WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

The Role of International Criminal Court (ICC) Jurisdiction in Prosecuting Cyberterrorism

Ishika Gupta[1], Dr. Prateek Deol[2]

[1] Student, LL.M. (Master of Laws), SRM School of Law, SRM University, Sonepat, Haryana, India.
[2]Associate Professor, SRM School of Law, SRM University, Sonepat, Haryana, India

ABSTRACT

The rapidly moving threat of cyberterrorism—cyberattacks motivated by ideology against critical digital infrastructure that pose a major challenge to the existing international legal architecture—constitutes an important element driving this research. The work therefore seeks to critically assess the ability of the ICC to prosecute acts of cyberterrorism under the Rome Statute. The methodology deployed throughout the study is doctrinal: it examines statutory provisions mainly Articles 5 to 8, ICC case law, as well as comparative instruments such as the Budapest Convention and EU Directive 2017/541. While cyberterrorism is not listed as a core crime under the Statute, this work interrogates whether cyberterrorism can constitute either a war crime or a crime against humanity insofar as those acts meet certain thresholds, such as systematic attacks on civilians or interference with protected infrastructure during an armed conflict. The study also highlights major barriers at the procedural and evidentiary stages; these include complexity of attribution, definitional issues, as well as problems of jurisdiction. National case law and legal contexts highlight the enhanced recognition of cyberterrorism within domestic courts as well as the possibilities and limitations of recourse to international adjudication. Recent ICC strategic documents and deliberations within the Assembly of States Parties appear to cautiously embrace a shift toward recognizing technology-enabled crimes. Yet the formal recognition of cyberterrorism either by way of treaty amendment under Article 121 or via an interpretational means through Article 21(1)(b) still awaits further strengthening of international cooperation and digital forensic capabilities. The study concludes that while the current institutional structure may not yet be able to competently prosecute cyberterrorist crimes, there exists a clear need for a multilevel development of law based on definitional clarity, treaty reform, and institutional change, to ensure accountability for cyberterrorism in the digital age.

Keywords: Cyberterrorism, International Criminal Court, Rome Statute, Jurisdiction, War Crimes, Crimes Against Humanity, Digital Attribution

Introduction

The rapid evolution of cyber threats in recent years has prompted a global reassessment of the legal mechanisms available for addressing acts of cyberterrorism. Thus, while the IT revolution brings great benefits, it also allows individualistic non-state actors greater chances for carrying out disruptive ideologically based attacks which go across national borders. These actions often undermine international peace and security. Under this circumstance, international criminal law finds itself at an important crossroads. The ICC is established under the Rome Statute to prosecute individuals for crimes of utmost concern to the international community. In this context, to the extent the traditional crimes listed under Article 5 of the Statute and which fall within the ICC's jurisdiction are genocide, crimes against humanity, war crimes, and the crime of aggression, they face serious limitations when confronted with the new-age threats of cyberterrorism. Therefore, this research in law aims to consider whether cyberterrorism as a new offense, technologically based, may fall under the ICC, and whether any interpretational, or structuring, changes will be necessary to equip the Court to respond properly to this new form of crime. [1]

Cyberterrorism is the use of digital channels and technologies to inflict harm, inculcate fear, or cause grave disruptions for political or ideological motives. It includes hacking to disrupt essential infrastructure such as electricity grids, air traffic control networks, or hospital information systems, causing mayhem, injury, or threats to the public safety. Also entailed by the definition are large-scale disinformation campaigns and the dissemination of propaganda using highly sophisticated AI tools to destabilize state or society. An alarming growth in such incidents, including ransomware attacks on public health institutions and AI-generated content used to manipulate elections and incite violence, has been observed in 2024 and 2025. The offenders are faceless, lawless entities operating with full impunity from one jurisdiction to another. This highlights the urgent need for international legal instruments to maintain accountability. Being the only permanent international court set up to prosecute individuals for core international crimes under the "Rome Statute," the ICC could thus be a critical forum for resolving such complex, transnational conduct. However, unlike crimes within the purview of the Statute, cyberterrorism stands not expressly listed; therefore, an immediate question that arises is: Can the existing provisions of the Rome Statute be interpreted or expanded in their scope to include cyberterrorist acts? An answer to this question requires an examination of the legal text, the Court's

[1] Shiv Raman, Nidhi Sharma, "Cyber Terrorism in India: A Physical Reality or Virtual Myth", 5 *IJLHB* 102 (2019).

jurisprudence, and international developments in dealing with cybercrime. Because cyberterrorists can hide their identities, initiate attacks from afar, and affect targets in various jurisdictions, better than anything else, they heavily undermine traditional principles of criminal jurisdiction and enforcement, hence necessitating an international coordinated legal response.

