Tech-Enabled Global Cybercrime: Exploitation by Transnational Criminal Organizations (TCOS)

MOLLY COOK-KWENDA
American Public University System

Abstract- ***The research delves into the use of technology by Transnational Criminal Organizations (TCOs) to orchestrate global cyberattacks. The study combines a literature review with case studies to show the interconnection between TCOs' actions and their technological exploits. The findings demonstrate the increasing sophistication of TCOs in carrying out unlawful activities globally. The study also highlights the challenges faced by law enforcement agencies in tracking, apprehending, and prosecuting TCOs involved in cybercrimes. Enhanced international cooperation and robust legal frameworks are critical to combating tech-enabled cybercrimes orchestrated by TCOs. As technology advances rapidly, TCOs find new ways to commit crimes across borders, making it challenging for law enforcement agencies to identify and successfully persecute cybercriminals. To address this trend, the study recommends that the international community work together to strengthen cooperation and establish effective legal frameworks. Successfully reaching this objective will necessitate the joint efforts of multiple parties who must share intelligence, resources, and expertise. It is important to note that technology alone is not responsible for increased cybercrimes; instead, TCOs use technology to carry out illegal activities. Policymakers and law enforcement agencies can utilize these research findings to develop effective strategies to combat these new and evolving forms of global cybercrime.***

Indexed Terms- ***Transnational Criminal Organizations (TCOs), Cyberattacks, Cybercrime***

I. INTRODUCTION

Technological advancements in recent times have entirely transformed the way we function. However, these developments have also led to increased illegal activities globally. Criminal enterprises and technological advancements have converged, creating transnational criminal organizations that engage in global cybercrimes.[1] Available empirical data suggest that criminals involved in illicit activities both online and offline are more likely to be affiliated with loosely associated networks than formal organizations.[2] In addition, extremist groups and insurgents have also begun to use internet technology to steal and finance their activities. For example, Imam Samudra, the convicted mastermind behind the 2002 Bali bombings, urged his followers to engage in credit card fraud to fund their militant activities.[3]

The progress of technology has led to an increase in illegal activities worldwide. Transnational criminal organizations (TCOs) use technological advancements to commit cybercrimes crossing geographical borders and multiple jurisdictions. They thrive on weak governance, socioeconomic vulnerabilities, and corruption, becoming a significant threat to global security.[4] These criminal networks use technology to carry out various illegal activities on a global scale, including hacking, identity theft, fraud, and money laundering.[5] The frequency and complexity of cybercrimes perpetrated by TCOs are increasing, posing a significant threat to individuals, businesses, and governments worldwide. These crimes cause financial losses, compromise sensitive information, erode privacy and trust, and potentially disrupt critical infrastructure systems.[6]

The rise of transnational organized crime (TOC) is a significant concern for global security, posing severe risks to public safety, health, democratic values, and economic stability.[7] Criminal networks have spread their operations to various areas, resulting in previously separated threats converging and causing explosive and disruptive consequences. Corrupting legitimate markets and economic activities can cause severe damage to the global financial system. Business leaders worry that TOC and corruption disadvantage

companies, especially in emerging markets where the rule of law is less reliable. Law enforcement agencies face new challenges in today's rapidly advancing technological era.

The advancements in information technology have led to the emergence of various means of carrying out illegal activities online. This includes using cryptocurrencies like Bitcoin, encryption software, and secure browsing technology like TOR. As a result, dark web markets, such as AlphaBay and Silk Road, have become popular platforms for illegal trade. These marketplaces connect buyers and sellers of illegal goods and services and have been a significant innovation in criminal markets. The conference primarily focused on these dark web markets and their impact on society during its first day.[8]

Transnational Criminal Organizations (TCOs) are increasingly using technology to commit various types of crimes, including cyber warfare, cyber-terrorism, phishing, cyber-espionage, cyber-bullying, money laundering, child pornography, distributed denial of service (DDoS) attacks, and ransomware attacks. As a result, traditional investigation and prosecution methods have become less effective in tracking and capturing these criminal groups. The increasing sophistication and global reach of these organizations make it difficult for law enforcement agencies to locate and apprehend them. Their activities often span multiple countries and involve complex networks of people and resources. Therefore, innovative solutions are needed to overcome the significant obstacles posed by this growing problem.

In the current technological era, law enforcement agencies must develop innovative tactics and allocate sufficient resources to combat the escalating threat of cybercrimes. The proliferation of these criminal activities has led to a significant increase in their size and scope, which poses a severe threat to global safety and stability. The different types of cybercrimes are constantly evolving. With the internet's anonymity and borderless reach, criminals have new opportunities for physical and virtual activities that pose real threats to society.[9] It is crucial to consider the impact of cybercrime on the global economy. Committing such illegal activities can lead to substantial monetary damages, harm to one's reputation, and a decrease in public confidence. Despite numerous attempts to eliminate these networks, they remain a severe threat to global security and stability.

Thorough research and analysis are crucial to comprehending illicit activities. Conducting in-depth research and analysis can provide valuable insights into the intricate tactics and strategies employed by these enterprises and their global impact. Understanding the scope and scale of criminal activities is vital to taking necessary measures to mitigate risks and safeguard against potential harm. The paper highlights the connections between transnational criminal organizations, transnational organized crime, and cybercrime.[10] It highlights the need for continued efforts to combat this growing threat.

Globalization has created opportunities for transnational criminal organizations (TCOs) to leverage the global marketplace to promote illicit activities. TCOs take advantage of the interconnectedness and interdependence of the world's economies, cultures, and populations to engage in the trafficking of drugs, arms, people, and counterfeit goods, as well as money laundering. TCOs are driven primarily by greed and profit, and their activities threaten the national security of the United States and its allies. They compromise the safety of consumers, rob inventors of their intellectual property, deny governments significant tax revenues, and undermine our economies. Globalization has not only increased the scope and scale of TCO activities but has also made it more challenging for law enforcement agencies to detect and disrupt their operations. The need for international cooperation and coordination in the fight against transnational crime is highlighted by thorough research and analysis, which can provide valuable insights into the complex tactics and strategies utilized by these enterprises and their global impact.

Globalization refers to the increased integration and interdependence of economies, cultures, and populations worldwide. It is a phenomenon that results in the blurring of national boundaries and creating a global community. Globalization involves the interconnection and integration of national economies into the global economy through various means,

including the exchange of goods and services through trade, foreign direct investment, the movement of capital, the migration of people, and the dissemination of technology and knowledge across borders. As a consequence of globalization, the world has become more interconnected and interdependent, with countries and individuals increasingly relying on each other for economic growth and development. Globalization has enabled the development of global social and economic relations.[11] However, opening borders and internationalization have also presented new opportunities for criminals in profitable areas like the economy and organized crime.[12]

The advancement of information technology, particularly the use of the Internet as a medium of electronic communication to disseminate information globally, is regarded as a significant driving force behind worldwide integration.[13] Although globalization has increased economic growth, job opportunities, and accessibility to products and services, it raises concerns about inequality, cultural standardization, and environmental degradation. Both cyberspace and globalization have been misused by criminals to carry out cybercrimes with impunity.[14] Globalization has allowed TCOs to exploit the global marketplace for their illicit activities. They engage in trafficking drugs, arms, people, and counterfeit goods, as well as money laundering. TCOs threaten national security by compromising consumer safety, robbing inventors of their intellectual property, and undermining economies. International cooperation plays a vital role in combating transnational crime.

Despite years of research, transnational crime remains a complex social and political phenomenon requiring a more comprehensive understanding. Law enforcement takes the significant threat posed by transnational criminal organizations seriously and must proactively hold perpetrators accountable for justice. However, these organizations are exceedingly well-structured and operate with a high level of secrecy, presenting significant challenges to law enforcement agencies regarding monitoring and disruption. Transnational criminal organizations are involved in diverse activities, including the illicit trade of drugs, smuggling of humans across international borders, cybercrime, and money laundering. These organizations can disrupt critical infrastructure, compromise national security, and cause economic and community consequences.

The cooperation between global criminal organizations demonstrates the development of a prohibited environment. Therefore, policymakers, law enforcement, and experts must understand this interconnection to stay ahead of emerging threats. Encryption technologies provide an additional layer of security that can make it challenging for law enforcement authorities to access criminal communications and data. On the other hand, the dark web provides a haven for illegal online marketplaces, which serve as a global platform for criminal transactions by TCOs.

The research is crucial as it sheds light on the evolving tactics of TCOs, providing insights to help combat this growing menace. The research aims to understand the involvement and outcomes of transnational criminal organizations (TCOs) in international cybercrimes. It emphasizes the upward trajectory of cybercrimes in recent years, their significance, and ramifications in our economy. The paper discusses the research design and methods employed in studying cybercrimes committed by TCOs, using quantitative and qualitative research approaches to analyze data and provide reliable results.

Several researchers have investigated the relationship between cybercrimes and international bodies as a critical component of safeguarding critical infrastructure, ensuring global security, and mitigating associated risks. This paper aims to examine these studies ide, identify gaps, and explore existing research to determine the current results of studies investigating how these organizations exploit technological advancements to carry out cybercrime globally.

- Statement Of the Problem

The emergence of digital technologies and increased connectivity has led to a significant shift in criminal behavior. Transnational criminal organizations have capitalized on the vast opportunities offered by cyberspace to engage in a range of illegal activities, such as financial fraud, data breaches, and ransomware attacks. While these groups were once primarily associated with conventional crimes like drug

trafficking and human smuggling, the digital world has allowed them to transcend geographical boundaries and expand their operations. Law enforcement agencies around the globe face a unique challenge in tracking and combating these cybercrimes as the online realm provides anonymity and allows criminals to operate across borders. To effectively combat this issue, law enforcement agencies must remain agile and innovative, adopting an approach responsive to the complex and ever-changing digital landscape.

- Purpose Statement

In our modern era, cybercrime poses an increasing threat, with criminal organizations operating across borders at the forefront of this issue. To better grasp the intricacies of this problem, a comprehensive research study is currently underway. It aims to investigate the complex relationship between these organizations and technology and how they use it to commit cybercrimes on a global scale.[15] The study will explore how these criminal organizations employ digital tools and technological advancements to support their illegal activities. Through analysis of actual cases, cybercrime trends, and existing literature, this study seeks to uncover the methods, motivations, and consequences of TCOs' use of technology for criminal purposes. By examining case studies, attack patterns, and emerging technologies, this research will provide a nuanced understanding of transnational cybercrimes. Ultimately, the goal is to develop more effective strategies for combating cybercrime and promoting online safety for all.

- Research Question:

How do transnational criminal organizations leverage technological advancements to carry out cybercrimes worldwide?

II. LITERATURE REVIEW

Transnational Criminal Organizations (TCOs)

In our modern world, cybercrime has become increasingly prevalent as criminal organizations and cybercriminal groups utilize advanced techniques to steal personal and financial information, hack computer systems, manipulate sensitive data, and cause severe harm to individuals, businesses, and governments. Despite years of research, transnational crime remains a complex social and political phenomenon requiring a more comprehensive understanding.[16] As such, it is crucial to have robust cybersecurity measures in place and remain vigilant to prevent cybercrime.

Transnational Criminal Organizations (TCOs) are complex illegal enterprises that operate globally. They leverage legal jurisdiction gaps and sophisticated methods to coordinate and deploy criminal activities across multiple countries and regions, maximizing profits while evading law enforcement.[17] Unlike domestic illegal organizations, TCOs establish a presence in various countries to expand their reach and reduce their chances of detection.

While criminal organizations have been around for centuries, modern-day TCOs emerged in the 20th Century due to globalization, technological advancements, and increased interconnectedness. The prohibition era in the United States played a significant role in their emergence as organized crime groups smuggled alcohol across borders. Over time, these groups diversified their activities and expanded their operations globally, tapping into the growing demand for drugs, weapons, and other illicit goods.

Today, TCOs can be found in nearly every country and engage in various criminal activities, including phishing, cyber warfare, cyber-terrorism, cyber espionage, ransomware, money laundering, and distributed denial-of-service (DDoS) attacks. These organizations use hierarchical structures and precise chains of command with leaders, middle administrators, and operatives. They form international networks with collaborators such as criminals, business partners, and corrupt officials, allowing them to carry out illegal activities in various countries. In some cases, TCOs resort to aggression and intimidation to protect their interests and eliminate rivals.

For centuries, criminal organizations have been a part of society. However, the emergence of modern transnational criminal organizations (TCOs) in the 20th century responded to the changing global landscape. Technological advancements, the globalization of economies, and the growing interconnectedness of the world created a

transnational scale of operation for TCOs. Unlike local illicit groups, TCOs operate across borders from the start.

G*lobalization* is a complex phenomenon that involves the economic, social, and cultural integration of countries worldwide. A broad range of activities are involved in globalization, such as trading goods and services, international investments, cross-border movement of people, and diffusion of technology and knowledge. The process of globalization has led to increased interconnectedness and interdependence among nations, creating both opportunities and challenges for individuals, businesses, and governments. It has brought benefits and challenges, including increased economic growth, job creation, and access to goods and services. However, it has also raised concerns over inequality, cultural homogenization, and environmental degradation. Globalization has not only expanded the scope and scale of TCO activities but has also made it more difficult for law enforcement agencies to detect and disrupt their operations. This underscores the importance of international cooperation and coordination in the fight against transnational crime.

TCOs are fundamentally different from domestic illegal organizations. They have access to advanced technologies, financial resources, and global networks. As a result, they are highly sophisticated and often operate like multinational corporations, with centralized leadership structures, division of labor, and specialized departments. TCOs use advanced encryption and communication systems to evade law enforcement agencies and can move money and goods across borders with ease.

One of the primary motives for TCOs is financial gain. Their actions have a substantial economic effect and can destabilize legitimate markets. According to Etges and Sutcliffe (2008), TCOs use information and communication technologies like legitimate businesses and respond to the same driving forces.[18]
The globalization of TCOs characterized the end of the 20th Century, with developments in financial systems, transportation, and communication facilitating their operations across borders.[19] TCOs are now highly organized and coordinated criminal enterprises with unmatched mechanisms to work together toward achieving shared outcomes with setups that span countries, regions, and even worldwide. Transnational Criminal Organizations (TCOs) pose a greater threat to global security than domestic illegal organizations due to their complexity. Despite having a long history, TCOs have undergone significant changes and will continue to do so with the advancement of technology and the increasing interconnectedness of the world.

Types of Transnational Criminal Organizations (TCOs)
During the 21st Century, criminal organizations have adapted to technological advancements, particularly the internet. As a result, they have become more involved in cybercrime, including cyber espionage, phishing, cyber warfare, cyber-terrorism, ransomware, and distributed denial-of-service (DDoS) attacks. The dark web and cryptocurrencies have provided new opportunities for illegal transactions and money laundering. Some of the most notorious groups include the North Korean Lazarus Group, Russian Fancy Bear and Cozy Bear.

The North Korean Lazarus Group is a state-sponsored cybercrime group known for its involvement in various cyber activities, including cyber espionage, ransomware attacks, and financial thefts targeting banks and cryptocurrency exchanges.[20] The activities of these organizations are highly complex and have resulted in considerable harm to the worldwide economy and security. Their most infamous attacks include the "Blockbuster" attack against Sony Pictures in 2014, the attack on the international financial wire system (SWIFT) in several countries in 2016, where they stole $81 million, and the WannaCry ransom worm that infected more than 200,000 computers in over 150 countries, causing billions of dollars in damages.[21] Their activities remain a significant concern for governments and organizations worldwide, and efforts to bring them to justice are ongoing.

The Lazarus Group is a notorious cybercriminal organization linked to several high-profile attacks worldwide. It is controlled by North Korea's RGB, making it a significant threat to global cybersecurity. Despite law enforcement agencies' efforts to dismantle the group, it continues to operate and carry out attacks on various targets, such as governmental, military,

financial, manufacturing, publishing, media, telecommunication, entertainment, international shipping companies, educational institutions, and critical infrastructures. The group's cyber espionage is mostly financially motivated, unlike other nation-state groups. The exact number of members in the group is currently unknown, and it is classified as an Advanced Persistent Threat (APT) because of its distinctive features. Presumably, due to its three main missions, the group has three subgroups that exchange information, tactics, and software tools. software tools.[22]

The three subgroups are named Andariel, BeagleBoyz, and Bluenoroff. Andariel specializes in tailoring malicious cyber operations to target South Korean governmental organizations and businesses. They also create unique malware to hack into online poker and gambling sites to steal money. This subgroup conducts malicious cyber activity against purposefully selected South Korean government personnel and military officers to gather intelligence.[23]

Andariel is a notorious hacking group known for cyberattacks against financial institutions and cryptocurrency exchanges. The group has been involved in multiple high-profile cyber-attacks, including the 2016 theft of $81 million from the Bangladeshi Central Bank. Andariel is believed to be based in North Korea and is thought to be closely affiliated with the North Korean government. The group uses advanced hacking techniques, such as spear phishing, malware, and distributed denial of service (DDoS) attacks. Despite extensive global efforts to identify the members of Andariel, the group continues to operate and presents a significant danger to the financial industry.

BeagleBoyz is a sophisticated cybercrime group that has been active for several years. According to experts, this group operates under the North Korean primary intelligence agency's guidance, the Reconnaissance General Bureau. BeagleBoyz is known for its involvement in several high-profile cyber-attacks, including the 2014 Sony Pictures hack. The group specializes in financial crimes, mainly targeting financial institutions and cryptocurrency exchanges. They use a variety of tactics, such as spear-phishing, social engineering, and malware, to carry out their attacks. In addition, they have been known to use destructive malware to cover their tracks and erase any evidence of their activities.

Despite attempts to crack down on the group, BeagleBoyz continues to operate and pose a significant threat to businesses and individuals. To protect against attacks from groups like Andariel, it is crucial to stay alert for suspicious emails or messages and to implement strong cybersecurity practices. BeagleBoyz is also responsible for sophisticated cyber-enabled ATM cash-out campaigns, identified as "FASTCash" in October 2018, that pose a severe risk to firms beyond reputational harm and financial loss from theft and high recovery costs. It has been publicly estimated that the BeagleBoyz has attempted to steal almost $2 billion since 2015.[24]

Lastly, Bluenoroff is a sophisticated hacking group that focuses on attacking foreign financial institutions. They have been involved in high-profile financial theft incidents, including the notorious SWIFT attack in 2016. During this attack, they targeted dozens of banks in 11 countries and managed to steal a staggering $81 million.[25] Bluenoroff's attacks are known for their meticulous planning and execution. They use advanced hacking techniques to infiltrate and compromise the targeted institutions' networks, giving them access to sensitive financial information. Once they have gained access, they use tactics such as phishing, malware, and social engineering to steal money and other valuable assets. Financial institutions worldwide are facing a significant threat from Bluenoroff, which remains active despite the efforts of law enforcement agencies and cybersecurity experts.

Some of the most sophisticated and notorious cyberattacks in recent times have been attributed to cybercriminal groups that speak Russian. Fancy Bear and Cozy Bear are two infamous hacking groups believed to be state sponsored. Fancy Bear is associated with the Russian military intelligence agency GRU, and Cozy Bear is linked to the Russian Federal Security Service (FSB). APT28, also known as Fancy Bear, has been known to target groups that are of interest to the Russian state using malware, including security ministries and journalists across the Caucasus region, the governments of Poland and Hungary, NATO, and the Organization for Security

and Cooperation in Europe. It is important to note that APT 28 does not steal financial information or sell the information it gathers for profit.[26]

Cozy Bear, conversely, is known for its sophisticated hacking techniques and stealthy approach to infiltrating networks. The group gained international attention in 2020 when it was linked to a cyber-attack on the U.S. government.[27] It targeted multiple federal agencies and is believed to have been one of the largest and most sophisticated cyber-attacks in history. Both groups operate highly secretively and covertly, making it difficult to attribute their activities with certainty. However, their tactics, targets, and tools have led cybersecurity experts to link them to various state-sponsored cyber operations over the years.

- Evolution of Cybercrimes

Cybercrime is an ever-growing form of digital crime, and the laws that regulate it need to keep pace with the fast-moving advancements in technology. Literature suggests that legislation is crucial in combating cybercrime.[28] Cybercrimes are illegal activities using the Internet, computers, and networks. These activities are often carried out by individuals or groups who are seeking financial gain, have ideological motives, or personal vendettas. Cyber fraud, which involves fraudulent activities such as online scams and credit card schemes, is one of the most common types of cybercrime. Cybercriminals and hackers are known to breach computer systems and networks, jeopardizing data security, causing identity theft, and engaging in cyber espionage. Financial cybercrimes, such as money laundering and online banking fraud, are becoming increasingly prevalent.

