- Resolution 64/211 "Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures" (2010)
    - This resolution calls for global collaboration as a response to protect information infrastructures and the need to bridge the digital divide, encouraging countries to evaluate and therefore enhance their cybersecurity measures using a voluntary self-assessment tool.
- "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" (2015)
    - The UN established the "UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", which produced several reports on the norms and principles for responsible behavior in cyberspace.
- UN General Assembly Resolution 73/266 (2018)
    - Established a Group of Governmental Experts (GGE) on advancing responsible state behavior in cyberspace in the context of international security or criminal and terrorist purposes.
- Budapest Convention on Cybercrime (2001)

    - An international treaty that establishes legal guidelines for addressing various forms of cybercrime, including unauthorized access, data interference, and system interference.
- UN GGE Reports (2010, 2013, 2015, 2021)
    - Reports from the UN Group of Governmental Experts have provided recommendations on norms, rules, and principles for responsible state behavior in cyberspace.

Evaluation of Previous Attempts to Resolve the Issue

The United Nations has made several attempts to address the issue of doxxing and information insecurity through various resolutions and initiatives over the past two decades. While these efforts have laid out a strong foundation to work with, the challenges of cybercrime and the protection of critical information infrastructures suggest that more comprehensive and coordinated action is still needed.

The early UN resolutions, such as Resolution 55/63 (2000) and Resolution 57/239 (2003), recognized the growing threat of criminal misuse of information technologies and called for international cooperation to combat cybercrime and foster a global culture of cybersecurity.

Building on this foundation, Resolution 58/199 (2004) and Resolution 64/211 (2010) further highlighted the importance of protecting critical information infrastructures and bridging the digital divide to ensure equal access to technology and security measures. The establishment of the UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security in 2015 was a significant step, as it provides reports on norms and principles for responsible behavior in cyberspace.

The Budapest Convention on Cybercrime (2001), an international treaty, has also been an important tool in establishing legal guidelines for addressing various forms of cybercrime, including doxxing and information insecurity. However, the limited number of signatories to the convention (currently 66 countries) suggests that more widespread adoption and implementation are still needed.

The most recent UN General Assembly Resolution 73/266 (2018) further enforces the need for a new and improved, coordinated approach, as it established a new Group of Governmental Experts to advance responsible state behavior in cyberspace, specifically in the context of international security or criminal and terrorist purposes.

While the UN's efforts have laid important groundwork, the challenges of doxxing, information insecurity, and the evolving nature of cybercrime indicate that more sustained and trustworthy action is required in order to properly mitigate this modern-world conflict. Strengthening international cooperation, fostering a global culture of cybersecurity, and ensuring the protection of critical information infrastructures should remain key priorities in the UN's continued efforts to address these pressing issues.

Possible Solutions

Strengthening Cybersecurity Regulations and Enforcement

Governments and organizations should work together to develop and enforce more robust cybersecurity regulations and standards. This could include mandating minimum security requirements for organizations that handle sensitive data, imposing stricter penalties for data breaches and cybercrime, and empowering regulatory bodies to conduct regular audits and enforce compliance. By creating a more stringent legal and regulatory framework, the costs and consequences of failing to protect critical information infrastructures would increase, which incentivizes organizations to prioritize cybersecurity as well as hold perpetrators accountable to avoid dealing with the enforced consequences and regulations of cybersecurity.

Enhancing Public-Private Collaboration and Information Sharing

Effective cybersecurity requires close collaboration between the public and private sectors. Governments should establish secure platforms and protocols for the timely sharing of threat intelligence, best practices, and incident response strategies with private companies and industry groups. This would enable a more coordinated and proactive approach to identifying and mitigating cyber threats and therefore help prevent the spread of this conflict. Additionally, public-private partnerships should be leveraged to develop effective cybersecurity training programs and awareness campaigns to educate both businesses and the public on the evolving landscape of cyber risks.