Cyberterrorism is the conscious use of digital networks and technologies to inflict harm or instil fear and great disturbances in pursuing one or more political or ideological objectives. These acts include hacking into the infrastructure systems for electricity, air traffic control, or hospital information systems to generate chaos, harm injuries, or threaten the safety of the public. The definition also contemplates wherein large disinformation campaigns and propagation are run through sophisticated AI tools in an attempt to destabilize governments or societies. There has been an alarming rise in incidents since 2024 and 2025, those being ransomware attacks on public health institutions and various forms of AI-generated content to manipulate elections and incite violence. The borderless nature of such offenses makes it difficult to seek an answer within the national framework and points toward the need for a robust international mechanism that can hold the perpetrators accountable. The ICC, as the only permanent international court to prosecute individuals for the core international crimes under the "Rome Statute", could be one truly important forum adjudicating such complex transnational conduct. However, none of the four categories of crimes set forth in the Statute explicitly refer to cyberterrorism. Hence, a pressing question arises: could the existing provisions of the Rome Statute be construed or expanded so as to include cyberterrorist acts? Such an inquiry must first include in-depth consideration of the Statute's text, the precedent of the Court, and the developments in international cybercrime jurisprudence. The need for an international legal solution is warranted by the fact that cyberterrorists can stay anonymous, launch attacks from the remotest part of the world, affect targets across several jurisdictions, and thereby completely destroy the traditional models of criminal jurisdiction and enforcement. [2]

The study follows the doctrinal research approach in law. It proceeds with a close-textual analysis of the Rome Statute and significant instruments of international law. It involves an examination of the definition and jurisdiction provisions under Articles 5 to 8 of the Rome Statute to determine whether acts of cyberterrorism may be construed within the range of existing international crimes. Jurisprudence of the ICC and other national courts will be reviewed critically to discern legal reasoning, either supporting or opposing the idea that cyberterrorism falls within the jurisdiction of the Court. Comparative perspectives would also be sought from systems like the Council of Europe's Budapest Convention on Cybercrime that, while aimed largely at the harmonization of domestic legislation, still offer useful references on international cooperation and criminalization. The analysis also incorporates more recent intelligence and data issued by international bodies, such as the 2024–2025 reports by the United Nations Counter-Terrorism Committee and the operational alerts of INTERPOL, to provide empirical and contemporary insight. These sources will be used to bring out the contemporary global dimension, methods, and effect of cyberterrorism and why it may require some form of extension or reinterpretation of present legal frameworks for the prosecution of such acts on the international stage. [3]

Defining Cyberterrorism in International Law

A doctrinal legal research methodology stands adopted in this study, relying heavily on close textual analysis of the Rome Statute and other relevant instruments of international law. It is concerned with analyzing the definitions and jurisdictional provisions laid out within Articles 5 to 8 of the Rome Statute to arrive at a firm conclusion on whether acts of cyberterrorism may fall within the ambit of existing international crimes. ICC and national courts' jurisprudence shall be reviewed in detail to extract legal arguments that may either support the inclusion of cyberterrorism within the jurisdiction of the Court or reject the same.

Conceptual Framework

Over the past years, global legal thinking has more and more considered cyberterrorism to be a significant threat to global peace and stability. As it appears in both policy and legal discussions, there is as yet no universally accepted definition in international law. This indefiniteness in terms of characterization creates the challenge of prosecuting and criminalizing cyberterrorism in a uniform manner. Although working definitions have been offered by the United Nations and other regional organizations, no binding international legal instrument yet defines or flatly outlaws cyberterrorism. This also has legal implications for domestic application as well as internationally against other organizations such as the International Criminal Court, which strictly requires exact legal definitions accepted under its constituent treaty, the "Rome Statute," to exercise jurisdiction. Accordingly, the parameters of cyberterrorism require legal definition and comprehension to marshal in the direction of an international convergence in reaction. This section will outline views on the international legal framework's approach to definition of cyberterrorism and will then address the conceptual challenges in situating cyberterrorism within the ambit of extant law. [4]

The separation in concepts between cyberterrorism, cybercrime, and cyber acts such as hacking or attacks is at the very core of determining how international law treats it. The term cybercrime is a far-reaching one that covers illicit online activities from identity theft, financial fraud, unauthorized data access, and breach of national and foreign laws. Hacking is not always criminalized, and even if it is, it generally does not have the political or ideological motivation behind it-the crime is actuality carried out by individuals or groups for their own personal or economic gains. While cyberattacks may include state and non-state actors, their existence lies between the breaches of data and infrastructure. Cyberterrorism is specific on intent and impact.