- Categories of Cybercrime

There are four main categories of cybercrime. These categories include David S. Wall's three types of cybercrime and James Martin's online illicit marketplaces/crypto markets[29] The first category is computer integrity crimes, which involve attacking the security of network access mechanisms. This includes hacking, cracking, vandalism, spying, denial of service, and planting and using viruses and Trojans.[30] The second category is computer-assisted crimes, which use networked computers to commit crimes, usually for acquiring money, goods, or services dishonestly. This includes internet frauds, socially engineered variants, and manipulating new online sales environments, particularly auction sites.[31] Using internet-based tools has facilitated the commission of crimes such as piracy, where digital content is unlawfully distributed, and ransomware extortion, where hackers demand payment in exchange for unlocking encrypted files. Online prostitution has also become prevalent, with traffickers using digital platforms to advertise and sell their victims.

Additionally, the internet has made it easier for criminals to engage in human trafficking and money laundering activities, with transactions being conducted anonymously and across borders. The third category refers to crimes associated with illegal content on computer systems connected to the internet. These crimes involve the unauthorized distribution of digital content, extortion through ransomware, the use of digital platforms to facilitate prostitution and human trafficking, and the possession or distribution of child pornography. Additionally, the internet provides anonymity and cross-border capabilities that make it easier for criminals to engage in money laundering activities. The fourth category is online illicit marketplaces (OIM) or crypto markets. A crypto market is an online platform where individuals can exchange goods and services anonymously using digital encryption to conceal their identities. Crypto markets differ from other online marketplaces because they rely on encryption technology. This category includes instances where offenders engage in the exchange of goods and services on online marketplaces.

- Cybercrime Issues Faced by Healthcare

Cybercriminals are constantly improving their methods for targeting financial institutions, government platforms, and personal computers by using techniques such as Distributed Denial of Service (DDoS) attacks, phishing, hacking attempts, and ransomware. With the advancement of technology, cybercrime is becoming more complex and extensive. The motives behind these attacks vary from curiosity to espionage, financial gain, and political influence. Healthcare organizations face an increasing threat from cybersecurity attacks, and several significant incidents have been reported globally. The most notable attacks occurred in 2015 on the Anthem Blue Cross Insurance System in the U.S., where over 78

million health records were stolen.[32]

Before 2016, healthcare organizations were not considered primary targets for ransomware. However, by October 16, 2016, 173 hacking and information technology (I.T.) incidents and 14 hospitals had fallen victim to ransomware attacks.[33] Hackers find hospitals an easy target due to the need to store patient care information, such as electronic medical records, on computer systems and the presence of security vulnerabilities in I.T. systems, as pointed out by Spence et al. (2018).[34]

In 2019, ransomware attacks affected 764 healthcare providers, while there was a surge in phishing attacks. For instance, a phishing attack on the Oregon Department of Human Services system impacted 645,000 patients. According to the U.S. Department of Health and Human Services Office for Civil Rights Breach Report, 38 million healthcare sector records were exposed in 2019, compared to 7 million in 2018.[35]

Fighting cyber-attacks is a collective responsibility that requires collaboration among various public and private stakeholders, including hospitals, I.T. vendors, medical device manufacturers, and different levels of government (state, local, tribal, territorial, and federal). This joint effort helps to mitigate the risks and minimize the impact of cyber-attacks, which is similar to how we combat deadly viruses.[36]

- Examples of Transnational Cybercrimes

Transnational cybercrime refers to criminal activities conducted via the internet or computer networks that cross national borders. These activities involve criminal organizations or individuals from one country or jurisdiction who carry out cybercrimes. These crimes may include hacking, fraud, data theft, or cyberattacks, targeting victims or entities in other countries. These criminals exploit the borderless nature of the digital realm to operate globally, making it difficult for law enforcement to track, apprehend, and prosecute them within a single jurisdiction. Transnational cybercrime poses significant challenges to national and international security, as well as economic stability.

In the 1980s, computer systems were exposed to significant harm due to the emergence of computer worms and viruses. While viruses need a host or human intervention to spread, worms can autonomously self-replicate and spread, infecting individual computers and networks with ease. Worms have the potential to cause far more damage than viruses, with the ability to destroy entire networks. Due to their ability to propagate at an alarming rate, worms have become a significant concern for cybersecurity experts. They are considered to be one of the most dangerous types of malware.

One of the most notable examples of a worm is the Morris Worm, named after its perpetrator, a graduate student in computer science named Robert T. Morris Jr. This worm infected U.S. computer networks in November 1988 and prompted a full-scale review of computer security in government, corporations, and universities.[37] As it relentlessly multiplied through networks, it consumed the storage space computers used to store information and slowed them to a halt.[38] The Morris Worm linked key university and government computers from coast to coast, ultimately attacking 6,000 computers. However, it was benign and used empty storage space instead of wiping out data like traditional computer viruses. Today, it is referred to as a "worm" in computer jargon because it was a self-contained program that entered via a communications network but did not seek to destroy data[39]

In 2010, a highly sophisticated computer virus named the Stuxnet Worm was discovered by Farwell and Rohozinski.[40] This cybercrime was a notable attack on Iran's nuclear programs, which interfered with the country's atomic capabilities.[41] It set a precedent for nation-sponsored cyberattacks on critical infrastructure. The worm was created to target specific industrial control systems used in Iran's nuclear program and to disrupt its operations. It exploited zero-day vulnerabilities in Microsoft Windows and Siemens software, infecting computers and spreading through networks and USB drives until it reached its target. Once inside the targeted systems, Stuxnet manipulated the frequency converters of uranium enrichment centrifuges, causing them to fail. This discovery marked a new era of cyber warfare and demonstrated that cyber-attacks can cause physical damage to critical infrastructure.

In 2017, the WannaCry ransomware attack affected numerous countries, causing widespread damage to healthcare systems, businesses, and critical infrastructure. This event highlighted the importance of prioritizing cybersecurity measures for governments and organizations. The attack was unprecedented in scale, affecting 200,000 systems in 150 countries, using 27 different languages, and covering every geographical region by May 14th.[42]

The malware used in the attack was a variant of 'WannaCry.' It exploited a flaw in Microsoft software, enabling the Server Message Block 1.0 to act as a vector for introducing the malware.[43] Although the National Health Service (NHS) in England was not directly targeted, it was one of the most significant casualties of the attack, with over 600 organizations affected. Among them, 34 hospital trusts were infected, and 46 were affected, providing acute care, specialized medical services, mental healthcare, or ambulance services.[44] On the evening of May 12th, a cyber researcher activated a kill switch, stopping the spread of the malicious software and preventing further devices from being infected.[45]

Over the past few years, several ransomware groups, such as REvil (also known as Sodinokibi), DarkSide, and Conti, have become infamous for using malicious software to encrypt data belonging to their victims and demanding large sums of money in exchange for the decryption key. These cyber-attacks usually target businesses and organizations and can cause severe damage, including financial losses, operational disruptions, and harm to their reputation. To safeguard themselves, organizations can take various measures, such as regularly backing up essential data, implementing security best practices, and providing employee training on identifying and responding to potential threats.

REvil is a notorious ransomware group that targets large corporations and demands a hefty ransom payment in exchange for the safe return of encrypted data. They have been responsible for several high-profile cyber-attacks, including one on software company Kaseya in 2021 that impacted thousands of businesses worldwide. Law enforcement agencies and cybersecurity experts have widely condemned these attacks.

In addition to the Kaseya attack, REvil also carried out a high-profile ransomware attack against JBS Foods, a global meat processing company, only one month after the Colonial Pipeline attacks. This attack raised concerns about potential food shortages in Australia and several other countries.[46] REvil was paid an $11 million ransom, and this incident led to an escalation in President Biden's determination to address Russian ransomware groups.[47] The JBS attacks occurred within days of the widely publicized attacks against Kaseya. This US-based software-as-a-service company significantly impacted over 1,500 companies across 20 countries.[48]

Conti is a relatively new ransomware group that started operating in early 2020. They have been targeting healthcare providers in different countries, including the Health Service Executive of Ireland, as reported by Martin and Whelan (2023).[49] Despite their short time in the business, Conti has already gained a notorious reputation for being one of the most dangerous and sophisticated groups. They are known for their speed and efficiency in encrypting data, as well as their ability to avoid detection by anti-virus software. In addition, following Russia's invasion of Ukraine, Conti publicly declared its support for the "special operation" and announced that it would launch cyber-attacks against any adversary of Russia. This statement was seen as overly patriotic. In response, one affiliate of the Conti group leaked tens of thousands of internal chat messages that disclosed their support for Ukraine.

DarkSide and REvil are two ransomware groups known for their similar attack methods and code. However, Conti is considered one of the most infamous, primarily due to its ability to operate quickly and effectively.[50] DarkSide has been active since August 2020 and gained notoriety for using advanced hacking tools and techniques to infiltrate corporate networks and steal sensitive data. Once they have the data, they threaten to release it unless a ransom payment is made. In May 2021, the group was linked to the ransomware attack on the Colonial Pipeline, which caused fuel shortages in the eastern U.S. After the attack, DarkSide claimed to have ceased operations, but experts suspect that the group may have rebranded or gone into hiding. The group's

location is unknown, but cybersecurity experts speculate they have ties to Russian-speaking countries based on the language used in their ransom notes and their target regions, primarily Europe and North America.

- Interconnectedness Between TCOs and Cybercrime

The connection between Transnational Criminal Organizations (TCOs) and cybercrime is intricate and constantly evolving. Criminal groups have realized the advantages of cybercrime, including high profits and low risks, which has led to the emergence of sophisticated and coordinated cyberattacks. The involvement of TCOs in cybercrime encompasses various aspects, such as expanding criminal operations, financial incentives, and utilizing cyber tools to facilitate their illegal activities. At times, organizations may hire skilled hackers to carry out cyberattacks on their behalf, aiming to breach systems and extract sensitive information that can be utilized for financial gains or other illicit purposes.

Collaboration between TCOs and cybercriminals is marked by specialization and division of labor. Cybercriminals may offer their services to criminal gangs in exchange for financial compensation. At the same time, TCOs provide them with the necessary resources, including infrastructure, funding, and protection from law enforcement, enabling them to execute cyberattacks on a larger scale. This cooperation allows criminal associations to expand their influence globally and commit more coordinated and sophisticated attacks.[51] Money laundering is critical in connecting TCOs and cybercrime. Cybercriminals frequently profit from money laundering, identity theft, online fraud, and ransomware attacks. Money laundering is a process that aims to legitimize illegally generated funds.[52] TCOs facilitate laundering proceeds from cybercrimes by providing the necessary resources, expertise, and networks to carry out such operations. Shell companies are often utilized to conceal the origin of illegal funds.

- Implications for Global Security

The issue of cybercrime is a significant concern for global security. These crimes can significantly disrupt critical infrastructure and economies, leading to economic, social, and political instability. This is especially true for essential services like transportation systems, power, and water supply. Communication systems and utilities are compromised in security breaches, resulting in theft of sensitive data such as personal, financial, and intellectual property. Cyber-attacks can have a significant impact, disrupting supply chains, causing job losses, and leading to other social and economic implications.

Additionally, cybercrimes can enable other criminal activities, including financing for terrorist and extremist organizations. Criminals can collaborate with other unlawful groups, such as drug cartels, to facilitate their illicit activities. The dark web provides an avenue for selling weapons, stolen data, and drugs using anonymizing tools and cryptocurrencies. The consequences of cybercrime are far-reaching, impacting individuals, businesses, governments, and society. Therefore, it is crucial to prevent and combat cybercrime using advanced technology, implementing cybersecurity policies, and raising public awareness through campaigns.

Transnational criminal organizations engage in illegal activities such as drug trafficking, human smuggling, and cybercrime, posing a significant threat to governance, states, and the economy, human smuggling, money laundering, arms trafficking, and cybercrime. These crimes not only jeopardize peace and the global economy but also undermine nations' sovereignty and the rule of law. In some cases, criminal organizations can even take over and control wealthy regions of a country or overthrow the government.

Recognizing the danger posed by these groups, the United Nations has implemented a strict policy against negotiating with terrorists.[53] Enhancing cybersecurity measures, establishing clear policies, and strengthening international relations to combat transnational crimes are essential. The cooperation of all nations is crucial to ensure that criminals are brought to justice and that the world is a safer place for everyone.

One practical approach to address this issue is establishing international governance to help solve transnational crimes. We can create the unity

necessary to overpower global criminal organizations by working together. Ultimately, this unity will result in synergy, allowing us to combat transnational crimes effectively.[54]

- Techniques used by TCOs

Transnational criminal organizations have developed sophisticated techniques to make it increasingly challenging for law enforcement agencies to trace cybercrimes to the responsible parties. However, advanced investigative techniques and international cooperation can help combat these tactics. It is also crucial for individuals and organizations to take proactive measures such as implementing strong cybersecurity policies, keeping software up-to-date, and remaining vigilant against potential threats.

One of the most common strategies used by criminal organizations is the use of proxies and virtual private networks (VPNs) to hide their location and identity while committing crimes. Encryption is another tactic used by cybercriminals to protect their communications and data. Cybercriminals may use compromised infrastructure like botnets to launch attacks, making it difficult to trace them back.

False flags are another strategy criminal organizations employ to mislead law enforcement agencies and cover their tracks. At the same time, money laundering techniques make it challenging for authorities to follow the money trail. Additionally, using cryptocurrencies for ransom payments and financial transactions provides a high degree of anonymity, making it difficult to identify the perpetrators.

Law enforcement agencies must develop new approaches to combat cybercrime. International cooperation and intelligence sharing are also crucial in addressing these evasion tactics, given the transnational nature of many cybercriminal organizations. By collaboratively implementing preemptive measures, such as cybersecurity protocols and best practices, we can effectively safeguard individuals and businesses against the potential risks and damages associated with cyber threats.

- Cybercrime Detection Techniques

The number of cybercrimes has rapidly increased as none of the traditional cybercrime detection systems implemented by forensics researchers can completely stop or mitigate them. This is because the victims or targets of cybercrimes (e.g., people, banks, properties, and governments) differ depending on the motivation for the crime (e.g., money, fame, sex, curiosity), and cybercriminals improve their methods and utilize new technologies to commit crimes and achieve their goals.[55] Many prior studies have been conducted to develop methods for detecting cybercrimes. Consequently, the tools for their detection and prosecution also have to be more sophisticated.[56]

The Hidden Markov Model (HMM) is one of the best models for detecting cyberattacks. HMMs are a valuable tool for modeling and analyzing sequential data, making them suitable for various cybersecurity applications. Sultana et al.[57] improved the Hidden Markov Model by minimizing the time required for data training to detect cyberattacks using the N-gram extraction algorithm.[58] This improved Hidden Markov Model utilizes recur rent or repeated patterns in trace files instead of whole trace events. This new algorithm, called the similarity of attack intentions (SAI) algorithm, generates a similarity matrix of previous and known attack intentions that is used to calculate the probability ratio for each attack intention. Similarity is calculated based on the ratio of new attacks to known and predefined attacks.[59] HMMs are often used in conjunction with other machine learning and statistical methods to enhance the accuracy of cyberattack detection. Additionally, HMMs may require substantial training data and periodic retraining to control adapt to evolving cyber threats.

Cyber-Physical Power Systems (CPPSs) are advanced power generation, distribution, and systems that integrate digital technologies and computational capabilities with physical infrastructure to improve the efficiency, reliability, and security of electrical power systems. CPPSs represent the convergence of traditional power systems with modern information and communication technologies, enabling more sophisticated monitoring, control, and automation of the electricity grid.[60] The integration of cyber-physical technologies into power systems is expected to lead to more sustainable and efficient electricity grids, reduce energy waste, and enhance the ability to adapt to changing energy needs. It also supports the transition toward cleaner energy sources and reduces the

environmental impact of power generation and distribution.[61] The emergence of CPPSs is to meet the needs for power system digitalization as well as more sustainable low-carbon power supply. In fact, CPPSs are power systems that can intelligently integrate the behavior of all stakeholders in the energy supply chain, so as to provide satisfactory power supply to the consumers.[62] Hence, with the increasing integration of modern technologies into the existing power systems, CPPSs transform the current power systems to be more interactive, responsive, and organic.[63]

Deep Learning Methods Deep learning methods have also been used for detection of malicious attacks in the literature. Popular deep learning methods in the IoT are deep belief networks and adaptive boost algorithms. The deep belief network (DBN) is a popular deep learning algorithm that consists of a visible layer (input Layer) and multiple hidden layers (latent variables). This algorithm works in layers. First, the input layer sends data to the first hidden layer and processes it. Secondly, the next hidden layer takes the first hidden layer as an input layer and processes the data.[64]

A Network Intrusion Detection System (NIDS) is a critical tool for identifying and mitigating a wide range of network-based threats, including viruses, malware, denial-of-service (DoS) attacks, intrusions, and unauthorized access attempts. It helps security professionals monitor and protect network assets, data, and sensitive information by providing early warning of potential security incidents. NIDS is often used in conjunction with other security measures, such as firewalls, endpoint protection, and security information and event management (SIEM) systems, to provide a comprehensive defense against cyber threats and intrusions.[65]

- The Role of International Cooperation in Addressing Transnational Cybercrime

Transnational cybercrime is a complex issue that requires a more in-depth approach from governments, law enforcement agencies, and private organizations across the world. It is difficult to combat cybercrime alone because it is a global problem that transcends borders. Therefore, international cooperation is essential for addressing this problem effectively. To prevent and combat cybercrime, it is crucial to establish strong collaborations between different entities. These entities must work together to develop strategies that can help them detect and prevent cybercrime. They must also share information and best practices on how to combat cybercrime effectively. This includes sharing intelligence on cybercrime trends, threats, and vulnerabilities that can help them stay ahead of the criminals.

Moreover, coordination among different entities is necessary to ensure that investigations are conducted in a timely and efficient manner. This means that they must establish protocols for sharing information and evidence, working together across borders, and harmonizing their laws and regulations. This will help them streamline their investigations and ensure that criminals are held accountable for their actions. Overall, international cooperation is a critical component of combating transnational cybercrime. It is essential for governments, law enforcement agencies, and private organizations to work together to prevent, detect, and respond to cybercrime effectively. By doing so, they can make the internet a safer place for everyone.

Various organizations, including the United Nations, have been actively working to combat cybercrime. The UN aims to support economic growth while preserving international law and security. To fight organized crime, the UN has approved the UN Convention on Transnational Organized Crime. In the past, the UN has published research on ways to minimize computer and high-tech crimes. At the 11th United Nations Conference on Crime Prevention, a discussion workshop was conducted to explore possible coordination among countries and the business sector to handle cybercrime. The report proposed that the UN assist member states in cybercrime management, provide training, and improve the enforcement of international law.

The United Nations has taken a proactive role in fighting cybercrime by establishing the Worldwide Telecommunications Union, which oversees international telecommunications while upgrading its infrastructure.[66] One of the main objectives of the International Telecommunication Union (ITU) is to address global issues such as enhancing cybersecurity. In 2003, the ITU developed model legislative

recommendations for creating harmonized cybercrime laws for its member states. The member states of the European Union work together to combat cybercrime, with cooperation being strengthened through the Commission and its Council of the European Union. The EU has implemented a strategy that allows for the creation of robust legal frameworks to tackle cybercrime, as well as the recruitment of highly skilled security personnel.[67] Experts in the field continue to collaborate with IT professionals and scientists to improve standards for investigations into cybercrime.
The Council of Europe (CoE) is implementing initiatives to curb cybercrime. As early as 2001, the CoE has been requiring its member countries to have laws in place to address cybercrime and to establish adequate security agencies to enforce these laws.[68] The CoE's subdivision also provides its member nations with recommendations for laws protecting against cybercriminal activities. Meanwhile, Interpol, which provides support to police personnel across the globe, plays a vital role in the fight against cybercrime.[69] By accessing each other's databases, Interpol member nations' police personnel can collaborate and effectively combat significant criminal operations, particularly cybercrime-related ones. Interpol's partnership with commercial companies such as Microsoft allows it to address and eliminate imminent threats.

Existing Efforts to Combat Transnational Cybercrimes
The threat of cybercrime looms over the world, and governments worldwide have taken measures to establish regulatory agencies and legal frameworks to protect against data breaches and cyber threats. These agencies collaborate with specialized cybercrime units such as Interpol and the FBI to investigate and enable global police cooperation. Despite their efforts, cybercrime is escalating rapidly due to the internet's anonymity and speed, providing criminals with opportunities to commit crimes across borders.

