AL-HAYAT Research Journal
Jlali Research Institute of Social Science, Lahore
Category Y
ISSN (Online): 3006-4767
ISSN (Print):: 3006-4759
Volume 2 Issue 3 (April-June 2025)

# From Ideology to Extortion: The Convergence of Cyberterrorism and Ransomware in the Digital Age

**Aliya Saeed**
PhD Fellow at School of Law, University of Karachi, Pakistan, aaliasaeed@yahoo.com

**Dr. Tansif Ur Rehman**
Teaching Associate, Department of Sociology, University of Karachi, Pakistan; and Visiting Faculty, Department of Law, Dadabhoy Institute of Higher Education, Pakistan (tansif@live.com) (https://orcid.org/0000-0002-5454-2150)

**Dr. Adeel Abid**
Advocate Supreme Court of Pakistan; and Assistant Professor, Department of Law, DIHE, Karachi, Pakistan adeel77abid@yahoo.com

**Adnan Zawar**
M.Phil. Research Scholar, Institute of Social & Cultural Studies, University of the Punjab, Pakistan
adnan.zawar@gmail.com

**Syed Adeel Ali Bukhari**
Ph.D. Research Scholar, Department of Public Administration, University of Karachi, Pakistan
adeelali84@hotmail.com

## Abstract

The world now faces serious security problems because of cyberterrorism and ransomware. It's getting harder to tell the difference between regular terrorism and online crime. Cyberterrorism is when people use computer attacks to scare governments or people to push their beliefs or political goals. Ransomware, on the other hand, is used to make money by locking up important computer systems and demanding payment. Both use the internet, strong encryption, and secret tools like cryptocurrencies and the dark web to do their work. It's harder than ever to find, stop, and blame the groups doing these attacks because they're getting smarter and can be governments or just groups of people, and they often operate in many countries. These attacks cause a lot of damage to the economy and people's mental health, making people lose trust, messing up important services, and endangering countries. This study looks at cyberterrorism and ransomware around the world, showing how they are connected, how their methods are changing, and how important it is for countries to work together, have similar laws, and build strong computer defenses to fight these growing online dangers.

**Keywords:** Cybersecurity, Cyberterrorism, Hybrid Threats, International Cooperation, Ransomware

## Introduction

The rise of the digital age has radically reshaped global security. It's brought entirely new kinds of threats, ones that aren't really limited by borders—whether those are political, geographical, or even legal (Martellozzo & Jane, 2017). Cyberterrorism and ransomware definitely stand out as two major problems facing governments, businesses, and just regular people (Littler & Lee, 2020). Generally speaking, cyberterrorism is usually about politics or ideology. It aims to scare or pressure governments and societies using digital tools, and it often goes after important infrastructure like power grids, communications networks, and banks (Willems, 2019). Ransomware, on the other hand, is mostly about making money. It involves locking up data and demanding payment from victims, often using cryptocurrencies and the dark web to stay hidden (Austin, 2020; Lavorgna, 2020).

Even though they have different goals, these two things are increasingly similar in how they work, what they do, and what happens as a result (Yar & Steinmetz, 2019). Both take advantage of the weaknesses in societies that are super-connected, using complex malware, tricking people, and breaking into networks (Marsh & Melville, 2019). In the vast

majority of cases, the line dividing political warfare and criminal activity is becoming more difficult to trace. Certain terrorist organizations nowadays make money by resorting to ransomware; cybercriminals are occasionally politically motivated (Leukfeldt & Holt, 2019). This amalgamation shows the increase of fusion of threats - ideological extremism and the opportunity to earn money (Abaimov and Martellini, 2020).

Cyberspace is global, and it is difficult to determine who is responsible, what laws are applicable, and how to react. These issues are not grounds on which a single country can be the only solution (Hufnagel & Moiseienko, 2019). It has led to the fact that cooperation on an international level, harmonization of laws in different countries, and even investing in cyber defenses have become inevitable (Bancroft, 2019). This paper will take a look at where cyberterrorism and ransomware meet from a global point of view. Analyzing what tactics they share, how their motives are changing, and what that means for international security and governance in a world that really depends on digital tech.

## Research Justification

This research is so important boils down to a pressing issue: cyberterrorism and ransomware are increasingly blurring together, and that's a problem. You see, cyberterrorism is usually about making a statement – political or ideological, generally speaking – while ransomware is all about the money. But when it starts to mix, well, that's where things get complicated. Our current laws, policies, and even our security measures just aren't really designed to handle this kind of hybrid threat. This research is trying to get a handle on how these two things are overlapping – in their methods, why they do it, and the impact it has. In most cases, this ends up changing our understanding of what digital conflict and global security even mean.

