Page 508 - 518 **DOI:** *https://doij.org/10.10000/IJLMH.116739*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 7 | Issue 1

2024

National Security Challenges in Extradition: Analysing Cybercrime Cases in the Digital Age

ABIYA REHMA[1]

ABSTRACT

The digital age has ushered in a new era of national security challenges, primarily driven by the evolving landscape of cybercrimes. Extradition, the legal process facilitating the transfer of individuals across jurisdictions for trial or prosecution, has assumed a pivotal role in addressing cybercrimes directly impacting the security of nations and their citizens. This study delves into the complex domain of extradition in the digital age, with a specific focus on cybercrime cases intertwined with national security interests. The central theme that emerges is the critical importance of harmonizing legal frameworks, particularly in the context of dual criminality requirements. Cybercrimes often transcend borders and can involve actions recognized as criminal in one country but not in another. Divergent legal frameworks, jurisdictional conflicts, and the absence of a comprehensive global treaty on cybercrime contribute to the complexity of extradition in this domain. Cases such as those of Gary McKinnon, Alexei Burkov, Julian Assange, and Meng Wanzhou, exemplify the intricacies of international extradition when dealing with cybercrimes and national security interests. Beyond legal considerations, the study explores the diplomatic, political, and human rights dimensions of cybercrime extradition. Striking a balance between national security imperatives and individual rights becomes a delicate challenge that extradition processes must navigate. It emphasizes the critical role of international cooperation in addressing jurisdictional challenges inherent to cybercrime extradition. In the rapidly evolving landscape, the development of best practices and model approaches is essential to mitigate jurisdictional difficulties and ensure justice prevails, even in the face of cyber threats transcending borders.

Keywords*: Cybercrime, Dual Criminality, Extradition, Human Rights, Jurisdictional Challenges, National Security.*

I. INTRODUCTION

The difficulties of preserving national security have changed in an increasingly digital and networked world, where cybercrime poses a serious and ever-increasing threat. The practice of

[1] Author is a student at Christ University, School of Law, India.

 [ISSN 2581-5369]

extradition, which is the legal procedure of moving someone from one nation to another for prosecution or trial, is essential to thwarting these dangers and apprehending hackers. An essential instrument at a country's disposal for pursuing offenders worldwide who commit cybercrimes that jeopardise national security and that of its inhabitants is extradition.

Fundamentally, extradition is a legal system intended to guarantee that criminals are held responsible for their acts, wherever in the world they may have committed them. It is based on the ideas of reciprocity and reciprocal legal support among sovereign governments. The legal basis supporting this practise is provided by extradition treaties and agreements, which allow nations to ask for the surrender of those who have committed crimes elsewhere, guaranteeing that justice is universal.

The role of extradition becomes distinct and crucial in the situation of cybercrime. Cybercrimes comprise a broad spectrum of unlawful actions carried out via digital channels, such as cyber espionage, hacking, identity theft, and data breaches. These crimes have the potential to seriously affect a country's national security since they can target vital infrastructure, jeopardise private data, and interfere with the operation of the political or economic system.

The legal definitions that form the foundation of the cybercrime extradition process must be thoroughly understood to successfully navigate its complex web. The word "cybercrime" is broad and includes a variety of illicit acts carried out using computers, digital devices, and the internet. The concept of cybercrime in the context of extradition must be compliant with the laws and legislation of both the requesting and requested countries.

The difficulty in obtaining extradition for cybercrime is due to the distinct and changing nature of these offences as well as the differences in the legal systems of other jurisdictions. As a result, it is essential to explore the subtleties and complications of extradition in the modern day, with an emphasis on cybercrime cases that directly affect national security. To shed light on how international law enforcement is changing in an interconnected world by examining the ideas, difficulties, and ramifications of extraditing cybercriminals engaged in actions that endanger national security. This analysis also emphasises how important it is for nations to cooperate and create legislative frameworks that take into account the dynamic and worldwide character of cybercrime.

(A) Research objective

The research objective of this paper is to provide a comprehensive analysis of the evolving landscape of international extradition concerning cybercrime cases with direct implications for national security. Examine the extradition agreements and legal systems in place for handling

 [ISSN 2581-5369]

cybercrimes that have an impact on national security, paying particular attention to how legal norms and definitions are standardised. Analyse the jurisdictional difficulties and disputes that occur when several nations claim the authority to prosecute cybercriminals, especially in cases when the offences are extraterritorial in character. Study the idea of dual criminality in the extradition of cybercriminals, looking into the ways that different countries' legal definitions of the same crime affect the extradition procedure.