To tackle this issue, public-private partnerships have been formed through initiatives like Computer Emergency Response Teams and Information Sharing and Analysis Centers. These partnerships encourage cooperation and information sharing among industries, governments, and critical infrastructure associations. They also facilitate joint efforts between the public and private sectors, such as the World Economic Forum Partnership for Cyber Resilience.

Promoting safe practices through online safety campaigns and cybersecurity training is crucial in encouraging individuals to report any incidents and preventing potential threats. Countries also designate specific periods to raise public awareness and promote best practices in cybersecurity. These efforts are vital in mitigating the risks posed by cybercrime and equipping individuals and organizations to protect themselves against potential threats.

According to the National Security Strategy (2022), to effectively counter transnational criminal and trafficking networks, a comprehensive strategy is imperative.[70] This approach must prioritize safeguarding citizens, weakening the financial resources of criminal and terrorist networks, disrupting illicit trafficking operations, defeating transnational criminal organizations, combating corruption within governments, reinforcing the rule of law, enhancing judicial systems, and promoting transparency. Despite these challenges, the United States can leverage its capabilities to formulate and execute a collaborative strategy with nations with similar threats.

The Goldwater-Nichols Department of Defense Reorganization Act of 1986 (Public Law 99-433) requires a report called the National Security Strategy (NSS). The NSS talks about how the U.S. can use its power to achieve its security goals. It discusses the country's international interests, commitments, objectives, and policies, along with the defense capabilities necessary to deter threats and implement security plans.[71] The report also highlights the need for the U.S. to work with other countries to promote cybersecurity by developing international norms and standards for responsible state behavior in cyberspace. It emphasizes the importance of defending critical infrastructure against cyber threats and ensuring the capability to respond to and recover from cyber attacks.

The NSS acknowledges the importance of safeguarding individuals' privacy and civil liberties in the context of cybersecurity. It also recognizes the importance of a robust cybersecurity workforce in the

government and the promotion of innovative technologies to enhance cybersecurity. Overall, the U.S. National Security Strategy provides a framework for tackling the complex and evolving threat landscape posed by cybercrime and other cybersecurity challenges. It is essential that all national governments, including the United States, possess a deep understanding of the critical components, weaknesses, and incentives of transnational criminal organizations (TCOs) to effectively identify, thwart, dismantle, and discourage their efforts to threaten our safety and economic well-being. The U.S. can combat TCOs by limiting, denying, or neutralizing their access to vital resources. To effectively implement the 2011 Strategy to Combat Transnational Organized Crime, a comprehensive approach utilizing all available national power tools, such as diplomacy, military, intelligence, law enforcement, information, finance, and economics, must be employed.[72]

- Challenges and Gaps in Current Literature

The study of transnational criminal organizations exploiting technological advancements to commit cybercrimes on a global scale poses several challenges. The main obstacle is acquiring extensive and current information on transnational cybercrimes and their consequences, which arise from many unreported incidents. The absence of comprehensive data makes it challenging to obtain a complete understanding of the cybercrime landscape. These offenses often involve multiple actors and activities across various countries, creating difficulty in comprehending the legal and regulatory frameworks of different jurisdictions and their impact on cybercrime investigations. As a result, it is challenging to identify and prosecute cybercrime perpetrators, leading to an increased cybercrime rate overall.

Researching cybercrime is often challenging due to methodological limitations caused by its secretive and ever-changing nature. Cybercriminals use various techniques to conceal their identity and activities, making it difficult to track and study their behavior. Moreover, the rapid pace at which technological advancements occur makes it challenging to keep pace with the evolution of new cybercrime techniques. Additionally, existing literature highlights a significant gap in research regarding the gender dimensions of cybercrime. While some research exists, there is a lack of knowledge regarding the experiences of female victims, gender-based variations in cybercrime prevention and response, and the involvement of women in cybercriminal activities. An in-depth understanding of these gender dimensions is critical for developing effective policies and strategies to combat cybercrime.

The exploitation of technological advancements by transnational criminal organizations to conduct crimes on a global scale has become a prominent issue in recent years. In order to gain a comprehensive understanding of this intricate issue, researchers have carried out a vast array of studies utilizing various secondary research methods. These methods have allowed for a more in-depth problem analysis, providing invaluable insights and enabling researchers to draw meaningful conclusions. Employing an exploratory design, these studies have sourced information from various outlets, including government publications and experts in the field of cybercrime. Furthermore, research articles have been used as primary data sources.

Researchers have been meticulous in selecting their samples, ensuring they align with projected outcomes, enabling them to gather both primary and secondary data that meet specific research requirements. This comprehensive approach aims to provide a detailed understanding of how transnational criminal organizations exploit technological advancements to conduct global crimes, leading to the implementing of more effective strategies to combat this issue.

Cybercrime is a complex and multifaceted issue that has far-reaching implications. Although a vast amount of literature on this topic, it still needs to be understood completely. The challenges include the constantly evolving nature of cyber threats, the lack of standardization across countries and legal systems, and the difficulty in tracking and prosecuting cybercriminals. Conducting further research is crucial to deepen our understanding of this issue and develop effective policies to combat cybercrime. This is necessary to ensure the safety and security of individuals, organizations, and governments.

It is crucial to conduct further research in order to fill the gaps in knowledge and develop effective policies

to combat cybercrime. Researchers face various challenges, such as obtaining the latest and most comprehensive information, understanding legal and regulatory frameworks, and dealing with the constantly evolving and secretive nature of cybercrimes. Therefore, it is necessary to adopt a comprehensive and interdisciplinary approach to investigating cybercrime. Additionally, it is vital to conduct further research to explore the gender aspects of cybercrime. This includes examining the experiences of female victims, gender-based differences in cybercrime prevention and response, and the involvement of women in cybercriminal activities. Such research can help create targeted policies and strategies that are not biased towards any gender to combat cybercrime effectively.

In the past, it was commonly believed that women had no direct involvement in the violent activities of criminal organizations, nor were they considered to hold significant positions within criminal structures. The role of Italian Mafiosi wives and sisters was traditionally restricted to running the household and raising children while instilling the family's values and codes.[73] The last two decades have seen several publications showing that women play an essential role in transnational organized crime. There is a great variety in these roles, as they range from Nigerian 'madams' holding critical positions in human trafficking networks to Mexican female coyotes and women at the head of drug trafficking networks in Colombia to Sicilian and Calabrian local godmothers.[74]

More and more historical evidence is presented in the criminological literature of the active participation of women in criminal activities, their knowledge and support of the criminal' business,' and their leading positions in criminal networks. For example, women often played the role of posting (mailwoman) or *messaggera* (messenger) in nineteenth-century Sicily.[75] Another task of women involved in criminal organizations was to mediate between rival criminal families or clans. The so-called 'sisters' in Russian criminal groups were often asked to negotiate with rivals.[76] Women also reminded their partners of their duty to defend the honor of the family and to take revenge, violently if necessary, and even the women who were not actively involved in their husbands' crimes reveled in the status, wealth, and power resulting from their actions.[77]

III. METHODOLOGY

Research design

In order to gain a comprehensive understanding of the cybercrimes perpetrated by transnational criminal organizations (TCOs), it is vital to employ quantitative and qualitative research methods. Quantitative research methods enable the collection of measurable data on the frequency and nature of TCO cybercrimes, which can be sourced from cybersecurity companies, incident reports, and law enforcement agencies. This data provides invaluable insights into the patterns and trends of cybercriminal activity.[78] By utilizing quantitative research methods, researchers can analyze vast datasets and identify critical factors that contribute to cybercrime, including the tactics and techniques employed by TCOs, the industries and sectors that are most susceptible to cyber-attacks, and the impact of cybercrime on both businesses and individuals.

Quantitative research methods can be crucial in informing policy decisions and improving cybersecurity strategies to protect against cyber threats. These methods can be utilized to analyze financial transactions, network traffic, and law enforcement data to determine the extent and significance of the involvement of Transnational Criminal Organizations (TCOs) in cybercrimes. Qualitative research methods can provide deeper insights into TCO tactics and their impact on society and individuals. By conducting surveys and interviews with individuals or organizations involved in cybercrimes or their victims, researchers can gather firsthand insights into the intricacies of TCO operations. This qualitative data can complement the quantitative data and provide a more comprehensive understanding of cybercrimes and the role of TCOs in perpetuating these crimes.

The integration of both quantitative and qualitative research methodologies can provide researchers with a more comprehensive and nuanced comprehension of the intricate relationship that exists between transnational criminal organizations (TCOs) and cybercrime. This can ultimately assist law

enforcement agencies and policymakers in developing more effective strategies to combat cybercrime and disrupt the activities of TCOs.

Traditionally, cybercrime research has been divided into four categories: qualitative, observational, quantitative, and instrumental studies. However, this research aims to bridge the gap in knowledge by integrating qualitative and descriptive objectives with quantitative clustering techniques for analytical purposes. By adopting this approach, one can gain a deeper and more nuanced comprehension of the subject matter.

Furthermore, it allows for identifying any underlying patterns or relationships that may have been overlooked. This method is beneficial in revealing connections that may take time to be apparent, providing valuable insights and enhancing the overall understanding of the topic at hand. The study measures various types of cybercrimes, such as hacking, data breaches, identity theft, and financial fraud, which are considered dependent variables. Data is collected annually from multiple sources, including cybersecurity companies, incident reports, and law enforcement agencies, to track trends and changes over time.[79]

Quantitative clustering techniques are a valuable tool for cybercrime researchers to group different cybercrimes based on their attributes. These techniques involve mathematical algorithms and statistical models to analyze large sets of cybercrime data, identifying patterns and trends. Researchers can gain a better understanding of cybercrime by studying its nature and scope, which can help them develop effective strategies to combat it.

The benefits of quantitative clustering techniques include categorizing cybercrimes based on similarities and differences. This can help identify clusters of similar cybercrimes that may be related to one another, as well as clusters of dissimilar cybercrimes that may have distinct characteristics or modus operandi. By analyzing these clusters, researchers can gain insights into the underlying causes and motivations of cybercrime and develop targeted interventions to prevent and deter it.

Furthermore, quantitative clustering techniques can help identify emerging trends and patterns in cybercrime, such as new types of attacks or changes in the tactics and techniques used by cybercriminals. Researchers can stay ahead of the curve and develop new strategies to counter the latest threats by keeping up with current trends.

In the realm of cybercrime research, the use of quantitative clustering techniques is crucial. These techniques enable researchers to delve deeper into cybercrime's intricate and ever-changing landscape. Using these methods, researchers can effectively analyze and categorize large amounts of data, identifying patterns and trends that may take time to become apparent. This analysis allows for a more comprehensive understanding of cybercrime, aiding in developing effective prevention and mitigation strategies.

The focus of this research is to analyze the influence of Transnational Criminal Organizations (TCOs) on the frequency of cybercrimes. Illicit activities, such as money laundering, drug trafficking, human smuggling, and cyberattacks, are often associated with TCOs. To analyze the extent of TCO involvement in cybercrimes, experts examine financial transactions, network traffic patterns, and data from law enforcement agencies. By examining these indicators, it is possible to understand the scope and significance of TCO participation in cybercrime activities.

Cybercrimes committed by TCOs pose a severe threat to individuals and organizations worldwide. In order to gain a better understanding of the nature and impact of these crimes, it is necessary to employ qualitative research methods. Techniques such as in-depth interviews, observations, and other qualitative approaches can provide detailed and insightful data, revealing the intricate and multi-faceted aspects of these criminal activities.

Qualitative research methods, such as surveys and documented interviews, provide an opportunity to gain firsthand knowledge about the nuances, tactics, and societal impact of TCO operations by engaging with individuals or organizations involved in cybercrimes or those who have fallen victim to them. The data gathered from these interviews can be analyzed to

identify patterns and trends in TCO activities and their motivations.[80] Such an approach adds depth to the analysis by providing more detailed insights into the purposes, methods, and impacts of cybercrimes.

Through qualitative and quantitative research methods, this study aims to provide a comprehensive understanding of cybercrimes and the significant role that TCOs play in perpetuating these crimes. Using both methods will enable the gathering of detailed insights and statistical data, providing a more complete picture of the issue. Ultimately, this study will help develop more effective strategies to combat cybercrime and hold TCOs accountable for their actions. It is imperative to employ qualitative research methods to effectively combat cybercrime and safeguard individuals and organizations from the threats posed by TCOs.

- Case Selection

Investigating transnational criminal organizations (TCOs) that engage in cybercrimes is a complex task that requires careful consideration in case selection to ensure that research is compelling. This study examines various instances of TCOs' participation in cybercrimes globally based on data accessibility, the significance of the cases in illuminating TCOs' use of technology, and the broad range of cybercrime types. To comprehensively examine the involvement of specific TCOs in cybercrimes, this research will use a case study approach that involves an in-depth investigation and analysis of particular individuals, groups, or situations.

In the context of cybercrime, a case study approach will involve a detailed examination of specific instances of cybercrime that involve a particular TCO. The aim is to gain a better understanding of their involvement, motivations, and methods. By implementing this approach, researchers will have the opportunity to gain in-depth and intricate knowledge about the intricate and multi-faceted nature of cybercrime and the extent of TCOs' involvement in it. Since researching TCOs committing cybercrimes is complex, selecting appropriate cases is vital to ensure effectiveness. Therefore, this research will examine various TCOs' involvement in cybercrimes in different geographical areas worldwide. Case selection will be based on the accessibility of data, the importance of shedding light on TCOs' use of technology, and the broad spectrum of cybercrime types.

The research will adopt a multi-step process to ensure the selection of the most relevant and significant cases. The first step will be identifying cybercrime cases committed by different global TCOs, including hacking, data breaches, identity theft, and financial fraud. The second step will be to evaluate the significance of each case by analyzing its impact on individuals, businesses, and governments. The third step will be to assess the data availability of each case, as the quality and quantity of data are crucial to conducting a detailed analysis.

The selected cases will represent high-profile cases and those that significantly impact individuals, businesses, and governments. The research will examine the cases in detail, using various data sources, including official reports, court documents, and interviews with relevant stakeholders. The study aims to provide a comprehensive understanding of TCOs' involvement in cybercrimes and their use of technology.

The proposed research investigates two critical variables: the frequency of cybercrimes and the involvement of transnational criminal organizations (TCOs) in such crimes. In order to gain a better understanding of the frequency of cybercrimes, a thorough analysis of cybercrime incidents that have taken place across the globe over a specific period will be carried out. Through this analysis, the study aims to present a detailed and all-encompassing overview of the nature and extent of cybercrimes. By identifying patterns and trends, we hope to provide valuable insights to inform future prevention and response strategies. The data from various sources, including incident reports, law enforcement agencies, and cybersecurity firms, will be analyzed to identify the frequency, types, and severity of cybercrimes committed. By examining annual trends in cybercrime occurrences, any significant changes in the pattern of cybercrime activity will be identified. This analysis will help develop a clear understanding of the cybercrime landscape and formulate effective cybersecurity strategies to mitigate cyber threats.

To evaluate the involvement of transnational criminal organizations (TCOs) in cybercrimes, a comprehensive analysis of various indicators will be conducted. This will include closely examining financial transactions linked to TCO activities and monitoring network traffic patterns to identify suspicious activity. The authorities will use information from law enforcement agencies to gain insights into the typical tactics and strategies of transnational criminal organizations (TCOs) in cybercrimes. The primary objective of the analysis is to collect and evaluate data from diverse sources, including but not limited to financial records, computer systems, and law enforcement agencies. The purpose is to gain a thorough and detailed understanding of the nature and scope of TCO activities linked to cybercrime, including the type of cybercrimes committed, the methods employed, and the financial gains generated. By taking a multi-faceted approach to the analysis, patterns, and trends will be identified that will enable better quantification of the extent of TCO activities in this domain.

The research aims to understand the nature and extent of cybercrimes and TCO involvement in these crimes by analyzing various indicators such as financial transactions, network traffic analysis, and law enforcement information. By examining these two variables in detail, policymakers and law enforcement agencies can develop effective strategies to combat cybercrime and reduce its impact on individuals and organizations.[81]

- Data Sources

It is crucial to have a clear understanding of the origins of our data. In order to gather information, we will use primary and secondary data sources. Obtaining primary data is essential, and there are several effective methods to do so, including case studies, surveys, interviews, content analysis, experiments, and focus groups. Surveys can be conducted through different mediums, such as in-person, over the phone, or online. The choice of medium depends on the purpose of the survey, the target audience, and the resources available.

Content from various sources, including social media, news articles, websites, and documents, can be analyzed using textual, visual, audio, or video content. Controlled experiments measure specific variables, while focus groups provide feedback and opinions from a specific group of people on a particular topic or product. These methods provide first-hand insights from individuals or organizations involved in cybercrime or its victims.

Secondary data sources can be accessed through academic journals, government reports, books, news articles, and online databases. These sources provide information that has already been published and can be used to support or supplement primary data. The internet is a vast secondary data source accessed through online libraries, databases, and search engines. Government websites and reports are also valuable sources of data on specific topics. Academic journals and books are reliable sources of detailed information that can be accessed online or through libraries. Utilizing primary and secondary data sources provides a comprehensive understanding of cybercrimes and TCOs.

- Data Collection Methods

The method used to collect data depends on various factors, including research objectives, the type of information needed, and the study's context. Researchers often use a combination of methods to enhance the validity and reliability of their results. In studying cybercrimes, a multidisciplinary approach involving various research techniques such as surveys, interviews, secondary literature, archives, and quantitative analysis is required. One of the data collection methods is distributing structured questionnaires to individuals and groups affected by cybercrimes.

These studies aim to acquire numerical data on the incidence and types of cybercrimes. In-depth interviews are used to obtain qualitative insights into cybercrimes' operations, tactics, and impact. Lastly, document analysis involves reviewing current reports, case studies, and research papers on cybercrime to identify pertinent facts and trends. A comprehensive understanding of cybercrimes and their impact can be achieved using various research methods. Secondary literature, such as academic articles, reports, and news articles, can provide historical context, theoretical frameworks, and trends in transnational cybercrimes. Archives that include law enforcement records, court

documents, and cybercrime incident reports provide more insight into specific cases.

Transnational criminal organizations (TCOs) often manipulate data to commit cybercrimes, such as financial fraud and identity theft. Ensuring data integrity is essential to building trust in the information that cybersecurity professionals rely on to combat cyber threats. Maintaining the quality and integrity of data during analysis is crucial, and that is where data treatment comes into the picture. This process is of utmost importance while dealing with cybercrime involving TCOs. Data treatment involves collecting, organizing, analyzing, interpreting, and presenting data using various techniques to derive insights that aid informed decisions. Accurate and reliable information is critical in finance, healthcare, marketing, and scientific research, and data treatment ensures that organizations have access to reliable data to make informed decisions.

In cybercrime, TCOs frequently manipulate data to conceal their actions, making it challenging for cybersecurity professionals to track them. This text explores TCOs' methods to hide their tracks and suggests countermeasures to detect and minimize these tactics. Effective data treatment methods are crucial in uncovering TCOs' operations, as they modify data to conceal their footprints. Data cleaning is the most critical step in data treatment, which involves removing inconsistencies, errors, or anomalies that could distort the study, ensuring the reliability and accuracy of the data.

Data cleaning is a critical process that identifies and removes inconsistencies, errors, or anomalies in data that could compromise accuracy. It involves analyzing the data, correcting errors, filling in missing values, and removing duplicates. This time-consuming process ensures that data is accurate, complete, and consistent, leading to better business decisions and outcomes.

Data transformation may also be necessary to enable accurate analysis and comparisons. This process involves formatting and unit conversion to make the data more readable and understandable. Additionally, data integrity controls are vital for detecting and reducing any data alteration or tampering by TCOs. By ensuring the accuracy of their analysis and uncovering concealed illegal activity, organizations can confirm the reliability of the information.

Quantitative data analysis uses descriptive statistics and correlation analysis to identify patterns between organizational characteristics and cybercrime tactics.[82] Data analysis involves statistical methods like regression and correlation to reveal patterns, trends, and relationships within the data.

Regression analysis is a statistical technique that helps to explore the relationship between variables. Examining the impact of one variable on another enables us to forecast the value of the dependent variable based on the values of the independent variables. This method is widely used in analyzing data to identify trends or patterns within a dataset and can be applied to both linear and nonlinear relationships. Due to its ability to make predictions and forecast future outcomes, regression analysis is a valuable tool across many fields. It has been utilized to identify the contributing factors behind the rise of cybercrime.[83]

Correlation analysis is a statistical technique that gauges the strength and direction of the association between two or more variables. It enables us to evaluate the degree of correlation between variables and how closely they are intertwined. Through the examination of data, correlation analysis can reveal patterns or trends in a given dataset and evaluate the link between variables, ultimately pinpointing potential vulnerabilities. This methodology is valuable for obtaining a deeper understanding of the connections between various variables.