What's more, there's a real lack of consistent international rules, and tracing these attacks back to who's responsible is incredibly difficult when they cross borders. It basically creates an environment where these criminals can thrive without much fear of getting caught. So, for policymakers, cybersecurity folks, and even the police, it's essential to really dig into this convergence to figure out how to respond in a coordinated, multi-faceted way. By looking at the technical, legal, and ethical sides of this global problem, this study aims to inform the development of good strategies for cyber defense, prevention, and better international cooperation. Ultimately, this research is aimed at improving scholarly understanding and policy readiness, ensuring we are better armed in mitigating ideology-driven and financially motivated cyber aggression.

## Research Objectives

1. To explore the aspects of cyberterrorism.
2. To elaborate on ransomware and the mechanism through which it operates.
3. To focus on the international laws and aspects of cybercrime and initiatives taken by the E.U., USA, and China, encompassing cybercrime.

## Research Methodology

This research operates within a theoretical framework. To explore the subject matter, a descriptive approach was chosen. Now, descriptive study, as Nassaji (2015) puts it, is less about the "how" or "why" of a thing and more about simply defining its properties, what it is, if you will. Think of it as shining a light, like Fox & Bayat (2007) suggest, on present-day issues, allowing for a fuller understanding. We're talking about studies that paint a picture of various facets of a given phenomenon. What's interesting is that a descriptive study can work with multiple variables, but it only needs one. In most cases, these studies describe, explain, and, of course, validate research findings. And given what this research wanted to achieve, a descriptive methodology seemed like the most sensible path to take.

## Cyberterrorism

Another defining term of cyberterrorism is the intentional application or threat of application, having no legal basis, of violence, disruption, or interference of the cyber system, when it is probable that such application would lead to loss of life or injuries to a person or persons, physical property damage, civil order, or other serious harm. Terrorism may be viewed as an assault on the interests of the state, and at times, it may be an assault on the private industry (Lavorgna, 2020). The term is self-explanatory because it is a combination of the words cyberspace and terrorism to emphasize the applicability of terrorism to or via the internet (Hufnagel and Moiseienko, 2019; Marsh and Melville, 2019). The use of the internet by terrorists has been a significant trend in the last ten years, and it could be an effective method of targeting a large audience (Abaimov & Martellini, 2020; Martellozzo & Jane, 2017).

Scholars such as Bancroft (2019), Leukfeldt and Holt (2019), and Yar and Steinmetz (2019) identify the following as the primary uses of the internet by terrorists:

## Propaganda

The Internet, and especially since the development of Web 2.0, is a very inexpensive means of conveying a message. It may also be conveyed without criticizing the message, and this would not be the case with other media. It is clearly reflected through the respective videos posted on YouTube, which frequently depict the inhumane activities of

terrorists. The recruitment videos are also uploaded, and they give a very skewed perception of the aims of the terrorist group to create the impression that their actions are somehow justified.

**2. Fundraising**

Terrorism is a costly operation, but with a political agenda that individuals relate to, there will always be people willing to donate to the cause. Having a global reach had become a much easier task, as a fundraising site can be established and then distributed via email, social media, and hyperlinks. There are a number of online payment systems that permit individuals to give donations. Anonymous money transfers can also be made using the internet, and this may be especially appealing to the problem of terrorism because the citizens of the United States will be able to contribute money without any form of punishment.

**3. Information Dissemination**

It is different from propaganda; the flow of information would benefit the cause and not a particular group. There are many instances of bomb-building instruction on the internet and manuals that help in terrorism. This spread is not supposed to be a recruitment of a specific group, but empowering those who are sympathetic to the cause to work out their strategies for producing terror. Such information spread is a genuine threat to society because it enables individuals to make improvised explosive bombs at low cost, without any reason, which may broaden the danger of an assault.

**4. Secure Communication**

The Internet opens up completely new means of communication, i.e.. VoIP (Voice Over Internet Protocol) software packages like FaceTime, Facebook, WhatsApp, and Skype. It is a benefit because one can create an anonymous email address, which is associated with an anonymous Skype address. Hence, the possibility of the authorities knowing that there is the existence of the call exists might be distant.