(B) Research Questions

1. How does dual criminality principle requirements in cybercrime extradition cases with national security implications impact the laws and process?
2. What are the key jurisdictional challenges and conflicts that arise in the extradition of cybercriminals with national security implications?

II. THE IMPACT OF DUAL CRIMINALITY REQUIREMENTS IN CYBER CRIME EXTRADITION CASES WITH NATIONAL SECURITY IMPLICATIONS ON LAW AND PROCESS

The transfer of a criminal suspect or defendant from one country to another for prosecution or to serve a sentence is known as extradition, and it is a complicated and multidimensional legal process. It is an essential instrument for international collaboration and law enforcement, allowing nations to combat transnational crimes. However, there are difficulties in the process, especially when handling cybercrimes that affect national security. Requirements for dual criminality are crucial in extradition cases containing these offences because they influence the legal system and the way extradition requests are processed.

(A) Dual criminality

The concept of dual criminality is essential to extradition law. For extradition to proceed, the claimed offence must be illegal in both the seeking and requested countries. This concept essentially guarantees that people are not extradited for crimes that are not considered crimes in the nation of request. It serves as the foundation for determining whether extradition requests are legitimate and lawful. When it comes to cybercrime extradition, dual criminality is crucial. To fulfil the twofold criminality requirement, it is crucial to harmonise legal standards and definitions across nations because cybercrimes can include complex legal, technological, and jurisdictional factors. A complicated network of domestic and international legal systems and procedures are involved in extradition. Conventions, accords, and treaties between nations usually control international extradition. These accords set forth the requirements for

extradition, such as dual criminality, as well as the legal duties and processes associated with it. Every nation has its own extradition laws and regulations that are intended to carry out the terms of the international accords and make the extradition process easier. Among other things, these laws frequently include the concept of dual criminality. In the case of Lauri Love[2], a British hacker, faced extradition to the United States for alleged involvement in hacking U.S. government agencies, including the Federal Reserve and NASA. The U.S. charged him with computer crimes and aggravated identity theft. The case raised dual criminality concerns as the charged offences did not precisely align with the laws in the United Kingdom. The question of whether Love's actions constituted criminal conduct in both jurisdictions was central. The extradition request was denied by the U.K. authorities. They argued that the severity of the penalties in the U.S., such as mandatory minimum sentences, could breach Love's human rights. This case highlights the challenge of reconciling legal frameworks and the potential human rights implications.[3]

(B) **Impact on Legal Definitions and Framework**

The legal structure and concepts of cybercrimes that have ramifications for national security are greatly impacted by dual criminality requirements. While certain nations may have detailed legal definitions for different kinds of cybercrimes, differences may occur when other nations have different legal systems or don't have laws specifically addressing these offences.

1. Case-Specific Considerations: Evaluations of dual criminality are by their very nature case-specific. The facts and circumstances of the case determine whether an offence qualifies as dual criminality. Even if the claimed conduct is somewhat identical, what would qualify as a cybercrime in one instance might not satisfy the dual criminality criterion in another.
2. Difficulties and Ambiguities: When legal frameworks and definitions vary between nations, difficulties and ambiguities related to dual criminality may arise. Different evaluations of dual criminality may arise from divergent legal interpretations of what defines a given cybercrime, which may have an impact on extradition proceedings.
3. Complicated Legal Evaluations: In cases involving cybercrime, extradition requests frequently call for complex legal evaluations. Authorities and legal professionals need to carefully examine the legal aspects of the alleged offence, taking into account whether

[2] Lauri Love v. United States, [2018] EWHC 172 (Admin) (High Court of Justice, Queen's Bench Division, Administrative Court, 05/02/2018)b
[3] J. A. Coutts, Double Criminality, 48 J. CRIM. L. 93 (1984).

 [ISSN 2581-5369]

or not it complies with the laws of both nations. This procedure, which entails a thorough examination of the particular acts in question, can be difficult and time-consuming.