Utilizing data visualization techniques, including charts, graphs, and heat maps, is a practical approach to presenting complex data in a more accessible and intelligible manner. These visual tools simplify intricate information, allowing patterns and trends to be easily identified. By leveraging such methods, it can convey insights gained from data analysis clearly and concisely. Visuals are a powerful means of illustrating complex relationships and patterns in data, streamlining the decision-making process, and facilitating informed actions based on the insights gleaned.[84]

IV. FINDINGS & ANALYSIS

The rapid pace of technological advancements has dramatically changed the global landscape, providing new opportunities for transnational criminal organizations (TCOs) to engage in cybercrimes worldwide.[85] In the field of International Relations, it is essential to understand how TCOs exploit these technological advancements to carry out cybercrimes. This essay delves into how TCOs influence these advancements, the implications of their actions, and recommendations to counter their activities. To address these questions, we examine the scale and scope of transnational cybercrimes, the tools and technologies employed, the entities targeted, law enforcement efforts, and noteworthy case studies to highlight the issue's complexity.[86]

The study has revealed that Transnational Criminal Organizations (TCOs) employ various tactics to execute cybercrimes, such as employing complex malware and social engineering techniques. Furthermore, the research has found that TCOs generally target crucial infrastructure and financial institutions, which poses a significant danger to global security. Overall, the study's results provide valuable insights into the actions of TCOs and the methods they use to carry out cybercrimes. By comprehending these strategies, researchers can create practical solutions to fight against these illegal activities and safeguard people and firms from the harmful impacts of cybercrime.

The report titled 'Organised Crime in the Digital Age' investigates how criminal organizations use digital technologies to commit crimes. It also explores the characteristics of these organizations and how policies and strategies can be developed to address digital crime. The study was conducted by Dr. Michael McGuire, a criminologist at the John Grieve Centre, on behalf of BAE Systems Detica. This company works with government and law enforcement agencies to fight cybercrime.[87] The report challenges the common assumptions about the perpetrators of cybercrime. Contrary to popular belief, the research shows that almost half (43%) of organized digital crime group members are over 35. In contrast, only 29% of these members are under 25, and many have only basic IT knowledge. The study highlights that the increased accessibility to off-the-shelf software and simpler technologies, such as pre-paid mobile phones, has made digital crimes more appealing and attainable to a broader range of people.[88]

As Broadhurst (2014) notes, McGuire's typology[89] represents a 'best guess' based on current knowledge about cyber offenders and is likely to change as the digital environment evolves and includes three primary group types, each divided into two subgroups depending on the strength of association between members.[90]

Ransomware has become a significant threat in the world of cybersecurity. According to the FBI, monetary losses due to ransomware attacks reached over $1 billion by the end of 2016. There has also been a significant increase in the number of ransomware variants. At the same time, McAfee Labs2018 Threats Predictions Report predicted that ransomware attacks would peak in 2017 and decline afterwards while others believe that ransomware attacks will continue to increase in number and sophistication in 2018 and beyond.[91] Bitdefender, an internet security software firm, found that over 61.8 percent of malicious internet files in the United States contained some form of ransomware, according to an analysis of internet traffic in 2016.[92]

- Importance of Findings and Analysis

The findings and analysis presented in this paper are significant. As the cyberspace threat landscape is constantly changing, it is crucial to keep up to date with the latest trends and tactics used by threat actors. Cyber threats are now at the forefront of international relations, affecting national security, economic stability, and global geopolitics.[93] Understanding how Transnational Criminal Organizations (TCOs) utilize technological advancements is crucial. Policymakers, law enforcement agencies, and cybersecurity professionals need this knowledge to combat cybercrime.[94] This research provides valuable insights into the methodologies used by cybercriminals, enabling the development of precisely targeted prevention and response strategies. These strategies are essential for safeguarding critical infrastructure, intellectual property, personal data, and national interests in an interconnected digital world.

- Challenges of Theory and Evidence

The lack of evidence concerning the size, function, and nature of organized crime groups operating in cyberspace hinders the development of effective countermeasures. While many experts believe that cybercrime is now primarily perpetrated by organized groups and that individual hackers are less common, there still needs to be more knowledge about the structures and longevity of these groups, how trust is established, and how they relate to other forms of crime.[95] There is a lack of research-based evidence regarding offender behavior and recruitment in cyberspace, though learning and imitation are essential factors.[96] Therefore, it is not enough to understand organized crime groups solely from their illicit activities as rational, profit-driven networks of criminals, as socio-cultural forces also have a significant role in the creation and continuation of these groups. In some cases, there may be signs of obsessive-compulsive behavior, while in others, a sense of impunity (stemming from over-confidence in anonymity) may be evident. As previously mentioned, greed may be just one of many motives, with others present to various degrees depending on the type of crime.

Studying transnational criminal organizations (TCOs) that use technology to commit cybercrimes presents several theoretical and evidentiary challenges. Understanding and combating criminal activities can be challenging due to various factors that impede the process.[97] As we navigate the complexities of modern society, it is essential to address the inherent challenges that come with it. To effectively address these challenges, we need to adopt a multifaceted approach that includes fostering international cooperation, implementing advanced cybersecurity measures, embracing technological advancements, and developing robust legal frameworks. By doing so, we can ensure a safer, more secure, and more prosperous future for all. Researchers, law enforcement agencies, and cybersecurity professionals are continuously working to develop strategies and tools to understand better and combat TCOs that exploit technology for cybercrimes.

The discussion of cybersecurity can provide valuable suggestions for enhancing data privacy strategies. Technology plays a significant role in communication, data storage, and productivity. Unfortunately, many countries have experienced theft of important governance, currency, and cash flow data. Financial institutions have also lost essential customer data and cash flow records and have even been involved in illegal transactions with unauthorized persons outside the banks.[98] Cybercrime has become so prevalent that online shoplifting and phishing overtake physical theft. Improving cybersecurity is crucial in preventing unauthorized access to data, which can be used for malicious purposes. Hackers utilize data from prominent companies to make illegal profits and they disappear once people pay such money to given bank accounts or till numbers.[99]

Cybersecurity discussions can also help to prevent such cybercrimes by developing data privacy strategies. Additionally, global cybersecurity debates can provide better ways of preventing terrorism. Cybercrime enhances terrorism by allowing terrorist groups to access government information on major national events, weddings, political and business conferences, and meetings of prominent figures in each country.[100] Terrorists use this information to launch attacks for revenge, kidnap family members, demand ransom, and bring down significant businesses. Eavesdropping is one of the most dangerous cybercrimes, whereby hackers can intercept conversations and listen to them secretly without anyone's knowledge. They use this information to plan counterattacks on government and business activities.
Scale and Scope of Transnational Cybercrimes

The alarming increase in transnational cybercrimes has become a significant cause of concern. Criminal organizations are expanding their illicit operations through digital means, which has led to a wide range of illegal activities that affect individuals and institutions globally. These cybercriminal activities are becoming more complex, and their impact is devastating. From intricate financial fraud to massive data breaches, deceptive online scams, and identity theft, transnational criminal organizations (TCOs) have found ways to operate globally with impunity. The vast expanse of the digital realm provides them with the perfect platform to carry out their unlawful activities, making it a significant challenge for law enforcement and cybersecurity efforts worldwide.

Transnational criminal organizations (TCOs) are highly adaptable, utilizing various tools and technologies to carry out their cybercrimes. It is crucial to understand their methods, which include malware, social engineering, hacking, and phishing.[101] Malware, such as ransomware and keyloggers, is a particularly effective tool TCOs use to infiltrate computer systems, steal data, or disrupt critical infrastructure.[102] Social engineering tactics exploit human psychology to manipulate individuals into divulging sensitive information and breach defenses. Hacking techniques allow TCOs to gain unauthorized access to secure systems, often by exploiting vulnerabilities in software or hardware.

In-depth investigations reveal that TCOs adopt the latest technological innovations to enhance the effectiveness and sophistication of their cyberattacks. As a result, cybersecurity professionals and organizations need to adapt and strengthen their defenses continuously. Transnational criminal organizations often use sophisticated tools and techniques to commit cybercrimes and exploit kits designed to take advantage of vulnerabilities in software and hardware systems. They may also use techniques such as social engineering and spear phishing to gain access to sensitive information and compromise computer networks.

- Types of Cybercrimes

As technology progresses, cybercriminals are constantly discovering new ways to launch attacks. Therefore, individuals, organizations, and governments must take proactive measures in both preventing and combating cybercrime effectively. The purpose of this study is to provide a comprehensive review of different cybercrime detection techniques, categorized based on various detection methods. The study first presents the different types of cybercrimes and discusses their consequences on individuals, organizations, and societies.[103]

Examples of tactics and techniques used by transnational criminal organizations to carry out cybercrimes include phishing, cyber warfare, cyber-terrorism, cyber-espionage, ransomware, money laundering, and distributed denial of service (DDoS) attacks. Criminals use various tactics such as phishing, pretexting, and baiting to acquire sensitive data such as login information and credit card numbers.

Phishing is a type of cyber-attack where the attacker deceives the victim into revealing confidential information, such as passwords, credit card numbers, or social security numbers.[103] The attacker typically sends an email from a trustworthy source, like a bank or an e-commerce site. The email usually includes a link that takes the victim to a fake website, where they are prompted to enter sensitive information.[104] These websites look legitimate but are controlled by the attacker, who uses them to steal the victim's information. Phishing attacks can also occur through social media, text messages, or phone calls. The attacker may use social engineering techniques to gain the victim's trust and persuade them to provide the requested information. The attacker may impersonate a customer service representative and request the victim to confirm their account information.

Cyberwarfare is a form of warfare that involves cyberattacks instead of physical weapons. Organizations or groups of hackers can carry it out without permission from the government, and it often leads to political problems between countries.[105] In recent times, cyber warfare and cyberattacks have become the most common types of warfare. Over the past 20 years, many cyberwars have occurred. For example, in 2008, Russia and Georgia engaged in a cyber war that involved several attacks on Georgian government websites using structured query language (SQL) injection, distributed denial-of-service (DDoS), and cross-site scripting.[106]

Cyberterrorism is an illegal action that involves violence against people and property. It often has a political, racial, or ideological motive. This type of cybercrime can spread fear, anxiety, and violence amongst people or even sabotage and destroy properties, such as computers and networks. Cyberterrorism can also impact the availability and integrity of information. Terrorists use the Internet to spread propaganda, recruit individuals, influence public opinion, and shut down national infrastructure, such as transportation, dams, traffic lights, and energy facilities. An example of cyberterrorism is the Ukrainian attack on a power grid in December 2015, which began with a phishing email. Specific

sequences of cyber terrorists can create fear and disruption among citizens regarding their safety. These sequences can also influence political decision-making. Economic losses, damage to property, and violence resulting from cyberterrorism can lead to death and affect the cohesion of society.[107]

Cyber espionage refers to the act of gaining unauthorized access to confidential information through computer networks. This practice is commonly employed by individuals, groups, or government agencies to clandestinely gather information about a specific person, organization, or government. It involves using various techniques such as surveillance, monitoring, and hacking to obtain sensitive data without the knowledge or consent of the target. Cyber espionage typically involves stealing trade secrets, intellectual property, financial information, and other sensitive data. It is often carried out by state-sponsored hackers or cybercriminal groups who use advanced techniques to breach security systems and gain access to protected information. Cyber espionage poses a significant threat to national security and can have significant economic and political consequences. Therefore, organizations and governments must implement robust cybersecurity measures and remain vigilant against potential threats to prevent cyber espionage.

In December 2007, over 300 British companies were subjected to cyber espionage attacks by Chinese organizations.[109] This organized series of attacks was called "Titan Rain".[110] Titan Rain, also known as "Titan Rain 2.0," is a series of cyberattacks believed to be state-sponsored and mainly targeted the United States. These attacks were first discovered and reported in 2003 by U.S. government agencies and cybersecurity firms. "Titan Rain" refers to a specific Chinese cyber espionage campaign, although the Chinese government denied involvement.

The Titan Rain attacks focused on infiltrating the computer networks of various U.S. government agencies and defense contractors. The attackers were suspected of being based in China and were interested in stealing sensitive military and defense-related information. The attackers used various techniques, including phishing emails, malware, and social engineering, to access the targeted systems. The Titan Rain attacks were a significant and persistent threat to U.S. national security. Over the years, U.S. government agencies and private cybersecurity firms worked to improve their defenses and countermeasures against such cyber threats. Although the exact identity and motivations of the attackers were never definitively confirmed, the attacks raised awareness about the importance of cybersecurity and the need to protect critical government and defense infrastructure from cyber espionage and cyberattacks.
Ransomware is a type of malicious software that hackers use to encrypt data on computer systems or networks. After encrypting the data, the attackers demand payment for the decryption key. They usually exploit vulnerabilities in computer networks and operating systems to gain access. Once they have access, they encrypt the data and ask for payment in cryptocurrency, such as Bitcoin, to decrypt it. Unfortunately, these types of attacks have become more common in recent years. The attackers often threaten to delete or publish the victim's files if the ransom is unpaid. Ransomware attacks can devastate individuals and organizations, leading to the loss of sensitive data, financial losses, and damage to reputation.

Ransomware attacks can happen in various ways, including malicious downloads, phishing emails, or software vulnerabilities. Once the ransomware infects the victim's computer, it encrypts files and displays a ransom note that demands payment in exchange for the decryption key. The attacker may also threaten to increase the ransom amount or delete the files if the payment is not made within a specific timeframe. To protect against ransomware attacks, it is crucial to exercise caution when clicking links or downloading attachments from unknown sources. Ensure that your software is up to date with the latest security patches and use anti-virus software to detect and block malicious software. It is also essential to regularly back up your important files, as it enables you to restore your data in the event of a ransomware attack.
Money laundering is a long-standing global problem where illegally obtained funds are disguised as legally obtained. This financial crime is implemented at various levels, from small amounts to billions of euros.[111] Terrorists also use it to move funds between countries. Various businesses, such as gambling, pre-paid telephone cards, and trade in gold and jewelry,

generate large sums of money and cover money laundering.[112] The practice needs to be addressed by governments, financial institutions, and regulatory authorities through enhanced cooperation and information-sharing.

One of the most well-known systems used for money laundering is Hawala, an ancient system based on trust.[113] Hawala is an informal and traditional system of money transfer and remittance that has been used for centuries, primarily in parts of Asia, the Middle East, and Africa. It operates outside the conventional banking and financial system and is often characterized by its reliance on trust and personal relationships.[114] A US Treasury Department study identified hawala as the primary means of money laundering from drug trafficking and other crimes in Pakistan.[115] It revealed that Pakistan, India, and Dubai in the Persian Gulf formed the "Hawala triangle" to move money secretly worldwide. While Hawala can be used for legitimate purposes, such as providing a means for expatriates to send money to their families in their home countries, it is also susceptible to abuse for illegal purposes, including money laundering and terrorist financing. As a result, many countries have implemented regulations to monitor and control Hawala operations to prevent misuse.

Distributed Denial of Service (DDoS) attacks are a malicious technique cybercriminals use to disrupt computer systems. During a DDoS attack, the attacker sends an overwhelming amount of traffic or data to the targeted system or network, rendering it inaccessible to genuine users. The attacker may use a botnet, which is a network of compromised computers, to launch the attack. The botnet comprises computers infected with malware, which allows the attacker to control them without the owner's knowledge.[116] Once the attacker has control of the botnet, they can direct it to flood the target system with traffic or data, making it unable to respond to legitimate requests. It can result in system crashes or make it so slow that it becomes unusable. For businesses and organizations that depend on their computer systems, DDoS attacks can be catastrophic. The attacks can result in lost revenue, damage to reputation, and even legal liability. To protect against DDoS attacks, organizations can use specialized software and hardware to detect and block traffic from malicious sources.[117]

- Entities Targeted by TCOs

Transnational criminal organizations (TCOs) are complex and highly organized groups that operate across international borders to achieve their diverse objectives. These objectives range from gaining political leverage and disrupting economies to stealing sensitive data and financial assets. TCOs' targets are diverse, and they often focus their efforts on governments, multinational corporations, and individual citizens.[118] These criminals target governments and multinational corporations to gain access to sensitive information, exert political influence, or advance their strategic objectives. Multinational corporations, in particular, are attractive targets because of their vast financial resources and valuable data that hackers can steal, sell, or use to exert leverage.[119] Unfortunately, individual citizens are also frequently targeted through digital scams, identity theft, and other forms of fraud, which can have devastating effects on their lives.

These criminal organizations employ sophisticated tactics, such as cyber-attacks, phishing, and social engineering, to achieve their objectives. Their adaptability and versatility enable them to exploit opportunities in the digital landscape, making them a persistent threat to law enforcement and cybersecurity efforts.[120] With the ever-increasing complexity of TCOs, governments, private sector entities, and individuals must stay alert and take proactive steps to safeguard themselves against these threats. By being vigilant and implementing preventive measures, we can effectively protect ourselves from the potential harm caused by these sophisticated organizations.

- The Challenges Cybercrimes Pose to Law Enforcement

Law enforcement faces numerous challenges when it comes to combating cybercrimes. These crimes, which sophisticated hackers often commit, can be challenging to trace and prosecute. Additionally, cybercrimes can cross national borders, making it challenging for law enforcement agencies to coordinate and collaborate effectively. As technology evolves, cybercrimes become more complex and frequent, posing an ongoing challenge for law enforcement.

According to Holt (2018), technology has produced unintended consequences for society by creating opportunities for online and offline criminality.[121] The spread and ubiquity of technology make it easy for offenders to target victims in other countries, creating jurisdictional challenges for investigators.[123] Law enforcement agencies' response to cybercrimes has been complicated by jurisdictional limitations, budget and training issues, and potential interest among police management.[124]

Combating transnational cybercrimes is a complicated task that requires both legal and technical strategies. Law enforcement agencies from different countries collaborate to identify and capture cybercriminals. However, the challenges posed by the jurisdictional limitations and the secretive nature of cybercriminal operations in different areas make these efforts challenging.[125]

One of the most significant obstacles that local and state agencies encounter when addressing cybercrime is their limited staff and budget. Police management usually prioritizes the most pressing criminal issues identified by the local community to meet the needs of the population they serve.[126] These conditions create disparities in local agencies' investigative capabilities. They may influence line officers' perceptions regarding their need to investigate cybercrime rather than technology misuse, minimizing any focus on cybercrime. These conditions create disparity in local agencies' investigative capabilities and may shape line officers' perceptions of their need to investigate cybercrime.[127]

Local and federal law enforcement agencies face similar challenges in responding to cybercrime. The Federal Bureau of Investigation (FBI) and the U.S. Secret Service are two agencies responsible for investigating domestic and international cybercrimes.[128] These agencies employ various techniques and tools to gather evidence and track down cybercriminals who engage in hacking, identity theft, and other cyber-attacks. Through their work, they aim to protect individuals, organizations, and the country's critical infrastructure from the harmful effects of cybercrime.[129] However, they are limited by existing legislation and cooperative agreements with other countries.

- Case Studies and Lessons Learned

Exploring noteworthy case studies is crucial to developing a thorough comprehension of the matter at hand. By delving into two significant case studies, we can gain insight into the methodologies implemented by TCOs and the corresponding law enforcement responses. These case studies offer a wealth of information to help us better understand the issue and take informed action.