Investing in Cybersecurity Research and Innovation

Governments and the private sector should allocate significant resources towards cybersecurity research and development, with a focus on emerging technologies and innovative approaches to data protection, identity management, and threat detection. By funding research, supporting cybersecurity startups, and fostering a culture of innovation, nations, and governments can stay ahead of the rapidly changing tactics and tools used by cybercriminals. This investment in cybersecurity solutions will be crucial in strengthening the resilience of infrastructure and therefore safeguarding against the growing threat of cyberattacks and crimes.

Enforcing Educational Opportunities Regarding Cybersecurity

Lastly, governments may provide comprehensive training and learning opportunities regarding appropriate cybersecurity prevention measures and reactions. This could involve integrating cybersecurity curricula into school and university programs and launching public awareness campaigns to reach a wider audience. By furnishing individuals and organizations with the knowledge to navigate these potential cyber threats, possible victims can prevent and mitigate the impact of doxxing, data breaches, and other forms of cyber information insecurity.

Sustainable Development Goal (SDG)

This issue relates to the United Nations' Sustainable Development Goal (SDG) 16, which promotes peace, justice, and strong institutions. Strengthening cybersecurity to help stop or prevent doxxing and information insecurity contributes to a safer and more secure online environment, essentially protecting individuals' rights to privacy and freedom of expression. Doxxing and cyberattacks pose significant threats to individual privacy and the fundamental human rights of freedom of expression and association. This issue's persistence contributes to conflict, injustice, and the weakening of institutions and organizations, spotlighting the urgency to address this discord on a global scale.

Bibliography

"2024 Data Breach Investigations Report." *Verizon Business*, www.verizon.com/business/resources/reports/dbir/. Accessed 31 May 2024.

"A/RES/55/63 General Assembly." *United Nations*, United Nations, 22 Jan. 2001, www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf.

"Cost of a Data Breach 2023." *IBM*, www.ibm.com/reports/data-breach. Accessed 31 May 2024.

"Data Breach." *Wikipedia*, Wikimedia Foundation, 18 May 2024, en.wikipedia.org/wiki/Data_breach#:~:text=The%20first%20reported%20breach%20was,data%20breaches%20are%20never%20detected.

"Healthcare and Finance Suffer Most Cyberattacks." *MSSP Alert*, BlackBerry Cybersecurity, 20 Dec. 2023, www.msspalert.com/native/healthcare-and-finance-suffer-most-cyberattacks.

Hudson, David L. "Doxxing, Free Speech, and the First Amendment." *The Foundation for Individual Rights and Expression*, www.thefire.org/research-learn/doxxing-free-speech-and-first-amendment#:~:text=State%20laws%20addressing%20doxxing&text=Some%20state%20laws%20actually%20use,law%2C%20focus%20on%20civil%20liability. Accessed 31 May 2024.

Hulsey, Lynn. "2023 Will Go down for Record-Setting Number of Data Breaches." *Governing*, Governing, 23 Feb. 2024, www.governing.com/management-and-administration/2023-will-go-down-for-record-setting-number-of-data-breaches.

Jones, Corrin. "Warnings (& Lessons) of the 2013 Target Data Breach." *Red River*, 26 Oct. 2021, redriver.com/security/target-data-breach#:~:text=What%20Happened%20During%20the%20Target,was%20one%20of%20the%20largest.

Kamel, George. "What You Need to Know About Data Breaches." *Ramsey*

Solutions, 14 May 2024, www.ramseysolutions.com/insurance/data-breach-impacts#:~:text=But%20any%20data%20breach%20can,150%20million%2C%20to%20be%20exact.

Lewis, James Andrew, et al. "The Hidden Costs of Cybercrime." *Center for Strategic & International Studies*, 9 Dec. 2020, www.csis.org/analysis/hidden-costs-cybercrime.

Maayan, Gilad. "Five Years Later, Heartbleed Vulnerability Still Unpatched." *ThreatDown by Malwarebytes*, 12 Sept. 2019, www.threatdown.com/blog/five-years-later-heartbleed-vulnerability-still-unpatched/.