(C) National Security Concerns and Cybercrime Extradition

The influence that dual criminality has on cybercrime extradition is significantly shaped by national security considerations. For nations, national security is of utmost importance, and some cybercrimes are intimately associated with these worries. These worries frequently collide with ideas about dual criminality, which makes the extradition procedure more difficult. Concerns about national security have several noteworthy consequences, such as when a country feels that a cybercrime constitutes a serious risk to national security, it may request extradition. Cybercrimes that pose a risk to vital defence systems, the economy, or key infrastructure are especially concerning. Software entrepreneur John McAfee [4]faced extradition to the United States from Spain. He was charged with various tax-related offences, including tax evasion and wilful failure to file tax returns. The U.S. claimed that his actions had national security implications as they could undermine the tax system. The case brought dual criminality into question, as the tax offences in the U.S. did not perfectly match Spanish tax laws. Spain's extradition laws include dual criminality as a requirement for extradition. John McAfee was found dead in his prison cell in Spain before extradition could occur, so the case did not reach a final resolution. However, it highlighted the complexities of extraditing individuals for tax-related offences with potential national security implications.[5]

(D) Interplay with Dual Criminality

There are several intricate ways in which national security issues and dual criminality can interact. Even though a cybercrime might not have a corresponding crime in the requested country's legal system, it might be seen as a threat to national security in the asking country. The dual criminality requirement is not always met by the existence of national security issues. In cybercrime cases involving national security, dual criminality assessments necessitate a careful balancing act between protecting national security interests and upholding the rule that extradition should not be used to prosecute acts that are not considered criminal in the country of request. One of the most important issues in these kinds of extradition proceedings is finding this balance.[6]

(E) Extradition Treaty Provisions

[4] United States v. McAfee, 1:20-cr-10029-STA, Document 3 (W.D. Tenn. 2020).
[5] John Bassett Moore, Treatise on Extradition and Interstate Rendition (1891).
[6] J. A. Coutts, Double Criminality, 48 J. CRIM. L. 93 (1984).

When it comes to handling dual criminality issues in cybercrime cases that have an impact on national security, extradition treaties frequently play a critical role. A legal basis for extradition relations is provided by these treaties, which are negotiated and ratified by nations. A lot of extradition treaties have clauses addressing dual criminality and provide instructions on how to determine if an accused offence satisfies this condition. Extradition treaties may differ in their provisions about dual criminality. Certain treaties may contain more precise definitions or criteria, while others may have broader language that covers a wider variety of offences. These clauses give a more defined legal framework for determining the legitimacy of the accused offence and clarify how dual criminality applies in extradition situations.

III. JURISDICTIONAL CHALLENGES AND CONFLICTS IN EXTRADITION OF CYBER CRIMINALS WITH NATIONAL SECURITY IMPLICATIONS

The complex and dynamic character of cybercrime in the digital era is reflected in the plethora of jurisdictional difficulties and disputes that arise when cybercriminals with consequences for national security are extradited. This essay examines and offers a thorough examination of the main jurisdictional problems that emerge in these kinds of situations.

(A) Differing legal structures

Divergent legal frameworks across nations pose a significant jurisdictional difficulty in cybercrime extradition proceedings. Laws and definitions of cybercrime might differ greatly between states. There might not be a legal provision in another nation that corresponds to what is deemed a criminal offence in another. It is very difficult to assess whether the prerequisites for dual criminality are satisfied because of this disparity.

For instance, an act that falls under one country's legal definition of cybercrime may not be under the requested country's legal definition of hacking and data theft. Because of this, it might be difficult to prosecute cybercriminals when their actions have an impact on national security if the applicable legal criteria are not consistent. Alexei Burkov[7], a Russian national, was arrested in Israel at the request of the U.S. government. He was accused of operating a platform that facilitated various cybercrimes, including credit card fraud, identity theft, and computer intrusion. The U.S. sought his extradition for a range of offences. The case raised jurisdictional conflicts because Burkov's alleged crimes had global implications, affecting individuals and entities in multiple countries. It also involved diplomatic tensions between the U.S. and Russia, as both countries sought Burkov's extradition. Burkov was eventually extradited to the U.S.

[7] United States of America v. Burkov, No. 1:15-cr-00245-TSE (E.D. Va. Jun. 26, 2020).