- The Not Petya Ransomware Attack

In 2017, Russia launched a ransomware attack against a Ukrainian tax preparation software company, which became known as the NotPetya attack. This was part of Russia's long-standing assault on Ukraine.[130] The attack infected dozens of Ukrainian companies and institutions, including the National Bank of Ukraine, and caused significant global impact, affecting organizations in various countries.[131] The attack led to billions of dollars in damages, and victims included international shipping company Maersk, Mondelēz International, and pharmaceutical giant Merck, as well as smaller entities.[132] The attack encrypted files on infected computers, making them inaccessible and causing operational standstills for the victim organizations. Despite the ransom demands, paying did not result in file recovery, leading to the conclusion that the primary purpose was not financial gain but rather disruption and destruction. Mondelēz, the owner of well-known food brands like Cadbury chocolate and Philadelphia cream cheese, was among the hundreds of companies affected by the NotPetya cyberstrike. As Mondelēz employees worked at their desks, laptops froze suddenly, email and access to files on the corporate network became unavailable, and logistics software that orchestrates deliveries and tracks invoices crashed.[133]

The malware used in the NotPetya attack spread using the same EternalBlue exploit that was used in the WannaCry ransomware attack, which targeted a vulnerability in Microsoft Windows systems. The malware also employed other propagation methods, such as exploiting weak or default passwords. This notorious cyberattack, concealed as a seemingly innocent software update, is a stark example of the escalating threat of transnational cybercrime. The attack targeted multinational corporations in multiple countries, resulting in significant financial losses and

operational upheaval. It highlighted the sophisticated strategies adopted by Transnational Criminal Organizations (TCOs) to breach and subvert secure systems. Additionally, it underscored the challenge of tracing the origins of cybercrimes to specific entities, perpetuating an unsettling mystery regarding the perpetrators' identity.[134] This high-profile cyberattack emphasized the urgent need for enhanced cybersecurity measures and international cooperation to combat the ever-evolving landscape of digital threats in our interconnected world.[135]

- Lessons Learned

The NotPetya ransomware attack in June 2017 taught us some essential lessons about cyber security and the ever-changing threat landscape. It can be challenging to determine who is responsible for cyberattacks, as attribution can be complex and inconclusive. Despite initial assumptions that it was a criminal ransomware attack, further analysis suggests it was likely a state-sponsored or state-supported operation. This uncertainty highlights the challenges in identifying the true culprits of cyber attacks. The attack underscores the importance of cyber security and the need for regular updates to defend against evolving threats, while international cooperation is essential for investigating and prosecuting such cases.[136] It is a stark reminder that organizations must take robust cyber security measures, continuously monitor threats, and take a proactive approach to address evolving cyber threats. Organizations need to prepare for not only financially motivated attacks but also those aimed at causing disruption and destruction.

- The Lazarus Group's Bank Heists

The Lazarus Group, a notorious cybercriminal syndicate allegedly affiliated with North Korea, is notorious for executing a string of audacious bank heists. Their most infamous exploit was the Bangladesh Bank theft.[137] In February 2016, the group attempted to steal nearly $1 billion from the Bangladesh Bank's account at the Federal Reserve Bank of New York. They used a combination of malware, social engineering, and fraudulent transactions to transfer funds from the Bangladesh Bank's account to various locations worldwide.[138] The Lazarus Group employed "SWIFT" malware; a sophisticated malware strain that targeted the SWIFT financial messaging system used by banks for international money transfers.[139] The group accessed the Bangladesh Bank's SWIFT terminal, sent fraudulent transfer requests to the Federal Reserve Bank, and routed the stolen funds through a series of correspondent banks.[140]

The Lazarus Group is believed to be financially motivated and operates at the behest of the North Korean government. Their involvement in bank heists and financial cybercrimes is a means to fund North Korea's regime, which faces economic sanctions and isolation. The group's hacking methodologies are cutting-edge, and they systematically infiltrated financial institutions to steal multimillion-dollar hauls. Their actions highlight the increasingly brazen and sophisticated tactics of state-sponsored transnational cybercriminal organizations, shedding light on the evolving cybercrimes perpetrated by these well-resourced and highly elusive entities.[141] The Lazarus Group's exploits continue to raise concerns about the security of global financial systems and the need for enhanced cybersecurity measures.

The group's involvement in bank heists highlights the growing sophistication of state-sponsored hacking groups and their ability to target financial institutions globally. The group's activities have prompted financial institutions and governments to enhance their cybersecurity measures and collaborate on efforts to prevent and respond to cyber threats. Attribution is often challenging in the cyber realm. However, the U.S. government, private cybersecurity firms, and international investigators have linked the Lazarus Group to North Korea as the likely perpetrator of the Bangladesh Bank heist. The group's use of malware and techniques similar to those in other Lazarus Group operations contributed to this attribution.

- Lessons Learned

Valuable insights have been gleaned from the cyberattacks perpetrated by the Lazarus Group on financial institutions. Cybersecurity experts, governments, and financial organizations alike should heed these lessons. Enhanced attribution capabilities are crucial in identifying state sponsored TCOs. According to Park (2021), international sanctions and diplomatic efforts should be strengthened to combat state actors who support cybercriminal activities.[141] The main takeaways are the need to acknowledge

threats sponsored by nation-states, address any vulnerabilities in the SWIFT system, prioritize regulatory compliance, invest in cybersecurity measures, and encourage employee security awareness and training.

- Women as Transnational Organized Criminals

It is important to note that women may not always be as visible or well-documented as men when it comes to their involvement in transnational crime and cybercrime. Gender disparities in these fields can result in underreporting or underrepresentation. Law enforcement agencies and cybersecurity professionals are working to address these issues and understand the diverse roles individuals, regardless of gender, can play in these criminal activities.

In both transnational organized crime and traditional local contexts, women have reached top positions. Powerful godmothers have always been engaged in illicit activities and illegal trade, operating in different circumstances from 'cross-border female criminals.' These women have achieved their position in a specific context due to local economic conditions and law enforcement operations against local male criminals. Women are no longer invisible in both forms of organized crime.[142] They are becoming fully involved in the enterprise of crime, keeping the books, taking care of the organization, and ordering violent retaliation.[143]

In the 1990s, law enforcement in Italy was successful in combating the mafia. However, this success ironically led to changes within the criminal organizations. As a result, wives, daughters, sisters, and even grandmothers have started to engage in criminal activities.[144] Pizzini-Gambetta reports that 82% of women involved in Cosa Nostra activities and 79% involved in clan activities in Bari (Apulia) are related by kin or marriage to male members of those groups.[145] Maria Licciardi, also known as 'La Piccolina,' is the daughter and sister of the Secondigliano bosses. She leads an alliance of 20 criminal clans of the Camorra. Although her name vanished from the headlines during the mafia war in the 2000s, her power only increased while she remained free. Another woman, Concretta Scalisi, is considered the leader of the powerful clan of Laudani in Catania.[146]

Kalina Michailovna Nikiforova, known as 'Kalya,' was a notorious godmother in the Russian criminal underworld during the 1990s. She was particularly well-known for her exceptional business skills in dealing with stolen goods, particularly antiques, gold, and other valuable items. Her managerial and organizational abilities, combined with her international connections, made her a successful figure who rose to the top of the Russian mafia.[147] Nikiforova's story serves as an example of how the criminal world has changed, similar to those seen in the legal business world, where female managers are now occupying more and more prominent positions.[148]

Implications for Addressing Transnational Cybercrime

The implications of these research findings are significant for combating transnational cybercrime. To effectively address this issue, international cooperation is crucial. Enhancing coordination among nations and organizations to share threat intelligence, conduct joint investigations, and streamline extradition processes is essential. Additionally, the private sector must take an active role in enhancing cybersecurity measures. Lastly, investing in cyber resilience and cutting-edge technologies for attribution and deterrence will help to deter transnational criminal organizations (TCOs).[149]

- Implications for the field of International Relations

The research presented in this paper is of utmost importance in global cybersecurity and law enforcement. It underlines the pressing need to tackle transnational cybercrimes as a significant security concern in international affairs. The study further emphasizes the vital role of implementing all-encompassing global strategies in addressing cybersecurity threats, given the borderless nature of cybercrimes and their impact on diverse stakeholders.[150]

The impact of cybersecurity in global affairs is of utmost importance due to its extensive ramifications. With the increasing prevalence of technology and the internet, cyber-attacks have become more frequent, highlighting the importance of cybersecurity in international relations. The severity of cyber-attacks is evident, with the potential to cause widespread harm to national security, economic stability, and infrastructure, leading to grave outcomes.

Additionally, cyber-attacks can be conducted for criminal purposes or as part of intelligence collection or sabotage operations. Since cyber-attacks cross borders and pose a threat to critical infrastructure worldwide, cybersecurity has become a popular topic in international relations (IR) and security studies.[151]

In today's world, nations are increasingly using cyber-attacks to gain an edge over their rivals. This shift towards cyber warfare has highlighted the importance of robust cybersecurity measures. The EU and its partner countries recognize the need to protect critical infrastructures and institutions from cyber threats.[152] The European Union has taken a firm stance against cyberattacks by adopting the Common Foreign and Security Policy (CFSP) Decision 2019/797. This decision empowers the EU to take action against cyberattacks that pose a risk to the security of the EU or its member states. It allows the EU to impose restrictive measures to respond to such cyberattacks, ensuring that external threats are dealt with swiftly and effectively.[153] The Agreement between the USA and Europol, signed in 2001, aims to enhance cooperation between the Member States of the EU, acting through Europol, and the US in preventing, detecting, suppressing, and investigating severe forms of international crime, mainly through the exchange of strategic and technical information.[154]

In the modern world, the proper functioning of states and societies relies heavily on information technology (IT) infrastructure. However, this reliance also exposes new digital vulnerabilities that can be exploited with minimal resources, leading to significant harm and threatening international stability.[155] While the internet has opened up numerous business opportunities and given individuals a platform to express themselves freely, it has also become a breeding ground for criminal and politically motivated cyber-attacks, some backed by states. These incidents often lead to reactions from both governments and international organizations.[156]

In the modern era, cybersecurity has emerged as a critical element of global affairs, necessitating the involvement and cooperation of several nations. International laws and regulations are essential to address cybersecurity challenges that transcend borders effectively. Establishing worldwide standards and norms for responsible conduct by states in cyberspace is crucial to mitigating the risk of cyber-attacks. Furthermore, effective collaboration between countries in exchanging information, intelligence, and technology is essential for thwarting cyber threats. The issue of cybersecurity has evolved into a multifaceted concern in international relations, requiring a comprehensive and unified strategy.

The significance of cybersecurity in global relations has grown considerably, highlighting the importance of countries working collaboratively to establish international laws and regulations governing cyber activities. Creating international norms and standards for responsible state behavior in cyberspace is vital in reducing the risk of cyber-attacks. Countries must share information, intelligence, and technology to combat cyber threats. Nevertheless, an ongoing discussion exists on how territorial sovereignty applies to cyberspace.[157] While cyber activities have a physical aspect, interactions in cyberspace possess a virtual dimension through the transmission of data, signaling, and sending of content between physical devices.

In 2017, the Chinese government released a report called "International Strategy of Cooperation on Cyberspace" (ISCC). It advocates for principles like "peace, sovereignty, shared governance, and shared benefits" to guide international digital collaboration.[158] The ISCC has six strategic goals, including protecting sovereignty and security, developing international rules, and promoting cooperation on the digital economy. Additionally, it outlines nine specific action plans to promote international cooperation in cyberspace.[159] No nation should pursue cyber supremacy, interfere in other countries' domestic affairs, or engage in cyber activities that undermine another nation's national security.

Cyber-attacks conducted by one country against another are becoming increasingly frequent.[160] Tallinn Manual 2.0 created by international lawyers, aims to facilitate the regulation of cyber operations by international law.[161] This manual is just the beginning of a more comprehensive conversation about the application of international law to countries' cyber

operations in peacetime, and it is hoped that this paper will contribute to that discussion.[162]

The Tallinn Manual 2.0 provides a comprehensive regulatory framework comprising 154 rules delineating cyber operations' general legal principles and their interface with specialized international law regimes, including human rights, diplomatic, space, and telecommunication law.[163] The Tallinn Manual 2.0 adopts an approach that draws rules from sovereignty and non-intervention and applies them to operations conducted in cyberspace.[164] According to Rule 4, a State is prohibited from engaging in cyber operations that infringe on the sovereignty of another State.[165] The esteemed international group of experts opines that such violations encompass physical damage, loss of functionality, or interference with inherent government functions.

As per Moynihan's 2019 article, the Dutch government recognizes the finite nature of sovereignty in the digital realm. They endorse the fourth guideline of the Tallinn Manual 2.0, which aids in defining these constraints. Several countries propose that the magnitude and scope of societal repercussions should be considered before determining if a cyber assault violates sovereignty. Meanwhile, others concentrate on the attack's impact on the victim state's regulatory authority over its territorial sovereignty.[166]

- International Relations and Transnational Criminal Organizations

The exploitation of technology by transnational criminal organizations to commit cybercrimes poses complex challenges for International Relations. Such activities can disrupt the stability and security of nations and regions, blurring the lines between domestic and international concerns. Addressing these challenges requires increased international cooperation, diplomatic efforts, and the development of legal and policy frameworks that enable nations to work together to combat transnational crime and preserve global security and stability. Although transnational organized crime (TOC) has not been central to IR theories it is an international phenomenon with significant implications for international security, world politics, international trade, and human rights.[167] Thus, it should be explained and understood both theoretically and empirically. This would help scholars of IR to portray a more accurate picture of the contemporary international system.[168]

In the realm of international relations, non-state actors are entities that wield significant economic, political, or social influence on a national or global scale. These organizations or individuals operate independently of any particular government and are not financially supported or directed by them. Non-state actors include corporations, non-profit organizations, business magnates, non-governmental organizations, religious groups, aid agencies, and people's liberation movements.[169]

Scholars in international relations recognize the critical role of non-state actors in promoting economic liberalization, peace, and the rule of law.[170] Most literature in international relations (IR) privileges non-state actors (NSA), which arguably contributes to the embodiment of economic liberalization, international peace, and law.[171]

According to Thomas Hobbes' realism theory, non-state actors significantly shape international policies.[172] Hobbes believes that the state of nature lacks culture or community, which can provide a social framework for human interaction.[173] Morgenthau[174] notes Hobbes' influence on the structural understanding of the realist tradition.

In his book 'Leviathan,' Hobbes explains how the sovereign came into existence because of the natural faculties of human beings.[175] According to him, human beings are driven by desire - pleasurable and aversion - pursuits that cause displeasure. Since the ultimate goal for all human beings is self-preservation, they are all self-interested and strive to maximize their capabilities for a comfortable life.[176]

Hobbes' works exhibit rationalism by depicting human nature.[177] While passions may guide individuals, Hobbes does not categorize them as beasts since they possess a capacity for reason. According to Hobbes, reason is an arbiter between desire and aversion, determining human behavior. The state is a product of a rational approach to the state of nature.[178] The influence of Hobbes's thought is evident in the realist emphasis on determining self-interest through reason.[179] Hobbes also notes that the fear of death and

the desire for comfortable living, which are the primary driving forces behind human behavior, also lead individuals out of the state of nature through reason.[180]

Thus, creating an environment that promotes the respectful exchange of diverse perspectives is crucial to fostering peaceful coexistence. This approach emphasizes the importance of considering all parties involved in international relations, including non-state actors, to achieve positive outcomes and maintain global stability.

According to Hobson's concept of 'realms of opportunity' and 'realms of constraints,' structural mechanisms in internal and external contexts present both opportunities and constraints for each actor.[181] As a result, actors respond to these structural stimuli and adjust their policies, accordingly, indicating their adaptive nature and dynamic evolution in the socio-historical process. Hezbollah is a critical factor that leverages structural possibilities to strengthen its actor-hood.[182]

Hezbollah is a network of radical Shiite groups and organizations that follow a Khomeinistic ideology. It was formed after the 1982 Peace for Galilee War in Lebanon and the subsequent rise in Iranian influence.[183] Hezbollah's External Security Organization, with the help of the Lebanese Shiite diaspora in different parts of the world, has been accused of engaging in criminal activities globally. Despite its territorial divisions following Lebanon's governorates and three-tier formal structure overseeing religious, military, political, and social affairs, Hezbollah is still considered hierarchical. This information comes from Rudner's 2010 report, which cites the Party of God's involvement in criminal activities[184] and Azani's 2013 report, which discusses its organizational structure.[185]

Hezbollah is a complex organization that adapts to changes in its internal and external environment. Various factors shape its structure and influence those factors, leading to changes in both internal and external realities. Actors adjust policies based on structural stimuli in the social-historical process, reflecting their adaptive character and dynamic evolution. Structuration theory captures this idea.[186]

Structuration theory is a social theory of creating and reproducing social systems based on analyzing structure and agents without giving primacy to either. It states that social structures are created by human action and interaction and that they, in turn, constrain and enable that action and interaction. Sociologist Anthony Giddens developed it in the late 1970s as a response to the limitations of traditional structuralist and individualist theories.[187]

Collaboration and good governance are essential for effective leadership, and non-state actors play a crucial role in achieving these goals. Their contributions are vital in making the world a better place for everyone while ensuring that life is sustainable for all. However, non-state actors face many challenges, including criminal activities, bad governance, poor business environments, extreme weather conditions, human rights violations, and restrictions on fundamental freedoms. Despite these obstacles, non-state actors provide essential services such as healthcare, employment, and non-refundable loans to low-income earners, facilitate critical projects such as water and electricity, and offer relief to developing nations. Additionally, they can promote security, sovereignty, and survival by preventing political, social, and economic conflicts and wars. Therefore, the goodwill and contributions of non-state actors are fundamental to international relations matters.[188]

Theoretical implications of the rise of non-state actors
The involvement of non-state actors, such as transnational criminal organizations, is a constantly changing aspect of the International Relations field. The emergence of non-state actors like non-governmental organizations, multinational corporations, and civil society groups has significant theoretical implications for international relations. These actors are increasingly important in shaping global governance and policymaking, especially in human rights, environmental protection, and sustainable development. Research into the role of non-state actors in international relations has revealed that they contribute to a sustainable life and are crucial in making the world a better place for all.[189]

The emergence of non-state actors in international relations has given rise to intricate and far-reaching theoretical implications that demand thorough

exploration. These actors and their growing influence on global affairs have altered the course of international politics in novel and unexpected ways, underscoring the need for a deeper comprehension of their role in shaping the contemporary world order. In order to effectively combat transnational cybercrimes, a multilateral strategy is imperative, which could lead to the formation of international treaties, conventions, and agreements aimed at tackling cybercrime. A range of organizations, including INTERPOL, The Budapest Convention on Cybercrime, The Global Cybersecurity Alliance, The Cybercrime Support Network, National Cybersecurity Strategies, and The United Nations Convention against Transnational Organized Crime, can play a crucial part in this endeavor.

The potential to foster advanced international peace is one of the most significant implications of non-state actors. Non-governmental organizations (NGOs), international organizations, and civil society groups are just a few examples of these actors that can facilitate international cooperation and aid in resolving conflicts between states. The rise of non-state actors has also significantly impacted their ability to advocate for social and political issues. By promoting specific policies and ideas, they can influence the political agenda. Furthermore, non-state actors can act as watchdogs, scrutinizing the actions of state actors and holding them accountable for their behavior.

The International Criminal Court (ICC) was established to hold state actors accountable for political conflicts and human atrocities. The establishment of the International Criminal Court (ICC) has provided a platform for addressing political conflicts and human atrocities, and it holds state actors accountable for their actions. Regardless of their position in their own country, even if they are a president or a king, they are not above the law and can be held accountable by the ICC. Since its inception in 2002, the ICC has been controversial and criticized among its critics and supporters.[190] Despite this, the creation of the ICC has contributed to the "justice cascade," which has led to positive global developments in international criminal justice.[191]

The International Criminal Court (ICC) was established to address political conflicts and human atrocities. It serves as a forum for holding state actors accountable for their actions. Even if a president or a king is above the law in their own country, they can still be held responsible by the ICC, where they are not above the law. The ICC has been in operation since 2002 and has been the subject of controversy and criticism from its supporters and detractors. However, the creation of the ICC has contributed to what is now known as the "justice cascade." This has led to positive global developments in international criminal justice.[192]

The IMF, or International Monetary Fund, is a global organization that strives to promote international monetary cooperation and stability in exchange rates. Its main objective is to foster balanced international trade, sustainable economic growth, and poverty reduction among its member countries. The IMF achieves these goals by providing members with developmental capital, which can finance infrastructure and other beneficial projects such as education, healthcare, and social welfare programs. Additionally, the IMF offers its members technical assistance and policy advice to help them implement sound economic policies and strengthen their institutions. The IMF works towards creating a more stable and prosperous global economy through collaboration with member countries.[193]

INTERPOL, the International Criminal Police Organisation, is the largest and oldest organization for police cooperation worldwide.[194] Its primary objective is to enforce international laws and maintain order. The establishment of INTERPOL has exhibited a common interest among subjects of international law to create a means of combating domestic and international organized crime. Its years of successful operation and the increasing number of member states, currently at 194, confirm its feasibility and the urgency of further operation.[195]

INTERPOL should be noted for its ability to adapt to external factors that may impact its operations, such as cross-border threats, integration processes, democratization, and globalization.[196] It collaborates closely with law enforcement agencies in about 190 member countries to support investigations into cross-border crimes like terrorism, human trafficking, cybercrime, and drug trafficking. Additionally, it

assists countries with borders and internal political conflicts to maintain security and prevent violence.