**Ransomware**

Ransomware is a type of virus that attackers can employ to lock or encrypt a device to extort money from the individual or business in exchange for an unguaranteed promise to restore access (ESET, 2021). The Cuba ransomware gang has infected 49 companies that rely on vital infrastructure. The gang has paid at least $43.9 million in ransom, according to the FBI. Typically, the organization targets businesses in the United States, South America, and Europe. McAfee stated that the gang had, in certain instances, sold stolen data. Cuba ransomware is a more established ransomware strain that has been active for several years. According to the McAfee analysis, the criminals behind it recently turned to exposing stolen data to boost their damage and money, similar to what we have seen recently with other significant ransomware operations (Greig, 2021).

**The mechanism through which ransomware operates**

According to ESET (2021), a world-leading cybersecurity expert software house, cybercriminals who utilize ransomware employ a variety of approaches, including the following:

1. **Crypto-ransomware:** This ransomware encrypts user files stored on the computer's hard drive.
2. **Disk coding ransomware:** This ransomware encrypts the Master Boot Record and crucial file system structures, thus shutting down the operating system.
3. **PIN padlock ransomware:** This ransomware modifies the device's PIN code, preventing access to its content and functions.
4. **Screen locker ransomware:** This ransomware prevents users from accessing any part of the device's screen except for the malware's user interface.

**International Laws on Cybercrime**

International law provides many prohibitions, limitations, and authorizations of relations between nations and other international participants (most importantly, international organizations) (Kittichaisaree, 2017). It has opened the path to issues of global governance, such as nuclear proliferation, commerce, and the environment, among others, being controlled. The applicability of international law in cyberspace has increased as countries start to pay increased emphasis on cyberspace governance (the technological infrastructure that allows the World Wide Web to operate) and cyberspace governance (how governments, industry, and consumers can utilize this technology) (Hollis, 2021).

To make sure that legislation is enacted and it is well implemented by its signatories and subjects, public international law needs to have clear dispute resolution mechanisms, including arbitration (Cali, 2015). The complexity of the participants and the issues described above makes arbitration more advanced (Adonis, 2020).

**Cybercrime's International Aspects**

The gravity of the relevant difficulties has increased emerging countries' concern for prudently establishing and deploying reliability and security (Lavorgna, 2020; Littler & Lee, 2020). Thus, the benefits and advantages of ICTs may

benefit citizens not just through economic activity but also through their use in fields such as health, education, and e-government (Carlson, 2019; Gillespie, 2019).

International dimensions of cyber legislation, according to Schober and Schober (2019), include the following:

1. Create hardware and software solutions for encouraging and sharing best practices in information technology security and related legitimate concerns.
2. To enhance security and make the cyber environment less tempting to criminals, consumer trust is increased while using internet information on service apps.
3. To help and engage with member states in developing progressive law and establishing exemplary legislation in the areas of online services, online security, ethical issues, cybercrime deterrence, data protection, and privacy.
4. To identify cybercrime vulnerabilities and risks and to deploy solutions that protect the internet users and their applications' ICT infrastructure across many networks.

**The European Union and the United States of America's Initiatives**

The U.S. cyber-law operations are discussed below due to the position of the country as the technology giant and the largest economy in the world in terms of nominal GDP, 21.43 trillion. The European Union is a political and economic union comprised of 28 states. It is the most essential monetary union in the world with a nominal GDP of $18.70 trillion. China is the third-largest economy in the world after the United States and the European Union. It is favored by the fact that it is a regional powerhouse, and its nominal GDP is 14.14 trillion (IMF, 2020).

The following are among the best federal law enforcement agencies charged with the mandate to investigate cybercrime on a domestic scale:

1. Alcohol, Tobacco, and Firearms Bureau (ATF).
2. Immigration and Customs Enforcement of the United States (ICE).
3. The Postal Inspection Service of the United States (USPIS)
4. Federal Bureau of Investigation of the United States of America (FBI)
5. United States Secret Service (USSS).

The cybersecurity law in the United States of America has immense experience and knowledge. It has established and published a system that allows users of information communication technology to report cybercrime against other users.

1. All states have a cybercrime monitoring service that has convenient points of reporting. The state offices have friendly contacts, which are easily accessible, and cybercrime can be reported to the local office of the respective agencies by merely calling an accessible duty complaint officer.
2. The headquarters of all the law enforcement agencies are based in Washington, DC, where different law enforcement agents who are trained and specialized in their respective fields are on guard. The United States Secret Service and the Federal Bureau of Investigation are based in Washington and prevent the violent incursion by cybercriminals. The cybercriminals, in most cases, are driven by the desire to make money or get hold of secret information. They are mostly known as hackers, since they infiltrate legitimate computer networks.