---

[2] Chapter II: Cyber Crime and Its Classification, *available at:* https://www.bbau.ac.in/dept/Law/TM/1.pdf (Visited on May 11, 2025).

[3] D. Broeders, F. Cristiano, et.al., "Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy", 46 *Stud. Confl. Terror.* 2426 (2021).

[4] Sudhakar Rolan, "An Analysis of Law Relating to Cyber Terrorism in International Perspective", 2 *IJLRA* 13 (2023).

It entails the use of digital means to create fear, coerce governments, or force the attainment of political, religious, or ideological objectives. The modus operandi comprises the use of some digital system or platform; the outcome is either massive or intended to cause disruption, loss in the economy, or physical harm.

Existing Legal Definitions

This conceptual organization is aligned with the criteria emphasized in "UN General Assembly Resolution 74/149 (2019)" on counter-terrorism, which calls on Member States to appropriately deal with emerging threats posed by the use of ICT by terrorists. The resolution points out that there is a great need for global cooperation in order to best counter the abuse of technology by terrorist organizations in recruitment, propaganda, planning, and carrying out attacks. It encourages states to implement legislation and institutions to address these threats in full respect of international law. These could include the intentional targeting of critical infrastructure, such as power grids, water supply, or medical networks, in a manner that would intimidate civilian populations or destabilize states. This essentially captures the essence of cyberterrorism; however, while cyberterrorism is similar to cybercrime and cyberattacks in means, unlike those, cyberterrorism is distinguished by its motivations, magnitude, and social impact. The conceptual clarity is vital for any future attempt to extend the jurisdiction of international penal bodies such as the ICC to cyberterrorism, as it is founded upon the principle of legality requiring that well-defined crimes must be laid out in a statute. [5]

Challenges in Defining Cyberterrorism for ICC

There are lots of conceptual and practical difficulties in drafting a fitting definition of cyberterrorism within the framework of the "Rome Statute". The most fundamental challenge lies in differentiating cyberterrorism from cyberwarfare or cyberattacks sponsored by a state. Many operations in cyberspace with presumably large-scale disruptive effects will be pursued by states or entities acting on behalf of states; hence there is ambiguity as to the legal characterization since state-actor violations never fall within the general understanding of acts of terrorism, which are basically criminal acts perpetrated by non-state actors. While trying to seek an ICC prosecution, an act must meet the criteria stipulated in Articles 5-8 of the Rome Statute as crimes falling under genocide, war crimes, crimes against humanity, and crime of aggression. Interpreting such acts to fit cyberterrorism within these prescriptions would need a substantial amount of interpretation and will arguably not cover varieties of behaviors in cyberterrorism, especially those not considered as acts of armed conflict or that do not directly target protected groups. [6]

Visibility stands as a huge issue in the matter of attribution. By its nature, cyberterrorism is difficult to attribute. In an effort to remain anonymous, cyberterrorists utilize technologies to obscure their identities; communication methods are encrypted, and servers route communications in a complex manner that makes it immensely difficult to unmask perpetrators with a high degree of certainty required for conviction in criminal proceedings. For the ICC to begin an investigation, there must be reasonable grounds to believe that a crime within its jurisdiction has been committed; additionally, some specific persons must be alleged to have been responsible. The uncertainty of attribution not only affects the possibility of leveling an accusation but also constrains the strength and perception of related legal authorities to pursue the matter. The ICC may be wholly incapable of responding to alleged crimes if attribution never rises to at least a semblance of clarity. Hence, there must first be an agreed global definition for cyberterrorism before meaningful interaction with the ICC can take place.

ICC Jurisdiction under the Rome Statute

In 1998, the impossible became reality with a plan made by States to set up a Court of last resort for the prosecution and punishment of offenders in cases of genocide, war crimes, and crimes against humanity. Thus, as a result of this mechanism, the International Criminal Court acting as a permanent tribunal prosecutes persons for the gravest crimes of concern to the international community. The ICC as a treaty-based body derives its power from a jurisdiction laid in the "Rome Statute". That implies that for any act to be prosecuted by the Court, it must either be expressly contained in the Statute or fall within the interpretative ambit of the presently conceived categories of crimes. Although being transnational in character and capable of causing serious harm to civilian populations, cyberterrorism is not on the list of crimes contained in the Statute. That silence has been the source of much academic and diplomatic debate on whether cyberterrorism could be indirectly prosecuted through reinterpretation or an expansion of the Court's existing categories of jurisdiction. Technological change in warfare and terrorism in cyberspace consequently invites us to examine how the fundamentals laid down in the Statute may yield to the new realities. [7]

Overview of ICC Jurisdiction

Founded upon the entry into force of the "Rome Statute" in 1998, the International Criminal Court (ICC) was arguably a pinnacle of enforcement within international criminal law. As a permanent institution, it prosecutes persons for those crimes deemed most serious by the international community. As a

[5] Nibedita Mohanta, "Combatting Cyberterrorism via Spatial Insights", available at: https://geospatialworld.net/prime/special-features/combatting-cyberterrorism-via-spatial-data-insights/ (Visited on May 11, 2025).