The World Health Organization (WHO) was founded in 1948 by the United Nations to promote global health and well-being.[197] Its mandate is universal health coverage, including essential services such as immunization, maternal and child healthcare, and primary healthcare. In addition, WHO helps countries prepare for and respond to health emergencies such as pandemics, natural disasters, and outbreaks of infectious diseases. The organization collaborates closely with governments, civil society, and other partners to ensure that quality healthcare is accessible to everyone. WHO is creation resulted from the amalgamation of several existing organizations that represented a long history of international health cooperation dating back centuries.[198]

- Future Trends

Technology, tactics, and interconnectivity shape the future of cyberattacks. As new technologies emerge, such as WiFi, healthcare devices, robots, and drones, they become highly vulnerable targets for cyber-attacks. With the widespread use of WiFi technology among individuals and industries, there is an increased risk to the security of personal data and company information. To counter these threats, organizations and governments must invest in advanced cybersecurity measures, threat intelligence, and collaboration. In today's rapidly changing cyber landscape, it is essential to take proactive security measures and continuously monitor emerging threats. Regulatory frameworks and international cooperation also play a vital role in addressing global cyber threats. The *Key Reinstallation Attack* (KRACK) is a security vulnerability that affects the WiFi Protected Access 2 (WPA2) protocol, a widely used security protocol for securing WiFi networks. KRACK, short for "Key Reinstallation Attacks," is a weakness discovered by Mathy Vanhoef, a postdoctoral researcher with the iMinds-DistriNet Research Group at KU Leuven University in Belgium, in the WiFi network security standard WiFi Protected Access 2 (WPA2).[199] This vulnerability can allow an attacker to intercept and decrypt data transmitted over a WPA2-protected WiFi network.[200]

A signal-jamming attack, often called "jamming," is a form of electronic warfare where an attacker intentionally emits radio frequency signals to disrupt or overpower legitimate wireless communications. The primary goal of a jamming attack is to interfere with the functioning of wireless devices, such as radios, cellular phones, WiFi networks, GPS systems, and other communication systems, by flooding the airwaves with noise or interference.

Implantable medical devices (IMDs) used in the healthcare sector are vulnerable to security breaches that can cause harm to patients. In 2008, Harvard Medical School cardiologist William Maisel coauthored a paper that revealed how hackers could reprogram an IMD without authorization.[201] These devices, which include pacemakers, implantable cardiac defibrillators (ICDs), drug delivery systems, and neurostimulators, are used to manage various ailments such as cardiac arrhythmia, diabetes, and Parkinson's disease.[202] However, traditional safety measures such as ID numbers and redundancy do not prevent intentional failures and other security and privacy issues like replay attacks. As IMDs become more interconnected and essential to healthcare, it is crucial to address their cybersecurity vulnerabilities to safeguard patient privacy and safety.[203] Regulatory bodies, standards organizations, and the healthcare industry are vigorously working together to enhance the security of these devices.

- Cybercrime is Underreported

Underreporting and incomplete data present a significant challenge to researchers studying cybercrimes committed by TCOs. Due to concerns about reputational harm, legal implications, or the difficulty of identifying the offenders, many cybercrimes go undiscovered or unreported. This underreporting leads to incomplete and skewed data, making it challenging to obtain a comprehensive picture of the true extent of TCO involvement in cybercrimes. This limitation may result in quantitative analysis underestimating the frequency and impact of these crimes. Researchers can address this issue by exploring novel approaches to estimate underreporting, such as conducting surveys to ascertain the public's perspectives and experiences about cybercrimes.

Moreover, promoting reporting procedures and encouraging victims to come forward can aid in reducing this restriction. To ensure the credibility of the findings, acknowledging the study's limitations, such as data availability, geographic scope, and underreporting, is crucial. Researchers can overcome these limitations by collaborating with international partners, fostering information sharing, developing protocols for anonymizing sensitive data and exploring novel approaches to estimating underreporting levels.

The "State of Cybersecurity 2019" report presents the results of the annual ISACA® Global State of Cybersecurity Survey, conducted in November 2018.[204] Some findings reinforce discoveries from prior years, specifically that the top attacks and threat actors remain largely the same. Other findings provide new insight into cybersecurity management. Respondents indicate that cybersecurity departments are best served when reporting to either a chief information security officer (CISO) or chief executive officer (CEO) rather than reporting to a chief information officer (CIO). The report offers an outlook on cybersecurity from the perspective of cybersecurity managers and practitioners. According to 75% of respondents, cybercrime instances are intentionally suppressed, leading to underreporting and skepticism of statistics presented by governments and businesses.[205]

RECOMMENDATIONS

To combat transnational cybercrimes effectively, governments, law enforcement agencies, and international organizations must establish mechanisms for real-time information sharing, joint operations, and coordinated efforts.[206] Collaboration between governments and private-sector entities can improve cybersecurity measures and facilitate threat intelligence sharing. Private companies should also invest in robust cybersecurity practices to safeguard their data and assets.[207] Advanced technologies for attribution are necessary to identify and prosecute transnational cybercrime organizations (TCOs), which can be achieved through investment in state-of-the-art tools. To ensure that cybercriminals face legal consequences for their actions, policymakers should work on simplifying the extradition process and harmonizing international legal frameworks.[208] Raising public awareness and providing cybersecurity education to individuals and organizations is crucial in reducing the success of cybercriminals. With an informed and vigilant public, cybercrime victims can be avoided. Lastly, allocating adequate resources to law enforcement agencies and cybersecurity initiatives is essential for effectively combating cybercrimes.[209]

LIMITATIONS

Studying cybercrimes committed by Transnational Criminal Organizations (TCOs) is a complex task that presents various challenges and potential issues researchers must consider. While the research design and methods provide a comprehensive framework for studying these crimes, acknowledging the study's limitations is crucial to ensure the credibility of the findings. A primary hurdle that researchers face is the need for more accurate and comprehensive data due to TCOs operating covertly, making it challenging to obtain reliable information. Law enforcement agencies and cybersecurity firms may only occasionally share complete information due to concerns about revealing sensitive investigative methods or classified information, leading to incomplete or biased findings. Researchers can overcome this barrier by encouraging information sharing while respecting confidentiality concerns and developing protocols for anonymizing sensitive data.

Furthermore, the study's geographic scope is another area for improvement. Cybercrimes committed by TCOs are typically transnational, spanning multiple countries and jurisdictions. Researchers may require additional support to ensure thorough coverage of all geographical locations, as geographic bias could impact the accuracy and generalizability of findings. Different regions may have varying levels of cybercrime reporting, law enforcement capabilities, and data collection infrastructure, leading to incomplete or skewed data. To address this limitation, researchers can include diverse cases from various regions and collaborate with international partners to access data from a broader geographical spectrum. Understanding the geographic scope restriction in the study's conclusions is essential in contextualizing the results.

CONCLUSION

The comprehensive review in this paper has covered several types of cybercrimes committed by various transnational criminal organizations and analyzed numerous studies regarding their achieved detection rates and some of their limitations. This study has also intensively discussed the available literature that previous studies have used. Finding the proper dataset for testing and evaluating the research's method for cybercrime detection are critical challenges. This study has shown that cybercrime in developing and developed countries is rapidly gaining root. The leading offenders of cybercrimes are young people with technical expertise and experience in the committing of computer-related crimes. The research also revealed a discrepancy between the laws of nations, organizations, and authorities empowered to fight cybercrime. This research found that traditional legislation and regulations are presently unable to mitigate cybercrime instances, which is why it is essential to evaluate them so that they include new modifications in technology. It is also apparent that cybercrime in certain nations is underreported.

Furthermore, the research has highlighted the cybercrime intensity worldwide. Transnational criminal organizations have exploited vulnerabilities in cyberspace on a global scale by leveraging technological advancements. This study has explored the scale and scope of their activities, the tools and technologies they employ, the diverse entities they target, and the challenges law enforcement agencies face.[210] Notable case studies have illustrated the sophistication of TCOs and the difficulties attributing cybercrimes to specific actors. The implications for addressing transnational cybercrime are significant, emphasizing the need for international cooperation, public-private partnerships, advanced attribution capabilities, improved legal frameworks, and cybersecurity education. In the context of global cybersecurity, these findings underscore the urgency of addressing this evolving threat and the imperative to adapt and strengthen our defenses in cyberspace.[211] In order to effectively combat cybercrime, it is crucial to establish worldwide harmony in cybercrime regulations and laws. Consistency is vital in successful enforcement efforts. This is why it is essential to prevent confusion by implementing measures that promote uniformity. Cybercrime, as mentioned, is viewed differently in different nations. It is essential that all countries worldwide establish a uniform categorization of computer crimes. Understanding cybercrime's financial and nonfinancial motives is crucial for effectively preventing and combating these activities. It is crucial to take proactive measures to safeguard sensitive information. This can include using robust passwords, regularly updating software, and remaining vigilant against potential cyber threats. The study's comprehensive research design and methods aim to provide a comprehensive understanding of TCOs' involvement in cybercrimes, contributing to ongoing efforts to combat cybercrimes and safeguard global digital security.[212] The research design and methods section provides a comprehensive understanding of the study on cybercrimes committed by transnational criminal organizations. The study aims to investigate the involvement of TCOs in cybercrimes, which is a complex and challenging task due to the secretive and adaptable nature of these criminal enterprises.

To address this challenge, researchers utilize quantitative and qualitative methods to gather and analyze data on cybercrimes committed by transnational criminal organizations (TCOs). The study also employed various data collection methods, including surveys, interviews, and case studies, to ensure the data is of high quality and integrity. Documented interviews and surveys gather insights from experts, law enforcement officials, and individuals or organizations affected by cybercrimes involving TCOs. The aim is to enhance the depth and scope of the research and address the limitations discussed in the main paper.[213] Valuable information gained from the responses can help combat cybercrime.

The data and findings are systematically analyzed, and conclusions are drawn while considering the study's limitations. The research design also emphasizes the importance of selecting appropriate cases for investigation, and a multi-step approach will be used to identify the most relevant and significant cases. Analyzing selected cases using multiple data sources provides a comprehensive understanding of TCOs' cybercrime involvement. The researchers must be aware of the constraints and challenges of

investigating cybercrimes committed by TCOs and work diligently to overcome them to ensure the validity and application of their findings. It is essential to research TCOs' involvement in cybercrimes to combat cybercrime globally.

Efforts to combat tech-enabled global cybercrimes committed by Transnational Criminal Organizations (TCOs) require a comprehensive understanding of these criminal networks' tactics, techniques, and strategies. For this reason, a thorough and meticulous analysis of the extensive data and findings collected throughout the research is imperative. This will enable researchers to identify patterns and trends in TCO activity and develop effective countermeasures to combat their illegal activities. The research has collected information on the various types of cybercrimes committed by TCOs, including hacking, phishing, and ransomware attacks, as well as their preferred targets and methods of operation. The study's findings will contribute to ongoing efforts to combat cybercrimes and safeguard global digital security. Acknowledging the study's limitations, such as data availability or geographic scope, is essential to interpret the findings correctly.

Final Remarks

A comprehensive knowledge of organized cybercrime is essential in the efforts of law enforcement to prevent, investigate, and prosecute these intricate offenses. It is crucial to have a firm understanding of the modus operandi of cybercriminal groups in order to create targeted prevention measures. Digitalizing systems and integrating built-in security and control mechanisms is necessary to forestall potential system abuse. Furthermore, investigative measures and techniques must evolve to keep pace with the constantly changing cybercrime trends. Given that Cyber-OC has an international reach, law enforcement agencies must collaborate on a global level to stay ahead of criminal groups and their movements.

SUB REFERENCES

[1] Kethineni, Sesha, and Ying Cao. 2020. “The Rise in Popularity of Cryptocurrency and Associated Criminal Activity.” *International Criminal Justice Review* 30 (3): 325–44.

[2] Décary-Hétu, David, and Benoit Dupont. 2012. “The Social Network of Hackers.” *Global Crime* 13 (3): 160–175. https://doi.org/10.1080/17440572.2012.702523.

[3] Broadhurst, Roderic, Peter Grabosky, Mamoun Alazab, and Steve Chon. 2014. “Organizations and Cyber Crime: An Analysis of the Nature of Groups Engaged in Cyber Crime.” *International Journal of Cyber Criminology* 8 (1): 1–21.

[4] Leukfeldt, E. Rutger, Edward R. Kleemans, and Wouter P. Stol. 2017. “A Typology of Cybercriminal Networks: From Low-Tech All-Rounders to High-Tech Specialists.” *Crime, Law, and Social* Change 67 (1): 21–37.

[5] Bose, Malobika and Sonalika Gupta. 2022. “Digital Financial Services: Emerging Issues and Challenges.” The Next Normal: Building Agile, Sustainable, Tech-enabled Organizations, (*TNN–BASTO-2022*), 44-54.

[6] Bose and Gupta 2022, 44

[7] Adebowale, Moruf A., Khin T Lwin., and Hossain, M. Alamgir. 2023. "Intelligent phishing detection scheme using deep learning algorithms", *Journal of Enterprise Information Management* 36(3),747-766.

[8] Weber, Julia, and Edwin W. Kruisbergen. 2019. “Criminal Markets: The Dark Web, Money Laundering and Counterstrategies - An Overview of the 10th Research Conference on Organized Crime.” *Trends in Organized Crime* 22 (3): 346–56.

[9] Bulanova-Hristova, Gergana, Kasper Karsten, Odinot Geralda, Verhoeven Maite, Pool Ronald, Poot Christianne, Werner Yael and Korsell Lars. 2016. “Cyber-OC- Scope and manifestations in selected EU member states.” 1-299.

[10] Bulanova-Hristove et al. 2016, 2

[11] Dastjerdi, Shirin Ahmadi, and Abbas Sheikholeslami. 2019. “The Effect of Globalization on the National Criminal Law Systems.” *Library Philosophy and Practice* (4): 1–13.

[12] Dastjerdi and Sheikholeslami 2019, 3

[13] Jeronimo, Advento. 2019. “The Globalization Effect of Law and Economic on Cybercrime.” *Jurnal Pembaharuan Hukum* 6 (3).

[14] Dastjerdi and Sheikholeslami 2019, 1
[15] Catino, Maurizio. 2020. “Italian Organized Crime Since 1950.” *Crime and Justice* (Chicago, Ill.) 49 (1): 69–140. https://doi.org/10.1086/707319.
[16] Paarlberg, Michael Ahn. 2022. “Transnational Gangs and Criminal Remittances: A Conceptual Framework.” *Comparative Migration Studies* 10 (1): 1–20.
[17] Paarlberg 2022, 6
[18] Etges, Rafael, and Emma Sutcliffe. 2008. “An Overview of Transnational Organized Cyber Crime.” Information Security Journal 17 (2): 87–94.
[19] Millán-Quijano, Jaime. 2020. “Internal Cocaine Trafficking and Armed Violence in Colombia.” *Economic Inquiry* 58 (2): 624–41.
[20] Gulyás, Attila. 2022. “Lazarus’ The North Korean Hacker Group.” *International Scientific Conference Strategies* XXI, 75–83.
[21] “The WannaCry Ransomware Attack.” 2017. *Strategic Comments* 23 (4): vii–ix.
[22] Gulyás 2022, 79
[23] Gulyás 2022, 79
[24] Gulyás 2022, 79
[25] Gulyás 2022, 79
[26] Jensen, Benjamin, Valeriano, Brandon, and Maness, Ryan. 2019. “Fancy Bears and digital trolls: Cyber strategy with a Russian twist.” *Journal of Strategic Studies* 42(2), 212–234.
[27] Sanger, David and Charles Savage. 2016. “U.S. Says Russia Directed Hacks to Influence Elections” New York Times.
[28] Jensen et al. 2019, 220
[29] Wall, David S. 2021. "Cybercrime as A transnational organized criminal activity." In Routledge Handbook of Transnational Organized Crime, 318-336. Routledge.
[30] Wall, David S. 2007. “Cybercrime: The Transformation of Crime in the Information Age.” Cambridge: Polity.
[31] Wall 2007, 50
[32] Khan, Shereen, Tajneen Saleh, Magiswary Dorasamy, Nasreen Khan, Olivia Tan Swee Leng, and Rossanne Gale Vergara. 2022. “A Systematic Literature Review on Cybercrime Legislation [version 1; Peer Review: 1 Approved].” *F1000 Research* 11: 971–989.
[33] Mansfield-Devine, Steve. 2017. “Leaks and Ransoms - the Key Threats to Healthcare Organisations.” *Network Security* 6: 14–19.
[34] Spence, Nikki, Niharika Bhardwaj, David P Paul, and Alberto Coustasse. 2018. “Ransomware in Healthcare Facilities: A Harbinger of the Future?” *Perspectives in Health Information Management* 1–22.
[35] Chua, Julie Anne. 2021. “Cybersecurity in The Healthcare Industry - A Collaborative Approach.” *Physician Leadership Journal* 8 (1): 23–25.
[36] Chua 2021, 23
[37] Marshall, Eliot. 1988. “The Worm’s Aftermath.” *Science (American Association for the Advancement of Science)* 242 (4882): 1121–1122.
[38] The Wall Street Journal. 1988. "Spreading a virus: How Computer Science was Caught Off Guard by One Young Hacker - Outbreak Spread Nationally, caused no Lasting Harm but Much Embarrassment - Finding a Worm in the Mail - A Wall Street Journal News Roundup." *Wall Street Journal*, 1.
[39] The Wall Street Journal 1988, 2
[40] Farwell, James P., and Rohozinski, Rafal. 2011. “Stuxnet and the Future of Cyber War.” *Survival* (London) 53 (1): 23–40
[41] Farwell and Rohozinski 2011, 2
[42] The WannaCry Ransomware Attack 2017, 1
[43] The WannaCry Ransomware Attack 2017, 1
[44] Ghafur, S, S Kristensen, K Honeyford, G Martin, A Darzi, and P Aylin. 2019. “A Retrospective Impact Analysis of the WannaCry Cyberattack on the NHS.” *NPJ Digital Medicine* 2 (1): 98–105.
[45] Ghafur et al. 2019, 98
[46] Martin, James, and Whelan, Chad. 2023. “Ransomware through the Lens of State Crime: Conceptualizing Ransomware Groups as Cyber Proxies, Pirates, and Privateers.” *State Crime*, 12 (1): COV1–25.
[47] Miller, Zeke, and Eric Tucker. 2021. “President Biden Tells Putin Russia Must Crack down on Cybercriminals.” *The Philadelphia Tribune* (1884), 2021.
[48] Martin and Whelan 2023, 7
[49] Martin and Whelan, 2023, 6