Miller, Leila. "How We Identified White Supremacists after Charlottesville." *PBS*, Public Broadcasting Service, 7 Aug. 2018, www.pbs.org/wgbh/frontline/article/how-we-identified-white-supremacists-after-charlottesville/.

"Online Hate and Harassment: The American Experience 2022." *You Are Being Redirected...*, 20 June 2022, www.adl.org/resources/report/online-hate-and-harassment-american-experience-2022.

"Q3 2023 Data Breach Analysis: Record Smashed! How Many Data Breaches Will Be Reported In 2023?" *Identity Theft Resource Center*, www.idtheftcenter.org/wp-content/uploads/2023/10/20231011_Q3-2023-Data-Breach-Analysis.pdf. Accessed 31 May 2024.

"Q3 2023 Data Breach Analysis: Record Smashed! How Many Data Breaches Will Be Reported In 2023?" *Identity Theft Resource Center*, www.idtheftcenter.org/wp-content/uploads/2023/10/20231011_Q3-

2023-Data-Breach-Analysis.pdf. Accessed 31 May 2024.

Radauskas, Gintaras. “Russia Mistakenly Doxxes Its Own Secret Bases and Spies.” *Cybernews*, 14 Nov. 2023, cybernews.com/news/russia-leaks-secret-bases-spies-locations.

Sheridan, Max. “Doxxing Statistics in 2024.” *SafeHome*, 2 Apr. 2024, www.safehome.org/family-safety/doxxing-online-harassment-research/.

“Significant Cyber Incidents: Strategic Technologies Program.” *CSIS*, www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents. Accessed 31 May 2024.

“UN Resolutions.” *ITU*, www.itu.int/en/action/cybersecurity/Pages/un-resolutions.aspx. Accessed 31 May 2024.

“United Nations Digital Library System.” *United Nations*, United Nations, 22 July 2015, digitallibrary.un.org/.

Vogels, Emily A. “The State of Online Harassment.” *Pew Research Center*, Pew Research Center, 13 Jan. 2021, www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/.

Vogels, Emily A. “The State of Online Harassment.” *Pew Research Center*, Pew Research Center, 13 Jan. 2021, www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/.

Zifei, Chen. “Doxxing Campaign Targeting Hong Kong Protesters Had China Links: Report.” *Radio Free Asia*, 14 July 2023, www.rfa.org/english/news/china/hk-protesters-doxxing-07142023130019.html.

"Гостайна По Электричеству." *Досье*, 2 Oct. 2023, dossier.center/dz-russia/.

Appendix

I. The latest trends, patterns, and statistics related to data breaches
   A. www.verizon.com/business/resources/reports/dbir/

II. The alarming increase in the number of reported data breaches in 2023
   A. www.governing.com/management-and-administration/2023-will-go-down-for-record-setting-number-of-data-breaches.

III. An exploration of the legal implications of doxxing, examining how it intersects with issues of free speech and individual privacy rights.
   A. www.thefire.org/research-learn/doxxing-free-speech-and-first-amendment#:~:text=State%20laws%20addressing%20doxxing&text=Some%20state%20laws%20actually%20use,law%2C%20focus%20on%20civil%20liability

IV. Russian-language article that discusses a data breach that exposed sensitive information about Russia's electricity infrastructure
   A. www.dossier.center/dz-russia/

V. Webpage from the International Telecommunication Union (ITU) that provides an overview of UN resolutions and initiatives related to cybersecurity and the prevention of cybercrime.

   A. www.itu.int/en/action/cybersecurity/Pages/un-resolutions.aspx

VI. An interactive database from the Center for Strategic and International Studies (CSIS) that aims to track major cybersecurity incidents

A. www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

VII. Incident where the Russian government inadvertently revealed the locations of its own secret military installations and personnel

A. cybernews.com/news/russia-leaks-secret-bases-spies-locations