[6] Iftikhar S., "Cyberterrorism as a Global Threat: A Review on Repercussions and Countermeasures", 10 *PeerJ Comp. Sci.* 72 (2024).

[7] Astha Sharma, Aradhya Gupta, et.al., "Emerging Cybercrimes: Measures and Challenges in Cyberspace", available at: https://nhrc.nic.in/sites/default/files/Group%201_FEB%202022.pdf (Visited on May 11, 2025).

treaty-based institution, the ICC exercises jurisdiction strictly within the framework provided by the Statute. Therefore, any offense that can fall within the Court's prosecutorial jurisdiction either is statutorily included in the Statute or can be found to fit into one of the crime categories already in place there. Cyberterrorism, as having its reach transnational and potential for inflicting significant harm on civilian populations, is not now shown to be a named offense under the Statute. The void has generated sufficient debate in scholarly and diplomatic circles as to whether cyberterrorism may indirectly be tried through reinterpretation or expansion of the existing Court categories of jurisdiction. The evolution of war and terrorism under the cyber context necessitates an examination of the way the fundamental provisions of the Statute can be formulated to these new realities. [8]

Applicability to Cyberterrorism

The ICC exercises jurisdiction only over four crime categories explicitly enumerated in Articles 5 to 8 of the "Rome Statute" and these include genocide, crimes against humanity, war crimes, and the crime of aggression. Each category has certain specific legal elements, and the Court may only investigate and prosecute those crimes that meet such elements. Jurisdictional competence takes into account other vital provisions. "Article 12" sets forth the Court's territorial and personal jurisdiction, whereby the ICC can act if the crime was committed on the territory of a State Party or if the accused is a national of a State Party. If neither condition is satisfied, under "Article 13(b)", the Court would still be able to exercise jurisdiction if the matter is referred to it by the Security Council under Chapter VII powers of the UN Charter. Besides, "Article 13(a)" provides the possibility to refer a situation to the Court by a State Party, while "Article 13(c)" enables the Prosecutor to initiate investigations proprio motu on the basis of information received from victims, NGOs, or other reliable sources. These trigger mechanisms must be highlighted as they are essential in providing ways for matters to be brought before the Court notwithstanding possible jurisdictional ambiguities. Taken all together, they furnish an expansive but structured avenue for ICC intervention in grave international law matters- but in cases of cyberterrorism, their operationalization is legally unclear and procedurally complicated. Without a clear recognition of cyberterrorism, any attempt to encompass such acts under ICC jurisdiction must necessarily resort to a purposive and expansive interpretation of these provisions. [9]

Recent Developments

In response to rapidly evolving global security threats, the ICC has now taken a more deliberate stance with regard to the use of emerging technology in international criminal law. Although the Rome Statute remains silent on cyberterrorism among the crimes within the Court’s jurisdiction, a shift is evident in institutional policy and discourse. The 2023–2025 Strategic Plan of the ICC explicitly recognizes the increasing challenge posed by technology-driven crimes and emphasizes the need for increased Court capacity to investigate and prosecute crimes in which digital tools play a role, either in the commission of core crimes under its mandate or in the abuse of digital infrastructure for undermining civilian security and international peace. Key priorities set forth in the document include investment in cyber-forensics, fostering methodologies well-integrated with digital evidence, and building the expertise of the staff engaged in more technologically complex cases. While cyberterrorism itself is not mentioned, the umbrella term "technology-enabled international crimes" opens up the possibility of its accession through interpretive means or a future amendment to the Rome Statute. The strategic acknowledgment is a major stride in bridging the gap between the traditional jurisdiction of crimes and the more sophisticated nature of the threats today. [10]