[50] DiMaggio, J. 2022 “A History of REvil”, Analyst 1. Available online at: https://analyst1.com/file-assets/History-of-REvil.pdf.
[51] Covlea, Marian I. 2016. “Money Laundering - The Link Between International Organised Crime and Global Terrorism.” *Knowledge Horizons: Economics* 8 (1): 186–191
[52] Covlea 2016, 187
[53] Paarlberg 2022, 20
[54] Olajide, Elias Orogbemi, Adegboyega Adedolapo Ola, and Samson Adeoluwa Adewumi. 2022. “The Impact of Non-State Actors on World Politics: A Challenge to Nation-States.” *Journal of African Foreign Affairs* 9 (1): 133–50.
[55] Al-Khater, Wadha Abdullah, Somaya Al-Maadeed, Abdulghani Ali Ahmed, Ali Safaa Sadiq, and Muhammad Khurram Khan. 2020. “Comprehensive Review of Cybercrime Detection Techniques.” *IEEE Access* 8: 137293–137311.
[56] Badal-Valero, Elena, José A. Alvarez-Jareño, and Jose M. Pavía. 2018. “Combining Benford’s Law and Machine Learning to Detect Money Laundering. An Actual Spanish Court Case.” *Forensic Science International* 282: 24–34.
[57] Sultana, A., A. Hamou-Lhadj and M. Couture. 2012. "An improved hidden Markov model for anomaly detection using frequent common patterns", Proc. *IEEE Int. Conf. Commun.* (ICC), pp. 1113-1117.
[58] Al-Khater et al. 2020, 137298
[59] Al-Khater et al. 2020, 137298
[60] Lu, Kang-Di, and Zheng-Guang Wu. 2022. “Genetic Algorithm-Based Cumulative Sum Method for Jamming Attack Detection of Cyber-Physical Power Systems.” *IEEE Transactions on Instrumentation and Measurement 71*: 1–10.
[61] Lu and Wu 2022, 1
[62] Dajun Du, Minggao Zhu, Xue Li, Minrui Fei, Siqi Bu, Lei Wu, and Kang Li. 2023. “A Review on Cybersecurity Analysis, Attack Detection, and Attack Defense Methods in Cyber-Physical Power Systems.” *Journal of Modern Power Systems and Clean Energy* 11 (3): 727–743.
[63] Dajun et al 2023, 727
[64] Inayat, Usman, Muhammad Fahad Zia, Sajid Mahmood, Haris M. Khalid, and Mohamed Benbouzid. 2022. “Learning-Based Methods for Cyber Attacks Detection in IoT Systems: A Survey on Methods, Analysis, and Future Prospects.” *Electronics (Basel)* 11 (9): 1–20.
[65] Klein, Jan, Sandjai Bhulai, Mark Hoogendoorn, and Rob van der Mei. 2022. “Jasmine: A New Active Learning Approach to Combat Cybercrime.” *Machine Learning with Applications* 9(100351): 1-15.
[66] Broadhurst, Roderic. 2006. “Developments in the Global Law Enforcement of Cyber-Crime.” *Policing: An International Journal of Police Strategies & Management* 29 (3): 408–433.
[67] Broadhurst 2006, 416
[68] Council of Europe. 2004. “Organised crime situation report: Focus on the threat of cybercrime.”
[69] Broadhurst 2006, 418
[70] National Security Strategy. 2022. Page 1-48. https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.
[71] National Security Strategy 2022, 1
[72] Realuyo, Celina B. 2014. “Hezbollah’s Global Facilitators in Latin America. Testimony at a hearing entitled: Terrorist Groups in Latin America: The Changing Landscape.” Subcommittee on Terrorism, Non-Proliferation, and Trade, House Committee on Foreign Affairs, U.S. House of Representatives.”
[73] Siegel, Dina. 2014. “Women in transnational organized crime.” *Trends Organ Crim* (2014) 17:52–65.
[74] Siegel 2005, 52
[75] Siegel 2005, 53
[76] Siegel 2005, 53
[77] Siegel 2005, 54
[78] Zou, Yixin, Allison McDonald, Julia Narakornpichit, Nicola Dell, Thomas Ristenpart, Kevin Roundy, Florian Schaub, and Acar Tamersoy. 2021. "The role of computer security customer support in helping survivors of intimate partner violence." In 30th USENIX

security symposium, *USENIX Security* 21: 429-446
[79] Agarwal, Ritu, Michelle Dugas, Guodong (Gordon) Gao, and P. K. Kannan. 2020. "Emerging Technologies and Analytics for a New Era of Value-Centered Marketing in Healthcare." *Journal of the Academy of Marketing Science* 48 (1): 9–23.
[80] Pedroza, Belinda. 2023. "A Qualitative Study on the Threats Transnational Criminal Organizations and Texas Criminal Gangs Pose and Their Impact Along the Texas-Mexico Border" (Doctoral dissertation, Northcentral University).
[81] Agarwal et al. 2020, 16-17
[82] Bose and Gupta 2022, 44
[83] Adebowale et al. 2023, 765
[84] Adebowale et al. 2023, 765
[85] Velasco, Cristos. 2022. "Cybercrime and Artificial Intelligence. An Overview of the Work of International Organizations on Criminal Justice and the International Applicable Instruments." *ERA-Forum* 23 (1): 109–26.
[86] Velasco 2022, 113
[87] Eshel, Tamir. 2012. "Organized Crime in the Digital Age - Defense-Update." *Counter Terror & Homeland Security*.
[88] Eshel 2012, 1
[89] McGuire, M. (2012). Organised Crime in the Digital Age. London: John Grieve Centre for Policing and Security.
[90] Broadhurst 2014, 4
[91] "McAfee Labs 2018 Threats Predictions Previews Five Cybersecurity Trends, 2017."
[92] Spence et al. 2018, 3
[93] Andini, O. P. 2021. Cyber Terrorism Criminal Acts in the Perspective of Transnational Organized Crime. *Unnes Law Journal* 7(2), 333-346.
[94] Andini 2021, 337
[95] Broadhurst et al. 2014, 4
[96] Broadhurst et al. 2014, 4
[97] Broadhurst et al. 2014, 4
[98] Charountaki, Marianna. 2020. "Non-State Actors and Change in Foreign Policy: The Case of A Self-Determination Referendum In The Kurdistan Region Of Iraq." *Cambridge Review of International Affairs*, 33(3), 385-409.
[99] Hussein, Dalsooz Jalal. 2021. "Theoretical Approaches towards the Steps of Nongovernmental Actors in World Politics: Global Paradiplomacy of the Iraqi Kurdistan (KRI)." *Sententia*, 1: 31–41.
[100] Calò, Francesca, Simon Teasdale, Michael J. Roy, Enrico Bellazzecca, and Micaela Mazzei. 2023. "Exploring Collaborative Governance Processes Involving Nonprofits." *Nonprofit and Voluntary Sector Quarterly*.
[101] Al-Khater et al. 2020, 137293
[102] Al-Khater et al. 2020, 137295
[103] Al-Khater et al. 2020, 137294
[104] Wu, Longfei, Xiaojiang Du, and Jie Wu. 2016. "Effective Defense Schemes for Phishing Attacks on Mobile Computing Platforms." *IEEE Transactions on Vehicular Technology* 65 (8): 6678–6691.
[105] Wu et al. 2016, 6678
[106] Al-Khater et al. 2020, 137294
[107] Al-Khater et al. 2020, 137294
[108] Al-Khater et al. 2020, 137294
[109] Al-Khater et al. 2020, 137295
[110] Al-Khater et al. 2020, 137295
[111] Badal-Valero et al. 2018, 24
[112] Cassella, Stefan D. 2018. "Toward a New Model of Money Laundering." *Journal of Money Laundering Control* 21 (4): 494–497.
[113] Frantz, Douglas. 2001. "Ancient Secret System Moves Money Globally." *The New York Times*, 2001, 1-4. Late Edition (East Coast) edition.
[114] Frantz 2001, 2
[115] Frantz 2001, 2
[116] Al-Khater et al., 2020, 137297
[117] Al-Khater et al., 2020, 137297
[118] Schein, D. D., and Trautman, L. J. 2020. "The dark web and employer liability." *Colo. Tech. LJ*, 18, 49.
[119] Schein and Trautman 2020, 49
[120] Schein and Trautman 2020, 49
[121] Holt, Thomas J. 2018. "Regulating Cybercrime through Law Enforcement and Industry Mechanisms." *The Annals of the American Academy of Political and Social Science* 679 (1): 140–157.
[122] Collier, Ben, Daniel R. Thomas, Richard Clayton, Alice Hutchings, and Yi Ting Chua. 2022. "Influence, Infrastructure, and Recentering Cybercrime Policing: Evaluating

Emerging Approaches to Online Law Enforcement through a Market for Cybercrime Services." *Policing & Society* 32 (1): 103–124.
[123] Holt 2018, 151
[124] Collier et al. 2022, 124
[125] Holt 2018, 144
[126] Holt 2018, 144
[127] Holt 2018, 144
[128] Andress, Jason and Steve Winterfeld. 2013. "Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners." 2nd ed. San Diego: Elsevier Science.
[129] Vinocur, James. 2022. "How NotPetya Reveals the Future of Cyber Risks & Damages." *Property & Casualty* 360.
[130] Bansal, U. 2021. "A review on ransomware attacks." In 2021 2nd *International Conference on Secure Cyber Computing and Communications (ICSCCC)* 221-226. IEEE.
[131] Bansal 2021, 221
[132] Satariano, Adam, and Nicole Perlroth. 2019. "Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong." *New York Times* (Online).
[133] Bansal 2021, 223
[134] Bansal 2021, 223
[135] Bansal 2021, 226
[136] Park, Joshua. 2021. "The Lazarus Group: The Cybercrime Syndicate Financing the North Korea State." *Harvard International Review* 42 (2): 34–39.
[137] Park 2021, 34
[138] Park 2021, 36
[139] Park 2021, 36
[140] Park 2021, 36
[141] Park 2021, 39
[142] Siegel, Dina. 2014. "Women in transnational organized crime." Trends Organ Crim (2014) 17:52–65.
[143] Siegel 2014, 61
[144] Siegel 2014, 60
[145] Siegel 2014, 60
[146] Siegel 2014, 60
[147] Siegel 2014, 61
[148] Siegel 2014, 61
[149] Collier et al. 2022, 124
[150] Collier et al. 2022, 118
[151] Hansel, Mischa. 2018. "Cyber-Attacks and Psychological IR Perspectives: Explaining Misperceptions and Escalation Risks." *Journal of International Relations and Development* 21 (3): 523–551.
[152] Miadzvetskaya, Yuliya, and Ramses A Wessel. 2022. "The Externalisation of the EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox." *European Papers (Online. Periodico)* 7 (1): 413–438.
[153] Poli, Sara, and Emanuele Sommario. 2023. "The Rationale and the Perils of Failing to Invoke State Responsibility for Cyber-Attacks: The Case of the EU Cyber Sanctions." *German Law Journal* 24 (3): 522–536.
[154] Christakis, Theodore, and Fabien Terpan. 2021. "EU–US Negotiations on Law Enforcement Access to Data: Divergences, Challenges and EU Law Procedures and Options." *International Data Privacy Law* 11 (2): 81–106.
[155] Poli et al., 2023, 523
[156] Poli et al., 2023, 523
[157] Tsagourias, Nicholas. 2015. "The Legal Status of Cyberspace." In Buchan, R. and Tsagourias, N. (eds) (2015), *Research Handbook on International Law and Cyberspace*, 13-29.
[158] Xinbao, ZHANG. 2017. "China's Strategy for International Cooperation on Cyberspace." *Chinese Journal of International Law* (Boulder, Colo.) 16 (3): 377–386.
[159] Xinbao 2017, 377
[160] Moynihan, Harriet. 2019. "The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention." *The Royal Institute of International Affairs*, 1-61. Chatham House.
[161] Schmitt, Michael N., and Liis Vihul. 2017. "SOVEREIGNTY IN CYBERSPACE: LEX LATA VEL NON?" AJIL Unbound 111: 213–218.
[162] Jensen, Eric Talbot. 2017. "THE TALLINN MANUAL 2.0: HIGHLIGHTS AND INSIGHTS." *Georgetown Journal of International Law* 48 (3): 735-778.
[163] Efrony, Dan, and Yuval Shany. 2018. "A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice." *The American Journal of International Law* 112 (4): 583–657.
[164] Efrony and Shany 2018, 585

[165] Efrony and Shany 2018, 591
[166] Moynihan 2019, 22
[167] Yuliya, Zabyelina. 2010. "Unpacking Pandora's Box: Defining Transnational Crime and Outlining Emerging Criminal Trends." *Central European Journal of International & Security* Studies 4 (2):124-139.
[168] Yuliya 2010, 11
[169] Calderaro, Andrea, and Anthony J. S. Craig. 2020. "Transnational Governance of Cybersecurity: Policy Challenges and Global Inequalities in Cyber Capacity Building." *Third World Quarterly* 41 (6): 917–38.
[170] Yetim, Mustafa. 2023. "Neo-Weberian Reading of Violent Non-State Actors: The Case of Hezbollah." *All Azimuth* 12 (2): 155–73.
[171] Yetim 2023, 156
[172] Yetim 2023, 156
[173] Kashyap Shubhankar. 2022. "Tracing Hobbes in Realist International Relations Theory." *E-International Relations*, 1-5.
[174] Morgenthau, Hans J, Kenneth W Thompson, W David Clinton, and Oliver Jütersonke. 2006. "Politics among Nations: The Struggle for Power and Peace." *Cooperation and Conflict* 41(4): 463-469.
[175] Hobbes, Thomas. 2018. "Leviathan." Minneapolis, MN: First Avenue Editions, a division of Lerner Publishing Group.
[176] Hobbes 2018, 32
[177] Kashyap 2022, 1
[178] Hobbes 2018, 26-31
[179] Kashyap 2022, 1
[180] Kashyap 2022, 2
[181] Hobson, John M. 2001. "The 'Second State Debate' in International Relations: Theory Turned Upside-Down." *Review of International Studies* 27 (3): 395–414.
[182] Rudner, Martin. 2010. "Hizbullah: An Organizational and Operational Profile." *International Journal of Intelligence and Counterintelligence* 23 (2): 226–246.
[183] "A Hezbollah PRIMER." 1996.Jewish Advocate, May 01, 15.
[184] Rudner, Martin. 2010. "Hizbullah Terrorism Finance: Fund-Raising and Money-Laundering." *Studies in Conflict and Terrorism* 33 (8): 700–715.
[185] Azani, Eitan. 2013. "The Hybrid Terrorist Organization: Hezbollah as a Case Study." *Studies in Conflict and Terrorism* 36 (11): 899–916.
[186] Yetim 2023, 165
[187] Jones, Matthew R, and Helena Karsten. 2008. "Giddens's Structuration Theory and Information Systems Research." MIS Quarterly 32 (1): 127–57.
[188] Paarlberg 2022, 7
[189] Calderaro and Craig 2020, 919
[190] Sarkin, Jeremy Julian. 2021. "Reforming the International Criminal Court (ICC): Progress, Perils and Pitfalls Post the ICC Review Process" *International and Comparative Law Review* 21(1): 7-42.
[191] Sarkin, Jeremy. 2020. "Reforming the International Criminal Court (ICC) to Achieve Increased State Cooperation in Investigations and Prosecutions of International Crimes." *International Human Rights Law Review* 9(1): 27–61.
[192] Sarkin 2021, 7; Sarkin 2020, 27
[193] Olajide et al., 2022, p. 133
[194] Safjanski, Tomasz. 2015. "Prospects for the Development of the International Criminal Police Organisation Interpol." *Internal Security* 7 (2): 267-277.
[195] Perepolkin, S.M., and H.L. Kokhan. 2020. "The International Criminal Police Organization – INTERPOL." *Juridical Scientific and Electronic Journal* 6: 254-257.
[196] Safjanski 2015, 267
[197] Lee, Kelley and Jennifer Fang. 2013. "Historical Dictionary of the World Health Organization." 2nd ed. Lanham, Md: Scarecrow Press.
[198] Lee and Fang 2013, 36
[199] Simopoulos, Rob. 2018. "A KRACK in the Wireless Armor." Security Dealer, 40. Fort Atkinson: Endeavor Business Media.
[200] Simopoulos 2018, 1
[201] Halperin, D., T. Kohno, T.S. Heydt-Benjamin, K. Fu, and W.H. Maisel. 2008. "Security and Privacy for Implantable Medical Devices." *IEEE Pervasive Computing* 7 (1): 30–39.
[202] Halperin et al. 2008, 30
[203] Halperin et al. 2008, 30

[204] State of Cybersecurity 2019. Current Trends in Attacks, Awareness and Governance. www.isaca.org/info/state-of-cybersecurity-2019/index.html
[205] State of Cybersecurity Report 2019, 1
[206] Rasulev, Abdulaziz and Gayrat Sadullayev. 2021. "Training of Personnel in The Field of Countering Cybercrime: The Need and The Requirement of Time." *The American Journal of Political Science Law and Criminology* 3: 123-130.
[207] Rasulev and Sadullayev 2021, 124
[208] Rasulev and Sadullayev 2021, 127
[209] Rasulev and Sadullayev 2021, 128
[210] Velasco 2022, 109
[211] Velasco 2022, 126
[212] Zou et al. 2021, 446
[213] Agarwal et al. 2020, 23

REFERENCES

[1] "A Hezbollah PRIMER." 1996. *Jewish Advocate*, May 01, 15. http://ezproxy.apus.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fnewspapers%2Fhezbollah-primer%2Fdocview%2F205205724%2Fse-2%3Faccountid%3D8289. Accessed November 21, 2023.

[2] Adebowale, Moruf A., Khin T Lwin., and Hossain, M. Alamgir. 2023. "Intelligent phishing detection scheme using deep learning algorithms", *Journal of Enterprise Information Management* 36(3),747-766. https://doi.org/10.1108/JEIM-01-2020-0036. Accessed September 19, 2023.

[3] Agarwal, Ritu, Michelle Dugas, Guodong (Gordon) Gao, and P. K. Kannan. 2020. "Emerging Technologies and Analytics for a New Era of Value-Centered Marketing in Healthcare." *Journal of the Academy of Marketing Science* 48 (1): 9–23. https://doi.org/10.1007/s11747-019-00692-4. Accessed September 19, 2023.

[4] Al-Khater, Wadha Abdullah, Somaya Al-Maadeed, Abdulghani Ali Ahmed, Ali Safaa Sadiq, and Muhammad Khurram Khan. 2020. "Comprehensive Review of Cybercrime Detection Techniques." *IEEE Access* 8: 137293–137311. https://doi.org/10.1109/ACCESS.2020.3011259. Accessed October 24, 2023.

[5] Andini, O. P. 2021. Cyber Terrorism Criminal Acts in the Perspective of Transnational Organized Crime. *Unnes Law Journal* 7(2), 333-346. Accessed November 1, 2023.

[6] Andress, Jason and Steve Winterfeld. 2013. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. 2nd ed. San Diego: Elsevier Science. Accessed November 25, 2023.

[7] Azani, Eitan. 2013. "The Hybrid Terrorist Organization: Hezbollah as a Case Study." *Studies in Conflict and Terrorism* 36 (11): 899–916. https://doi.org/10.1080/1057610X.2013.832113. Accessed November 21, 2023.

[8] Bansal, U. 2021. A review on ransomware attacks. In 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC), 221-226. IEEE. Accessed November 1, 2023.

[9] Broadhurst, Roderic. 2006. "Developments in the Global Law Enforcement of Cyber-Crime." *Policing: An International Journal of Police Strategies & Management* 29 (3): 408–433. https://doi.org/10.1108/13639510610684674. Accessed November 5, 2023.

[10] Broadhurst, Roderic, Peter Grabosky, Mamoun Alazab, and Steve Chon. 2014. "Organizations and Cyber Crime: An Analysis of the Nature of Groups Engaged in Cyber Crime." *International Journal of Cyber Criminology* 8 (1): 1–21. Accessed October 31, 2023.

[11] Badal-Valero, Elena, José A. Alvarez-Jareño, and Jose M. Pavía. 2018. "Combining Benford's Law and Machine Learning to Detect Money Laundering. An Actual Spanish Court Case." *Forensic Science International* 282: 24–34. https://doi.org/10.1016/j.forsciint.2017.11.008. Accessed November 2, 2023.

[12] Bose, Malobika and Sonalika Gupta. 2022. "Digital Financial Services: Emerging Issues and Challenges." The Next Normal: Building Agile, Sustainable, Tech-enabled Organizations. (*TNN–BASTO-2022*), 44-54. Accessed September 24, 2023.

[13] Bulanova-Hristova, Gergana, Kasper Karsten, Odinot Geralda, Verhoeven Maite, Pool Ronald,

Poot Christianne, Werner Yael and Korsell Lars. 2016. Cyber-OC- Scope and manifestations in selected EU member states. 1-299. Accessed November 5, 2023.

[14] Calò, Francesca, Simon Teasdale, Michael J. Roy, Enrico Bellazzecca, and Micaela Mazzei. 2023. "Exploring Collaborative Governance Processes Involving Nonprofits." *Nonprofit and Voluntary Sector Quarterly*. https://doi.org/10.1177/08997640231155817. Accessed November 16, 2023.

[15] Cassella, Stefan D. 2018. "Toward a New Model of Money Laundering." *Journal of Money Laundering Control* 21(4): 494–497. https://doi.org/10.1108/JMLC-09-2017-0045. Accessed October 28, 2023.

[16] Catino, Maurizio. 2020. "Italian Organized Crime Since 1950." *Crime and Justice* (Chicago, Ill.) 49 (1): 69–140. https://doi.org/10.1086/707319. Accessed November 1, 2023.

[17] Charountaki, M. 2020. "Non-state actors and change in foreign policy: the case of a self-determination referendum in the Kurdistan Region of Iraq." *Cambridge Review of International Affairs*, 33(3), 385–409. https://doi.org/10.1080/09557571.2019.1663495 . Accessed November 15, 2023.

[18] Chua, Julie Anne. 2021. "Cybersecurity in The Healthcare Industry - A Collaborative Approach." *Physician Leadership Journal* 8 (1): 23–25. Accessed October 14, 2023.