In 2000, the Federal Bureau of Investigation established the Internet Crime Complaint Center (IC3) with the help of the National White Crime Complaint Center, another organization of significant U.S. law enforcement. It serves as a place of clearing cybercrime complaints, formulation of strategies, as well as referral of cybercrime complaints in fighting an increasing cyber threat.

Staff attitude towards victims of cybercrime is incredibly positive at the IC3, and it is not hard to report the crime due to their polite reporting system that immediately notifies the concerned authorities and provokes the required response to cybercriminals. Also, IC3 guarantees the sustained existence of the central referral system to the federal, state, and local regulatory and law enforcement agencies. Although the European Union has enacted virtually the same set of rules as in the United States regarding electronic commerce and commerce via legislation, and even requires non-member states to unify their laws with the E.U. initiative prior to joining (Fuster & Jasmontaite, 2020; Synodinou et al., 2020).

**Chinese Initiatives**

After the U.S., China has the second most significant internet user base. This country has roughly 111 million internet users. China benefits from technological innovation, but while a large number of people have accessed the internet, authorities have exercised little control or monitoring. It accelerated the expansion of cybercrime, including disseminating pornographic material, hate and threatening messages, illegal gambling, and online fraud. Chinese officials handled the situation admirably. They implemented monitoring and controlled their internet users, which slowed the spread of criminality and boosted their e-commerce.

Shenzhen is a contemporary metropolis in southern China. By the end of 2015, the city had 8.97 million internet users, according to the Shenzhen Association of Online Media and the China Internet Network Information Center

(CINIC). The highest proportion in the country, 83.2 percent of Shenzhen's total population, comes on the heels of success in battling online crimes and the rapid spread of harmful material through the establishment of a cyber police unit.

China's cyber police have established a system for monitoring and regulating internet activities. When a user signs in, a flashing icon denoting the police department's presence appears on the user's screen. When consumers intend to file a complaint against cybercrime, they must click the appropriate button and promptly notify the proper complaint officer. Within a few months, cyber police were alerted to online crimes by a click on an icon that had accumulated over 100,000 visits, including over 600 consultation services on cybercrime legislation, and 1,600 reports of illegal online conduct were given to the appropriate authorities for investigation. Following the success of Shenzhen, the Ministry of Public Security intends to deploy cyber police in eight major Chinese cities.

## Conclusion

Cybercrime is growing at a breakneck speed on a worldwide scale. It is a more difficult offense to identify and prosecute than typical offenses. The integration of cyberterrorism and ransomware in the digital era is a radical change in the character of the threats to global security. The two phenomena share the same technological vulnerabilities of networked systems, critical infrastructure, and digital communication channels, but the motives the two once had before are slowly becoming intertwined. The disruption, coercion, and control of cyberterrorism ideological goals and the financial gains of ransomware overlap as they seek to achieve the same goals. This convergence disrupts the conventional standards of law enforcement and counterterrorism, which have traditionally defined terrorism and cybercrime as distinct areas.

With the increase in the digital ecosystem, the distinction between state and non-state powers, ideology and profit, as well as crime and warfare, is becoming increasingly unclear. The emergence of cyber mercenaries or state-funded ransomware attacks, as well as the adoption of cryptocurrencies by terrorist activities, has also made the process of attribution and accountability more difficult. Such dynamics point to the lack of proper national efforts to tackle a transnational issue through fragmented means. The only way to solve these hybrid threats is through a concerted international policy- one that incorporates both legal, technical, and policy responses. The main areas of international cooperation should be intelligence sharing, capacity building, and standardization of the cybercrime laws. At the same time, it is crucial to strengthen the collaboration between the government and the business world, raise awareness of cybersecurity, and create resilient digital networks to minimize systemic vulnerabilities. Finally, to tackle the twin threat of cyberterrorism and ransomware, it is important to note that the two are not just a technological problem to solve but a multidimensional security problem. The world can only reduce the dangers of this developing nexus of ideology and extortion through the combined efforts of international policies and approaches to global governance, as well as through long-term international cooperation.