With evolving global security threats, the ICC is attempting to target emerging technologies in relation to international criminal law. Even though the Rome Statute does not yet clearly enumerate cyberterrorism amongst the crimes of the Court's jurisdiction, institutional and other levels of consideration infer a shift approach. The ICC 2023-2025 Strategic Plan identifies the increasing threat of technology-enabled crimes and emphasizes the importance of the Court building its ability to investigate and prosecute crimes that have been committed through digital means. The crimes may involve violations of the core crimes with the help of sophisticated technologies or the exploitation of digital infrastructure to target civilian security or international peace. The strategy also provides key priorities, including investment in cyber-forensics, application of digital evidence approaches, and enhancing personnel capacity in prosecuting technology-intensive cases. Although cyberterrorism is not specifically mentioned, the broader term "technology-enabled international crimes" leaves the door ajar to encompass it either through interpretative evolution or through a future revision of the Rome Statute. This strategic recognition is a significant advancement toward closing the gap between the jurisdictional rigs of traditional crimes and the too contemporary modes of threats. [11]

Legal Challenges in Prosecuting Cyberterrorism at the ICC

The prosecution of cyberterrorism subject to the jurisdiction of the ICC is mired in a complicated web of legal, procedural, and definitional challenges. Although the Court’s administrative and policy mechanisms have acknowledged the strategic importance of responding to technology-enabled crimes, various doctrinal and practical constraints currently bar the actual enjoyment of jurisdiction over such acts. Cyberterrorism by nature cuts across borders, discards traditional investigative methods, and exploits both domestic and international institutional limitations. By virtue of being the constitutive instrument creating the ICC, the Rome Statute places strict confines within which the Court can exercise its jurisdiction. These confines do not presently recognize cyberterrorism by name. Therefore, the ICC must either rely on the most creative interpretation of existing provisions of the Statute to prosecute

[8] PTI, "NIA Files Chargesheet Against 8 Terrorists in ISIS-Kerala Module Case", *The Economic Times*, January 28, 2022.

[9] Cyber Security Breach at National Informatics Centre, Malware Attack Traced to Bengaluru, *ETGovernment*, September 19, 2020.

[10] HT Correspondent, "Kashmir State Investigation Agency Produces Chargesheet in Cyber-Terror Case", Hindustan Times, December 24, 2024.

[11] S. Haataja, "The 2007 Cyber Attacks Against Estonia and International Law on the Use of Force: An Informational Approach", 9 *LIT* 159 (2017).

cyberterrorism or await an amendment of the Rome Statute to introduced it expressly as an offense. This section elaborates on the three categories of challenges discussed above-jurisdictional issues, evidentiary and attribution problems, and the lack of a precise definitional framework.

Jurisdictional Limitations

Cyberterrorism prosecution under the International Criminal Court (ICC) has remained entangled in a complex web of legal, procedural, and definitional difficulties. Although technology-enabled crimes have been recognized by the administrative and policy mechanisms of the Court as relevant, the actual exercise of jurisdiction over such acts has remained yet hindered by several doctrinal and practical barriers. Cyberterrorism transcends borders, sidesteps traditional investigation procedures, and preys upon the weak spots of both domestic and international legal institutions. The Rome Statute, being the constitutive instrument of the ICC, places strict confines within which the Court must operate. Occasions where these boundaries may now be held to accommodate cyberterrorism are extremely rare in express terms. Either they must now choose between pari-materia highly interpretative routes under present provisions of the Statute or collaborate towards a formal amendment route making cyberterrorism an express prosecutable offense. Herein more comprehensive treatment is given to three key categories of challenges: jurisdictional constraints, evidentiary and attribution conundrums, and the lack of a precise yet operative legal definition. [12]

Evidentiary and Attribution Issues

The ICC has limited jurisdiction by both statutory intent and territorial application. Substantively, the Court shall prosecute only the crimes enumerated in "Article 5" of the "Rome Statute," that is to say: genocide, crimes against humanity, war crimes, and the crime of aggression. Since cyberterrorism is not among these core crimes, its prosecution would be limited only to situations where the conduct was able to be recategorized as one of the other listed crimes. This interpretative issue is aggravated by the Statute's adherence to the principle of legality by which crimes must be clearly defined and foreseeable in law. The lack of clear provisions relating to cyberterrorism imposes significant limitations on the Prosecutor's discretion and upon the admissibility determinations made by the Court. A further complication is that some of the major cyber powers, including China and Russia, are States not Parties to the Rome Statute. This greatly restricts the ICC's personal and territorial jurisdiction as enumerated under "Article 12", which restricts Court action only when either the crime is committed on the territory of a State Party or the accused is a national of a State Party-unless the United Nations Security Council has made a referral under "Article 13(b)". Further, "Article 17", in essentially providing the principle of complementarity, dictates that the ICC shall yield to national jurisdictions unless it is established that the domestic systems are unwilling or unable genuinely. This provision promotes state sovereignty, but it introduces an extra procedural step that must occur before the Court can initiate proceedings. In these practical implications, great delays follow with jurisdictional claims being weighed in doubt; hence, there will be an immense delay or postponement in prosecuting cyberterrorism at an international level. [13]