 [ISSN 2581-5369]

following a lengthy legal process, highlighting the challenges of coordinating international extradition in complex cybercrime cases.

(B) Cross-Border Nature of Cybercrimes

Cybercrimes, by their very nature, transcend national boundaries and often have a cross-border character. Cybercriminals can operate from one nation while targeting victims or critical infrastructure located in another. This inherent international dimension of cybercrimes significantly complicates the jurisdictional issues in extradition cases, making the process far more complex and challenging. In is essential to explore how the cross-border nature of cybercrimes amplifies the jurisdictional difficulties in extradition proceedings. Unlike traditional crimes that are confined by geographic boundaries, cybercrimes are global in scope. Cybercriminals can launch attacks, steal data, engage in cyber espionage, or commit acts of online fraud from virtually anywhere in the world. This means that the physical location of a cybercriminal is often separate from the location of their victims or the systems they target. As a result, determining the appropriate jurisdiction for prosecution becomes a complex and sometimes contentious issue. In the case of Gary McKinnon[8], a British national, was accused of hacking into U.S. government computers, including NASA and the Pentagon. The U.S. sought his extradition to face charges related to computer intrusion and damage to national security. The case raised questions about the extraterritorial application of U.S. law and whether the alleged crimes occurred within U.S. jurisdiction. The U.S. asserted jurisdiction based on the location of the hacked servers, while the U.K. argued that the offences were committed on British soil. The U.K. Home Secretary decided not to extradite McKinnon due to concerns about his mental health. This case highlighted the legal and jurisdictional complexities in cybercrime cases with national security implications.[9]

(C) Lack of International Cybercrime Treaties

Cybercrime is a relatively young and quickly developing area of law, in contrast to established offences. There are international treaties in place for other types of transnational crime, such as drug trafficking and terrorism, but no all-encompassing global treaty that targets cybercrime explicitly. The lack of a generally recognised legal framework for cybercrime can make it more difficult to prosecute and extradite cybercriminals who engage in actions that could jeopardise national security. Bilateral and multilateral agreements between nations are essential to

[8] * McKinnon v. Government of the United States of America and Another, [2008] UKHL 59 (H.L. 2007-08), on appeal from: [2007] EWHC (Admin) 762.
[9] Austen D. Givens, Nathan E. Busch & Alan D. Bersin, Going Global: The International Dimensions of U.S. Homeland Security Policy, 11 J. Strategic Security 1 (2018)

 [ISSN 2581-5369]

international cooperation in the extradition process. These agreements might not go far enough in addressing the subtleties of cybercrimes, which could leave situations with national security concerns with unclear legal requirements.

(D) Jurisdictional Conflicts and Forum Shopping

Jurisdictional conflicts often arise when multiple countries assert their right to prosecute a cybercriminal. This may result in a situation where the offender searches for a forum where the odds of them being extradited or receiving a light punishment are lower. To avoid prosecution, the cybercriminal may choose a jurisdiction with lax cybercrime laws or insufficient extradition procedures. Conflicts like these can have a big impact on national security. Countries with a stake in the outcome of the case might fight about who should have jurisdiction diplomatically or legally, which might stall or even end the extradition process.[10]

(E) Human Rights and Privacy Concerns

Human rights and privacy issues must be taken into account during the extradition process. The nation requesting extradition can have strict laws and rules governing data collecting,

cybercrime case evidence collection, and surveillance. These actions might not be consistent with the requesting nation's standards for privacy and human rights. Finding a balance between pursuing cybercriminals and upholding individuals' rights becomes a difficult task in cases involving national security consequences. If the seeking country's investigative techniques infringe the accused's rights, the requested country may decline extradition.[11]

(F) Political Considerations and Diplomatic Relations

Political factors and diplomatic ties frequently come into play in extradition cases involving cybercrime. People who are seen as politically sensitive or who might have connections to the government might make other countries reluctant to extradite them. This hesitation may lead to drawn-out discussions and disagreements, which would make the case's jurisdictional issues even more challenging. The outcome of the extradition may also be influenced by political factors. Even if the cybercriminal's acts have an impact on the seeking country's national security, a government may decline extradition due to diplomatic or geopolitical issues. In the case of Meng Wanzhou, the CFO of Huawei Technologies, was arrested in Canada at the request of the U.S. government. She faced extradition to the U.S. on charges of bank fraud and