## Solutions and Recommendations

The United States of America has tremendous expertise and understanding of cybersecurity law. It has created and publicized a mechanism for information and communication technologies to report cybercrime. While the E.U. has adopted nearly identical standards to those in the United States governing internet commerce and commerce through legislation, the European Union also ensures that new members align their laws with the E.U. effort before formally joining. China's cyber police have created a system for patrolling and monitoring people's online activity. When a user logs in, a symbol indicating the presence of the police department flashes on the computer device. Whenever users wish to make a cybercrime complaint, they must click the appropriate button and immediately report to the relevant complaint officer. Cybercrime awareness initiatives should be launched on a broad scale. A worldwide cyber army is necessary, and pupils should be educated about the cyber world. International conventions must be held on an official level to explore topics and concerns relating to the virtual world. At the household level, a specialized task force should be formed to ensure frequent checks of accessible internet connectivity. Websites should be strictly regulated in terms of objectionable material. Scholars should explore cybercrime concerns in various venues, including print and electronic media.

## References

Abaimov, S., & Martellini, M. (2020). Cyber arms security in cyberspace. CRC Press.

Adonis, A. A. (2020, March 14). International law on cybersecurity in the age of digital sovereignty. E-International Relations. https://www.e-ir.info/2020/03/14/international-law-on-cyber-security-in-the-age-of-digital-sovereignty/

Austin, G. (2020). National cyber emergencies: The return to civil defense. Routledge.

Bancroft, A. (2019). The darknet and smarter crime: Methods for investigating criminal entrepreneurs and the illicit drug economy (Palgrave studies in cybercrime and cybersecurity). Palgrave Macmillan.

Cali, B. (2015). International law for international relations. Palgrave Macmillan.

Carlson, C. T. (2019). How to manage cybersecurity risk: A security leader's roadmap with an open FAIR. Universal Publishers.

ESET. (2021). Ransomware: How it impacts your business. https://www.eset.com/int/ransomware-business/

Fox, W., & Bayat, M. S. (2007). A guide to managing research. Juta Publications.

Fuster, G. G., & Jasmontaite, L. (2020). Cybersecurity regulation in the European Union: The digital, critical, and fundamental rights. In M. Christen, B. Gordijn, & M. Loi (Eds.), The ethics of cybersecurity (The International Library of Ethics, Law, and Technology, Vol. 21, pp. 85–108). Springer. https://doi.org/10.1007/978-3-030-29053-5_5

Gillespie, A. A. (2019). Cybercrime: Key issues and debates. Routledge.

Greig, J. (2021, December 4). FBI: Cuba ransomware group hit 49 critical infrastructure organizations. ZDNet. https://www.zdnet.com/article/fbi-cuba-ransomware-hit-49-critical-infrastructure-organizations/

Hollis, D. (2021, June 14). A brief primer on international law and cyberspace. Carnegie Endowment for International Peace. https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763

Hufnagel, S., & Moiseienko, A. (2019). Criminal networks and law enforcement: Global perspectives on the illegal enterprise. Routledge.

International Monetary Fund. (2020). World economic outlook database. https://www.imf.org/external/pubs/ft/weo/2019/02/weodata/index.aspx

Kittichaisaree, K. (2017). Public international law of cyberspace. Springer.

Lavorgna, A. (2020). Cybercrimes: Critical issues in a global context. Springer.

Leukfeldt, R., & Holt, T. J. (2019). The human factor of cybercrime. Routledge.

Littler, M., & Lee, B. (2020). Digital extremisms: Readings in violence, radicalization, and extremism in the online space. Springer Nature Switzerland AG.

Marsh, B., & Melville, G. (2019). Crime, justice, and the media. Routledge.

Martellozzo, E., & Jane, E. A. (2017). Cybercrime and its victims. Routledge.

Nassaji, H. (2015). Qualitative and descriptive research: Data type versus data analysis. Language Teaching Research, 19(2), 129–132. https://doi.org/10.1177/1362168815572747

Schober, S. N., & Schober, C. W. (2019). Cybersecurity is everybody's business: Solve the security puzzle for your small business and home. ScottSchober.com Publishing.

Synodinou, T. E., Jougleux, P., Markou, C., & Prastitou-Merdi, T. (Eds.). (2020). E.U. internet law in the digital era: Regulation and enforcement. Springer International Publishing.

Willems, E. (2019). Cyber danger: Understanding and guarding against cybercrime. Springer.

Yar, M., & Steinmetz, K. F. (2019). Cybercrime and society (3rd ed.). SAGE Publications Ltd.