Definitional Ambiguity

When it comes to prosecuting cyberterrorism, the evidentiary landscape presents enormous hurdles at the ICC. One of the pressing issues pertaining to cyberterrorism is attribution—linking the cyber operation directly to an individual or an identifiable State actor. Most cyberattacks are carried through anonymizing networks, virtual private servers, or through other technologies that disguise the identity and origin. The shield of technology becomes a barrier in the ascertainment of mens rea and actus reus, which are the most basic elements in criminal prosecutions. Without clear conduct attribution, the evidential weight required at trial under the ICC standards may prove impossible to meet. The "Rules of Procedure and Evidence," particularly "Rule 63," admit digital and electronic evidence, provided this kind of evidence passes rigorous tests on its authenticity, reliability, and relevance. Within the context of cyberterrorism, however, where digital evidence may prove to be encrypted, located remotely, or subject to tampering, fulfilling these requirements might be made difficult, if not impossible. The ICC's encounter in the "Situation in Ukraine (ICC-01/22, 2024)" exposes the dual nature of digital evidence-both from the perspective of promise and limitation. Although the Court referred to open-source intelligence and intercepted communications concerning war crimes, it opted not to pursue cyberterrorism as a separate charge, primarily because cyber operations were allegedly involved in rendering civilian systems inoperative. This lacuna highlights the greater challenge of fitting cyber incidents into the penal framework of extant legal doctrines. Without some techno-legal infrastructure to ensure the origin and sanctity of digital footprints, and with no compulsory investigative jurisdiction over non-State Parties, the ICC undoubtedly has a far-fetched trip fulfilling the standard of international criminal procedure whenever cyberterrorism is concerned. [14]

Case Studies and Comparative Analysis

In regard to the necessity of case law analysis for how cyber-related offenses could be treated under the ICC's present jurisdiction, while the Rome Statute does not explicitly include cyberterrorism, cases and interpretations of law eligible for consideration could shed light on how cyber elements may be

[12] Michael Kenney, "Cyber-Terrorism in a Post-Stuxnet World", 59 *Orbis* 111 (2015).

[13] Don Melvin and Greg Botelho, "Cyberattack Disables 11 French TV Channels, Takes Over Social Media Sites", *CNN*, April 9, 2015.

[14] Digital Arrests: Understanding Their Legal Framework, Technology, and Case Studies in India, available at: https://www.indiancybersquad.org/post/digital-arrests-understanding-their-legal-framework-technology-and-case-studies-in-india (Visited on May 11, 2025).

situated in the current ICC framework. Comparative legal developments at the national level have far-reaching lessons for prosecutors as regards themselves and to the problems of definitional limits and evidentiary fronts. National courts have, however, in recent years, stayed quite active in adjudicating cyber-enabled terrorism and related offenses, but ICC experience is still very scarce, while the evolution of digital conduct with some cyber elements is very likely to be scrutinized in international criminal law in the very near future. The clash between national legal trials and the constrained ICC practice based on statute accentuates, therefore, both opportunities and limitations attendant upon the trials of cyberterrorism at the international level. Within this framework, the study of both ICC case law and national judgments can provide a broadened viewpoint with respect to how cyberterrorism-related conduct could be adjudicated and which legal routes could guide in formalizing this course in the years ahead. [15]

ICC Case Law with Cyber Elements

Testing existing case law is necessary to ascertain the possibilities of the current International Criminal Court (ICC) jurisdiction for cyber-related crimes. Though cyberterrorism is not mentioned per se by the Rome Statute, the assessment of relevant rulings and legal interpretations still provides some insight into the ways cyber elements may be treated under the current ICC framework. Parallel legal developments at the national level also hold considerable importance for prosecutorial approaches, definitional limits and evidentiary methods. Increasingly national courts are adjudicating cyber-enabled terrorism and related offenses, meanwhile the ICC experience remains limited, save for a few early cases involving some cyber element that represent the growing potential of digital conduct being scrutinized through the lens of international criminal law. This divergence between national legal experimentation and the ICC's highly restrained, statute-bound practice serves to illuminate both possibilities and limits regarding the prosecution of cyberterrorism at the international level. Against this backdrop, a glance at ICC case law as well as national rulings would thus open up a wider view of how cyberterrorist conduct may be tackled and which legal perspectives may inform a more formal international approach in the future. [16]