[19] Cleary, Richard, and Jay C Thibodeau. 2005. "Applying Digital Analysis Using Benford's Law to Detect Fraud: The Dangers of Type I Errors." *Auditing: A Journal of Practice and Theory* 24 (1): 77–81. https://doi.org/10.2308/aud.2005.24.1.77. Accessed October 27, 2023.

[20] Collier, Ben, Daniel R. Thomas, Richard Clayton, Alice Hutchings, and Yi Ting Chua. 2022. "Influence, Infrastructure, and Recentering Cybercrime Policing: Evaluating Emerging Approaches to Online Law Enforcement through a Market for Cybercrime Services." *Policing & Society* 32 (1): 103–124. https://doi.org/10.1080/10439463.2021.1883608 . Accessed October 31, 2023.

[21] Council of Europe. 2004. "Organised crime situation report: Focus on the threat of cybercrime." http://www.coe. Accessed October 27, 2023.

[22] Covlea, Marian I. 2016. "Money Laundering - The Link Between International Organised Crime and Global Terrorism." *Knowledge Horizons: Economics,* 8 (1): 186–191. Accessed September 17, 2023.

[23] Christakis, Theodore, and Fabien Terpan. 2021. "EU–US Negotiations on Law Enforcement Access to Data: Divergences, Challenges and EU Law Procedures and Options." *International Data Privacy Law* 11 (2): 81–106. https://doi.org/10.1093/idpl/ipaa022. Accessed November 22, 2023.

[24] Dajun Du, Minggao Zhu, Xue Li, Minrui Fei, Siqi Bu, Lei Wu, and Kang Li. 2023. "A Review on Cybersecurity Analysis, Attack Detection, and Attack Defense Methods in Cyber-Physical Power Systems." *Journal of Modern Power Systems and Clean Energy* 11 (3): 727–43. https://doi.org/10.35833/MPCE.2021.000604. Accessed October 29, 2023.

[25] Dastjerdi, Shirin Ahmadi, and Abbas Sheikholeslami. 2019. "The Effect of Globalization on the National Criminal Law Systems." *Library Philosophy and Practice* (4): 1–13. Accessed November 16, 2023.

[26] Décary-Hétu, David, and Benoit Dupont. 2012. "The Social Network of Hackers." *Global Crime* 13 (3): 160–175. https://doi.org/10.1080/17440572.2012.702523. Accessed November 1, 2023.

[27] DiMaggio, J. 2022 "A History of REvil", *Analyst* 1. Available online at: https://analyst1.com/file-assets/History-of-REvil.pdf. Accessed September 17, 2023.

[28] Efrony, Dan, and Yuval Shany. 2018. "A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice." *The American Journal of International Law* 112 (4): 583–657. https://doi.org/10.1017/ajil.2018.86. Accessed November 22, 2023.

[29] Eshel, Tamir. 2012. "Organized Crime in the Digital Age - Defense-Update." *Counter Terror & Homeland Security.* https://defense-

update.com/20120328_organized_cyber_crime.html. Accessed October 13, 2023.

[30] Etges, Rafael, and Emma Sutcliffe. 2008. "An Overview of Transnational Organized Cyber Crime." *Information Security Journal* 17 (2): 87–94. https://doi.org/10.1080/19393550802036631. Accessed November 1, 2023

[31] Frantz, Douglas. 2001. "Ancient Secret System Moves Money Globally." *The New York Times,* 2001, 1-4. Late Edition (East Coast) edition. Accessed October 28, 2023.

[32] Farwell, James P., and Rafal Rohozinski. 2011. "Stuxnet and the Future of Cyber War." *Survival* (London), 53 (1): 23–40. https://doi.org/10.1080/00396338.2011.555586. Accessed September 17, 2023.

[33] Ghafur, S, S Kristensen, K Honeyford, G Martin, A Darzi, and P Aylin. 2019. "A Retrospective Impact Analysis of the WannaCry Cyberattack on the NHS." *NPJ Digital Medicine* 2 (1): 98–105. https://doi.org/10.1038/s41746-019-0161-6. Accessed September 17, 2023.

[34] Gulyás, Attila. 2022. 'Lazarus' The North Korean Hacker Group." *International Scientific Conference "Strategies XXI*", 75–83. https://doi.org/10.53477/2668-6511-22-08. Accessed September 17, 2023.

[35] Halperin, D., T. Kohno, T.S. Heydt-Benjamin, K. Fu, and W.H. Maisel. 2008. "Security and Privacy for Implantable Medical Devices." *IEEE Pervasive Computing* 7 (1): 30–39. https://doi.org/10.1109/MPRV.2008.16. Accessed November 4, 2023.

[36] Hansel, Mischa. 2018. "Cyber-Attacks and Psychological IR Perspectives: Explaining Misperceptions and Escalation Risks." *Journal of International Relations and Development* 21 (3): 523–51. https://doi.org/10.1057/s41268-016-0075-8. Accessed November 22, 2023.

[37] Hobbes, Thomas. 2018. Leviathan. Minneapolis, MN: First Avenue Editions, a division of Lerner Publishing Group. Accessed November 20, 2023.

[38] Hobson, John M. 2001. "The 'Second State Debate' in International Relations: Theory Turned Upside-Down." *Review of International Studies* 27 (3): 395–414. https://doi.org/10.1017/S0260210501003953. Accessed November 19, 2023.

[39] Holt, Thomas J. 2018. "Regulating Cybercrime through Law Enforcement and Industry Mechanisms." *The Annals of the American Academy of Political and Social Science* 679 (1): 140–157. https://doi.org/10.1177/0002716218783679. Accessed November 25, 2023.

[40] Hussein, Dalsooz Jalal. 2021. "Theoretical Approaches towards the Steps of Nongovernmental Actors in World Politics: Global Paradiplomacy of the Iraqi Kurdistan (KRI)." *Sententia*, 1: 31–41. https://doi.org/10.25136/1339-3057.2021.1.34624. Accessed November 16, 2023.

[41] Inayat, Usman, Muhammad Fahad Zia, Sajid Mahmood, Haris M. Khalid, and Mohamed Benbouzid. 2022. "Learning-Based Methods for Cyber Attacks Detection in IoT Systems: A Survey on Methods, Analysis, and Future Prospects." *Electronics (Basel)* 11 (9): 1502–. https://doi.org/10.3390/electronics11091502. Accessed October 29, 2023.

[42] Jensen, Benjamin, Valeriano, Brandon, and Maness, Ryan. 2019. Fancy bears and digital trolls: Cyber strategy with a Russian twist. *Journal of Strategic Studies*, 42(2), 212–234. https://doi.org/10.1080/01402390.2018.1559152. Accessed September 17, 2023.

[43] Jeronimo, Advento. 2019. "The Globalization Effect of Law and Economic on Cybercrime." *Jurnal Pembaharuan Hukum* 6 (3). https://doi.org/10.26532/jph.v6i3.10933. Accessed November 17, 2023.

[44] Kashyap Shubhankar. 2022. "Tracing Hobbes in Realist International Relations Theory." *E-International Relations*, 1-5. https://www.e-ir.info/2022/02/22/tracing-hobbes-in-realist-international-relations-theory/ Accessed November 20, 2023.

[45] Khan, Shereen, Tajneen Saleh, Magiswary Dorasamy, Nasreen Khan, Olivia Tan Swee Leng, and Rossanne Gale Vergara. 2022. "A Systematic Literature Review on Cybercrime Legislation [version 1; Peer Review: 1 Approved]." *F1000 Research* 11: 971–989.

https://doi.org/10.12688/f1000research.123098.1. Accessed September 6, 2023.

[46] Kethineni, S., & Cao, Y. (2020). The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. *International Criminal Justice Review*, 30(3), 325–344. https://doi-org.ezproxy2.apus.edu/10.1177/1057567719827051. Accessed August 13, 2023.

[47] Klein, Jan, Sandjai Bhulai, Mark Hoogendoorn, and Rob van der Mei. 2022. "Jasmine: A New Active Learning Approach to Combat Cybercrime." *Machine Learning with Applications* 9(100351): 1-15 https://doi.org/10.1016/j.mlwa.2022.100351. Accessed October 27, 2023

[48] Lee, Kelley and Jennifer Fang. 2013. "Historical Dictionary of the World Health Organization." 2nd ed. Lanham, Md: Scarecrow Press. Accessed November 21, 2023

[49] Leukfeldt, E. Rutger, Edward R. Kleemans, and Wouter P. Stol. 2017. "A Typology of Cybercriminal Networks: From Low-Tech All-Rounders to High-Tech Specialists." *Crime, Law, and Social Change* 67 (1): 21–37. https://doi.org/10.1007/s10611-016-9662-2. Accessed September 30, 2023.

[50] Lu, Kang-Di, and Zheng-Guang Wu. 2022. "Genetic Algorithm-Based Cumulative Sum Method for Jamming Attack Detection of Cyber-Physical Power Systems." *IEEE Transactions on Instrumentation and Measurement* 71: 727-743. https://doi.org/10.1109/TIM.2022.3186360. Accessed November 2, 2023.

[51] Mansfield-Devine, Steve. 2017. "Leaks and Ransoms - the Key Threats to Healthcare Organisations." *Network Security* 6: 14–19. Accessed October 31, 2023.

[52] "McAfee Labs 2018 Threats Predictions Previews Five Cybersecurity Trends, 2017." https://www.mcafee.com/blogs/other-blogs/mcafee-labs/2018-threats-predictions/. Accessed November 4, 2023.

[53] Marshall, Eliot. 1988. "The Worm's Aftermath." *Science* (American Association for the Advancement of Science) 242 (4882): 1121–22. https://doi.org/10.1126/science.242.4882.1121. Accessed November 1, 2023.

[54] Martin, James, and Whelan, Chad. 2023. "Ransomware through the Lens of State Crime: Conceptualizing Ransomware Groups as Cyber Proxies, Pirates, and Privateers." *State Crime*, 12 (1): COV1–25. https://doi.org/10.13169/statecrime.12.1.0004. Accessed September 16, 2023.

[55] McGuire, M. (2012). Organised Crime in the Digital Age. London: *John Grieve Centre for Policing and Security.*

[56] Miadzvetskaya, Yuliya, and Ramses A Wessel. 2022. "The Externalisation of the EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox." *European Papers (Online. Periodico)* 7 (1): 413–38. https://doi.org/10.15166/2499-8249/570. Accessed November 22, 2023.

[57] Millán-Quijano, Jaime. 2020. "Internal Cocaine Trafficking and Armed Violence in Colombia." *Economic Inquiry*, 58 (2): 624–41. https://doi.org/10.1111/ecin.12771. Accessed September 12, 2023.

[58] Miller, Zeke, and Eric Tucker. 2021. "President Biden Tells Putin Russia Must Crack down on Cybercriminals." *The Philadelphia Tribune* (1884), 2021. Accessed September 17, 2023.

[59] Morgenthau, Hans J, Kenneth W Thompson, W David Clinton, and Oliver Jütersonke. 2006. "Politics among Nations: The Struggle for Power and Peace." *Cooperation and Conflict* 41(4): 463-469. https://doi.org/10.1177/0010836706069616. Accessed November 20, 2023.

[60] Moynihan, Harriet. 2019. "The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention." *The Royal Institute of International Affairs*, 1-61. Chatham House. https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks/about-author. Accessed November 24, 2023.

[61] National Security Strategy. 2022. Page 1-48. https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf. Accessed October 30, 2023.

[62] Olajide, Elias Orogbemi, Adegboyega Adedolapo Ola, and Samson Adeoluwa Adewumi. 2022. "The Impact of Non-State Actors on World Politics: A Challenge to Nation-

States." *Journal of African Foreign Affairs* 9 (1): 133–50. https://doi.org/10.31920/2056-5658/2022/v9n1a7. Accessed November 16, 2023.

[63] Paarlberg, Michael Ahn. 2022. "Transnational Gangs and Criminal Remittances: A Conceptual Framework." *Comparative Migration Studies* 10 (1): 1–20. https://doi.org/10.1186/s40878-022-00297-x. Accessed November 16, 2023.

[64] Park, Joshua. 2021. "The Lazarus Group: The Cybercrime Syndicate Financing the North Korea State." *Harvard International Review* 42 (2): 34–39. Accessed October 31, 2023.

[65] Pedroza, Belinda. 2023. "A Qualitative Study on the Threats Transnational Criminal Organizations and Texas Criminal Gangs Pose and Their Impact Along the Texas-Mexico Border" (Doctoral dissertation, Northcentral University). Accessed August 13, 2023

[66] Perepolkin, S.M., and H.L. Kokhan. 2020. "The International Criminal Police Organization – INTERPOL." *Juridical Scientific and Electronic Journal* 6: 254-257. https://doi.org/10.32782/2524-0374/2020-6/62. Accessed November 21, 2023.

[67] Poli, Sara, and Emanuele Sommario. 2023. "The Rationale and the Perils of Failing to Invoke State Responsibility for Cyber-Attacks: The Case of the EU Cyber Sanctions." *German Law Journal* 24 (3): 522–36. https://doi.org/10.1017/glj.2023.25. Accessed November 22, 2023.

[68] Rasulev, Abdulaziz and Gayrat Sadullayev. 2021. "Training of Personnel in The Field of Countering Cybercrime: The Need and The Requirement of Time." *The American Journal of Political Science Law and Criminology*, 3: 123-130. 123-130. 10.37547/tajpslc/Volume03Issue02-18. Accessed October 31, 2023.

[69] Realuyo C.B., 2014. Collaborating to Combat the Convergence of Illicit Networks. Lecture delivered at Harvard University, John F. Kennedy School of Government, South Asian Senior National Security Seminar. Cambridge, MA. Accessed October 14, 2023.

[70] Rudner, Martin. 2010. "Hizbullah: An Organizational and Operational Profile." *International Journal of Intelligence and Counterintelligence* 23 (2): 226–246. https://doi.org/10.1080/08850600903565654. Accessed November 21, 2023.

[71] Rudner, Martin. 2010. "Hizbullah Terrorism Finance: Fund-Raising and Money-Laundering." *Studies in Conflict and Terrorism* 33 (8): 700–715. https://doi.org/10.1080/1057610X.2010.494169. Accessed November 21, 2023.

[72] Safjanski, Tomasz. 2015. "Prospects for the Development of the International Criminal Police Organisation Interpol." *Internal Security* 7 (2): 267-277. https://doi.org/10.5604/20805268.1212128. Accessed November 21, 2023.

[73] Sanger, David and Charles Savage, "U.S. Says Russia Directed Hacks to Influence Elections." *New York Times*, 7 Oct. 2016. Accessed September 12, 2023.

[74] Satariano, Adam, and Nicole Perlroth. 2019. "Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong." *New York Times* (Online), 2019. Accessed November 4, 2023.

[75] Sarkin, Jeremy. 2020. "Reforming the International Criminal Court (ICC) to Achieve Increased State Cooperation in Investigations and Prosecutions of International Crimes." *International Human Rights Law Review* 9(1): 27–61. Accessed November 21, 2023.

[76] Sarkin, Jeremy Julian. 2021. "Reforming the International Criminal Court (ICC): Progress, Perils and Pitfalls Post the ICC Review Process" *International and Comparative Law Review* 21(1): 7-42. https://doi.org/10.2478/iclr-2021-0001. Accessed November 21, 2023.

[77] Schein, D. D., and Trautman, L. J. 2020. "The dark web and employer liability." Colo. Tech. LJ, 18, 49. Accessed October 14, 2023.

[78] Schmitt, Michael N., and Liis Vihul. 2017. "SOVEREIGNTY IN CYBERSPACE: LEX LATA VEL NON?" *AJIL Unbound* 111: 213–218. https://doi.org/10.1017/aju.2017.55. Accessed November 24, 2023.

[79] Siegel, Dina. 2014. "Women in transnational organized crime." Trends Organ Crim (2014) 17:52–65. DOI 10.1007/s12117-013-9206-4. Accessed October 27, 2023.

[80] Simopoulos, Rob. 2018. “A KRACK in the Wireless Armor.” *Security Dealer*, 40. Fort Atkinson: Endeavor Business Media. https://advance-lexis-com.ezproxy1.apus.edu/api/document?collection=news&id=urn: contentItem:5RPG-G3F1-JC79-C00K-00000-00&context=1516831. Accessed November 4, 2023.

[81] Spence, Nikki, Niharika Bhardwaj, David P Paul, and Alberto Coustasse. 2018. “Ransomware in Healthcare Facilities: A Harbinger of the Future?” *Perspectives in Health Information Management*, 1–22. Accessed October 14, 2023.

[82] State of Cybersecurity 2019. Current Trends in Attacks, Awareness and Governance. www.isaca.org/info/state-of-cybersecurity-2019/index.html

[83] Sultana, A., A. Hamou-Lhadj and M. Couture. 2012. "An improved hidden Markov model for anomaly detection using frequent common patterns", Proc. IEEE Int. Conf. Commun. (ICC), pp. 1113-1117.

[84] Tsagourias, Nicholas. 2015. “The Legal Status of Cyberspace.” In Buchan, R. and Tsagourias, N. (eds) (2015), *Research Handbook on International Law and Cyberspace,* 13-29. Edgar Elgar Online. https://doi.org/10.4337/9781782547396.00010. Accessed November 25, 2023.

[85] The Wall Street Journal. 1988. "Spreading a virus: How Computer Science was Caught Off Guard by One Young Hacker - Outbreak Spread Nationally, caused no Lasting Harm but Much Embarrassment - Finding a Worm in the Mail - A Wall Street Journal News Roundup." *Wall Street Journal*, 1. http://ezproxy.apus.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fnewspapers%2Fspreading-virus-how-computer-science-was-caught%2Fdocview%2F398171075%2Fse-2%3Faccountid%3D8289. Accessed September 17, 2023.

[86] “The WannaCry Ransomware Attack.” 2017. *Strategic Comments* 23 (4): vii–ix. https://doi.org/10.1080/13567888.2017.1335101. Accessed September 17, 2023.

[87] Velasco, Cristos. 2022. “Cybercrime and Artificial Intelligence. An Overview of the Work of International Organizations on Criminal Justice and the International Applicable Instruments.” *ERA-Forum* 23 (1): 109–26. https://doi.org/10.1007/s12027-022-00702-z. Accessed October 31, 2023.

[88] Vinocur, James. 2022. “How NotPetya Reveals the Future of Cyber Risks & Damages.” *Property & Casualty 360*. Accessed November 4, 2023.

[89] Wall, David S. 2007. “Cybercrime: The Transformation of Crime in the Information Age.” Cambridge: Polity. Accessed November 1, 2023.

[90] Wall, David S. 2021. "Cybercrime as A transnational organized criminal activity." In Routledge Handbook of Transnational Organized Crime, pp. 318-336. Routledge. Accessed November 1, 2023.

[91] Weber, Julia, and Edwin W. Kruisbergen. 2019. “Criminal Markets: The Dark Web, Money Laundering and Counterstrategies - An Overview of the 10th Research Conference on Organized Crime.” *Trends in Organized Crime* 22 (3): 346–56. https://doi.org/10.1007/s12117-019-09365-8. Accessed November 1, 2023.

[92] Wu, Longfei, Xiaojiang Du, and Jie Wu. 2016. “Effective Defense Schemes for Phishing Attacks on Mobile Computing Platforms.” *IEEE Transactions on Vehicular Technology* 65 (8): 6678–91. https://doi.org/10.1109/TVT.2015.2472993. Accessed November 5, 2023.

[93] Xinbao, ZHANG. 2017. “China’s Strategy for International Cooperation on Cyberspace.” *Chinese Journal of International Law (Boulder, Colo.)* 16 (3): 377–86. https://doi.org/10.1093/chinesejil/jmx026. Accessed November 24, 2023.

[94] Yetim, Mustafa. 2023. “Neo-Weberian Reading of Violent Non-State Actors: The Case of Hezbollah.” *All Azimuth* 12 (2): 155–73. https://doi.org/10.20991/allazimuth.1310477. Accessed November 19, 2023.

[95] Yuliya, Zabyelina. 2010. “Unpacking Pandora’s Box: Defining Transnational Crime and Outlining Emerging Criminal Trends.” *Central European Journal of International & Security Studies* 4 (2):124-139. Accessed: August 13, 2023.

[96] Zou, Yixin, Allison McDonald, Julia Narakornpichit, Nicola Dell, Thomas Ristenpart,

Kevin Roundy, Florian Schaub, and Acar Tamersoy. 2021. "The role of computer security customer support in helping survivors of intimate partner violence." In 30th USENIX security symposium, (*USENIX Security*), 21:429-446. Accessed September 17, 2023.