[10]Enver Bucaj, The Need for Regulation of Cyber Terrorism Phenomena in Line with Principles of International Criminal Law, 2017 ACTA U. DANUBIUS JUR. 140 (2017).
[11] John Dugard & Christine Van den Wyngaert, Reconciling Extradition with Human Rights, 92 AM. J. INT'L L. 187 (1998)

conspiracy to commit wire fraud, related to alleged violations of U.S. sanctions against Iran. This case involved extradition challenges arising from the intersection of U.S. sanctions, trade issues, and national security concerns. The U.S. argued that Meng's actions had implications for national security, while Canada faced diplomatic pressure from China, where Meng is a prominent figure. Meng Wanzhou's extradition proceedings were ongoing as of the last update, and the case continued to have diplomatic and legal implications. It underscored the complex interplay of trade, national security, and legal jurisdiction in extradition cases. Julian Assange, the founder of WikiLeaks, faced extradition from the U.K. to the U.S. on charges related to the publication of classified documents. The U.S. argued that his actions compromised national security. This case raised questions about whether the act of publishing leaked documents by a non-U.S. citizen on a non-U.S. server constituted a crime under U.S. law. It also involved freedom of the press considerations, as Assange's defense argued that the charges were politically motivated. The extradition decision was denied by a U.K. court on the grounds of Assange's mental health and the potential for oppressive conditions in U.S. prisons. The case highlighted the legal complexities of extraditing individuals involved in cyber-related activities with perceived national security implications.[12]

IV. CONCLUSION

The digital age has ushered in an unprecedented era of national security challenges, largely attributed to the ever-evolving threat of cybercrimes. In this context, the practice of extradition, a legal process enabling the transfer of individuals between jurisdictions for trial or prosecution, has taken on a paramount role in addressing cybercrimes with direct implications for the security of nations and their citizens. This study delves into the intricate landscape of extradition in the digital age, with a specific focus on cybercrime cases entailing national security concerns. A central theme that emerges from this exploration is the critical significance of harmonizing legal frameworks. In the realm of cybercrimes, which recognize no borders, actions that may be deemed criminal in one country might not be recognized as such in another. Dual criminality requirements, which necessitate that an alleged offense be a crime in both the requesting and requested countries, assume a pivotal role in the extradition process. The alignment of legal definitions and standards is paramount to prevent cybercriminals from evading justice simply by crossing borders. Nonetheless, the road to harmonization is fraught with challenges. Divergent legal frameworks, jurisdictional conflicts, and the absence of a comprehensive global treaty on cybercrime contribute to the complexity of extradition in this domain. The cases of

[12] Manuel R. García-Mora, The Nature of Political Offenses: A Knotty Problem of Extradition Law, 48 Va. L. Rev. 1226 (1962)

 [ISSN 2581-5369]

individuals such as Gary McKinnon, Alexei Burkov, Julian Assange, and Meng Wanzhou exemplify the intricacies of international extradition when confronted with cybercrimes intertwined with national security interests. Beyond legal considerations, the study also delves into the diplomatic, political, and human rights dimensions of cybercrime extradition. These cases often intersect with diplomatic relations, geopolitics, and questions of human rights and privacy. Striking a balance between national security imperatives and individual rights presents a delicate challenge that extradition processes must skillfully navigate. Moreover, the study underscores the critical role of international cooperation in addressing the jurisdictional challenges intrinsic to cybercrime extradition. In the face of cyber threats that pay no heed to national borders, no nation can effectively combat these challenges in isolation. Countries must come together to streamline extradition processes, harmonize legal standards, and develop guidelines for determining jurisdiction. Effective international cooperation becomes the cornerstone of success in this domain. As our study concludes, it becomes abundantly clear that the extradition landscape is rapidly evolving, mirroring the dynamic nature of cybercrimes and national security concerns in the digital age. The digital era brings both opportunities and challenges, necessitating that the practice of extradition continually adapts and innovates to effectively address these evolving complexities. In this ever-changing landscape, the development of best practices and model approaches assumes utmost importance. By identifying and implementing these practices, nations can mitigate jurisdictional difficulties, streamline extradition processes, and ensure that justice prevails, even in the face of cyber threats that recognize no boundaries.

*****

 [ISSN 2581-5369]