National Case Laws

The International Criminal Court has never conducted a cyberterrorism trial per se. In any event, some cases show how cyber elements could be analogized with crimes already laid down under the Rome Statute. One such example is "*Prosecutor v. Al Mahdi*"[17], which dealt with the intentional destruction of cultural heritage in Timbuktu. Though it was a physical act rather than a cyberattack, it established the presumption that cultural property is worthy of international criminal protection. This opens the door for a conceptual application of similar logic to cyberattacks that destroy digital heritage-the historical archives, religious texts, or indigenous cultural databases-as cultural property. Were cyberterrorists to attack such digital repositories with the intent of erasing cultural memory or identity, their acts might be said to constitute crimes against humanity or war crimes, depending on the context. Another case with indirect cyber implications is "Situation in Georgia (ICC-01/15, 2023)," whereby it is reported that the cyberattacks on critical infrastructure during an alleged armed conflict in 2008 were being looked into. The investigations into such cyber operations considered the possibility of war crimes rather than hanging upon a charge of cyberterrorism; again, this highlights the circumspect approach the ICC adopts regarding the further extension of its jurisdiction over cyberconduct, even when such conduct is linked to armed conflicts.

Comparative Frameworks

The examination of comparative legal frameworks is of utmost importance for shedding light on the manner international and regional instruments have dealt legally with cyber-enabled offenses and to give possible directions to the extension of the jurisdiction of the International Criminal Court (ICC) to cover cyberterrorism. One of the widely referred instruments is the "Budapest Convention on Cybercrime", which remains the only binding international treaty that addresses cybercrime in general. Article 5 of the Convention criminalizes system interference, intending to hinder purposely the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data. The inconvenience in terms of the technical characteristics of cyberattacks is correctly defined, but the motive and bigger scheme of such attacks remain unaddressed. Hence, this provision does not distinguish between attacks committed for profit, espionage, or acts of terrorism but treats system interference just as any other general criminal offense. Conversely, the work of the ICC as contained in the "Rome Statute" is appointed to concentrate on crimes which outrage the conscience of humanity, that is, genocide, crimes against humanity, war crimes, and the crime of aggression. The variation in scope highlights the first major issue: the Budapest Convention being technical and behavior-based, while the ICC framework is motive-based and consequence-oriented. In other words, the Budapest convention could be an instrument in prosecuting cyber conduct at the operational level but is devoid of the jurisdictional and philosophical perspective embraced by the ICC to prosecute awful international crimes. [18]

Examining comparative legal frameworks is crucial to understanding whether and how international and regional instruments legitimize those cyber-enabled offenses and, consequently, how these approaches could be extended to the possible inclusion of cyberterrorism within the jurisdiction of the International Criminal Court (ICC). One of the widely cited and most pertinent instruments is the Budapest Convention on Cybercrime, which is still the only binding international treaty on cybercrime. "Article 5" of the Convention outlaws system interference, defined as the intentional hindrance of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data. While the provision

[15] Tanvi Mehta, "Indian Police Arrest Minor for Hoax Bomb Threats on Flights", *Reuters*, October 17, 2024.
[16] Indian WhatsApp Lynchings, available at: https://en.wikipedia.org/wiki/Indian_WhatsApp_lynchings (Visited on May 11, 2025).
[17] ICC-01/12-01/15, 2016.
[18] Press Trust of India, "Potential for Spread of Terror from Social Media Higher Than Ever: Centre", *NDTV*, December 13, 2022.

successfully captured the technical components of cyber attacks, it leaves out the motive and the greater context in which those attacks could have been committed. Therefore, it could be said that the Convention does not make any distinction among acts carried out for profit, for espionage, or for terrorism, treating system interference as just another ordinary offense. On the other hand, the ICC is based, under the Rome Statute, on crimes that utterly shock the conscience of humanity, namely genocide, crimes against humanity, war crimes, and the crime of aggression. This clear-cut distinction in scope emphasizes the fundamental problem: the Budapest Convention tends to be technical and behavior-oriented, whereas the ICC statutes are oriented toward motive and consequence. Thus, even if the Budapest Convention may be used to prosecute a cyberattack, that prosecution will not in any way be philosophically or jurisdictionally aligned with the ICC mandate to prosecute grave international crimes. [19]

Conclusion

The virtual globalisation of global war brings yet a further component of intricacy to the already fragile line between state sovereignty, technological advancement, and justice to victims of gross human rights abuses. Cyberterrorism is expanding in its reach and impact, freezing vital infrastructure, influencing public opinion, and endangering civilian lives; the current legal framework of the 'Rome Statute' is therefore found by many to be increasingly irrelevant. The current Statute fails to absolutely define crimes in cyberspace and does not leave enough space for a liberal interpretation without colliding into serious legal and procedural challenges. However, with cyberterrorism acts starting to match and sometimes surpass the destructive force of traditional crime, it is hardly debatable to place these crimes under ICC jurisdiction.

The International Criminal Court (ICC), when it comes to trying cyberterrorism, is a stark case of one of the more urgent and still pending international criminal law issues. The technological shift of international conflict imposed a further layer of complexity on an already precarious balancing act between state sovereignty, technological progress, and the quest for justice for victims of massive atrocity. The activities that form cyberterrorism, with their continuously growing magnitude and reach, obstruct critical infrastructure, affect public opinion, and even threaten civilian lives-from the Rome Statute's point of view, the necessity for an effective framework increases with each passing day. So evidently, the Statute as it stands now does not contemplate either crimes committed in cyberspace or more critically grant any material flexibility for their reinterpretation without hitting significant legal and procedural hurdles. But when the actions that fall under the category of cyberterrorism begin to look like and even surpass traditional crimes in terms of sheer destructive potential, compelling arguments begin to take shape for bringing them onto the ICC's agenda.

If one makes a comprehensive analysis of the legislation, institutional practice, and new international debate, one would perceive that the ICC, though currently constrained in scope, has the ability and responsibility to develop. Through the mechanisms of "Article 21(1)(b)," the Court can, by way of interpretation, engage with cyberterrorism within the category of other crimes, like crimes against humanity or war crimes, provided the conduct crosses the required thresholds. But any such interpretation needs to be carefully framed to maintain the legality, certainty, and non-retroactivity on which international criminal adjudication is founded. Statutory modification, conversely, if not a political minefield under "Article 121" of the Rome Statute, would be a more permanent and transparent foundation on which to try cyberterrorism. Even so, in pragmatic terms, the ICC could create internal prosecutorial policies targeted at cybercrimes and would be in a good position to coordinate nascent global initiatives, particularly with INTERPOL and the UN Counter-Terrorism Committee, thereby at least offering an interim remedy to gaps in enforcement.

Suggestions

Having explored the jurisdiction of the ICC in prosecuting cyberterrorism acts, it is fitting to propose the measures below in order to fill legal gaps and enhance the institutional responsiveness of the ICC:

1. Adopt model national laws aligned with international norms to criminalize cyberterrorism domestically. These laws should facilitate cooperation with the icc and other international bodies in transnational cyber cases.
2. Develop internal prosecutorial guidelines within the icc that outline investigative protocols for cyber-enabled offenses. These guidelines should include best practices for collecting, preserving, and authenticating digital evidence.
3. Encourage collaboration between the icc and interpol for the exchange of cybercrime intelligence and digital forensics. Joint task forces could accelerate attribution and improve case preparation.
4. Encourage the ICC’s office of the prosecutor to issue a policy paper interpreting how existing provisions on war crimes and crimes against humanity may apply to certain cyberterrorist acts. This would provide interim legal clarity and guide future case evaluations.
5. Facilitate multilateral dialogues between the icc and regional organizations such as the european union and african union. These dialogues should focus on harmonizing legal definitions and identifying shared enforcement strategies for cyberterrorist threats.
6. Initiate formal discussions under article 121 of the rome statute to consider an amendment explicitly including cyberterrorism as a core international crime. This process should be supported by a working definition of cyberterrorism that distinguishes it from cybercrime and cyberwarfare.

[19] Sampath Kumar Venkatachary, Jagdish Prasad, et.al., "Cybersecurity and Cyber-Terrorism Challenges to Energy-Related Infrastructures – Cybersecurity Frameworks and Economics – Comprehensive Review", 45 *Int'l J. Crit. Infrastruct. Prot.* 100677 (2024).

7. Invest in cyber-forensic capacity building within the icc's investigative units. This includes hiring technical experts and creating partnerships with cybersecurity institutions to enhance attribution capabilities.
8. Promote academic and policy-oriented research on the intersection of international criminal law and emerging digital threats. Such research should inform future treaty negotiations and help develop jurisprudence in this evolving field.
9. Propose the creation of an advisory cyber crimes panel under the assembly of states parties. This panel would review trends, propose definitional standards, and guide strategic planning for addressing cyberterrorism.
10. Support the development of hybrid courts that combine domestic jurisdiction with international legal standards for cyberterrorism trials. These courts can fill jurisdictional gaps when the icc's authority is limited or contested.