STUDIA IURIS

Jogtudományi Tanulmányok / Journal of Legal Studies

2024. I. évfolyam 4. szám

Károli Gáspár Református Egyetem
Állam- és Jogtudományi Doktori Iskola

A folyóirat a Károli Gáspár Református Egyetem Állam- és Jogtudományi Doktori Iskolájának a közleménye. A szerkesztőség célja, hogy fiatal kutatók számára színvonalas tanulmányaik megjelentetése céljából méltó fórumot biztosítson.
A folyóirat közlésre befogad tanulmányokat hazai és külföldi szerzőktől – magyar, angol és német nyelven. A tudományos tanulmányok mellett kritikus, önálló véleményeket is tartalmazó könyvismertetések és beszámolók is helyet kapnak a lapban.
A beérkezett tanulmányokat két bíráló lektorálja szakmailag. Az idegen nyelvű tanulmányokat anyanyelvi lektor is javítja, nyelvtani és stilisztikai szempontból.
A folyóirat online verziója szabadon letölthető (open access).

Kiadó: Károli Gáspár Református Egyetem Állam- és Jogtudományi Doktori Iskola
Székhely: 1042 Budapest, Viola utca 2-4
Felelős Kiadó: Tóth J. Zoltán

A tipográfia és a nyomdai előkészítés Csernák Krisztina (L'Harmattan) munkája
A nyomdai munkákat a Robinco Kft. végezte, felelős vezető Gembela Zsolt

Honlap: https://ajk.kre.hu/index.php/jdi-kezdolap.html
E-mail: doktori.ajk@kre.hu
ISSN 3057-9058 (Print)
ISSN 3057-9392 (Online)
URL: KRE ÁJK - Studia Iuris
https://ajk.kre.hu/index.php/kiadvanyok/studia-iuris.html

PROSECUTION AND CONTROL OF CYBERCRIME IN RWANDA. LEGAL STRATEGIES AND ENFORCEMENT PRACTICES

Francois Regis Nshimiyimana[1]

ABSZTRAKT ■ Ez a tanulmány Ruanda jogi stratégiáit és bűnüldözési mechanizmusait vizsgálja a kibertámadások növekvő kihívásának kezelésére. Ruanda jogi keretrendszerét és bűnüldözési képességeit próbára teszik a fejlődő digitális fenyegetések, amelyek rámutatnak az eredményes büntetőeljárás és bűnmegelőzés hiányosságaira. A tanulmány kísérletet tesz a hatályos jogszabályok elemzésére, a bűnüldöző hatóságok által tapasztalt gyakorlati kihívások értékelésére, valamint a fejlesztést elősegítő javaslatok megfogalmazására. Összehasonlító jogi elemzések, esettanulmányok, illetve jogi szakemberekkel és bűnüldöző szervekkel folytatott interjúk révén jelen tanulmány célja, hogy értékelje a jelenlegi gyakorlatok hatékonyságát, és reformokat javasoljon Ruanda kiberbűnözés elleni küzdelemre irányuló erőfeszítéseinek javítására.

ABSTRACT ■ This paper investigates Rwanda's legal strategies and enforcement mechanisms to address the growing challenge of cybercrime. Rwanda's legal framework and law enforcement capabilities are tested as digital threats evolve, revealing effective prosecution and crime prevention gaps. The study seeks to analyze the existing legal provisions, assess enforcement agencies' practical challenges, and propose improvement measures. Through a comparative legal analysis, case studies, and interviews with legal professionals and law enforcement, this paper aims to evaluate the effectiveness of current practices and suggest reforms to enhance Rwanda's cybercrime control efforts.

Keywords: cybercrime, enforcement practices, cyber-security

1. Introduction

The emergence of digital technology in Rwanda has led to a notable rise in cybercrime rates, creating new obstacles for the nation's legal and enforcement frameworks[2]. Cybercrime, which ranges from sophisticated computer attacks to

[1] PhD student, Doctoral School of Law and Political Sciences, Károli Gáspár University of the Reformed Church in Hungary.

[2] William Maluleke: Exploring Cybercrime. An Emerging Phenomenon and Associated Challenges in Africa. *International Journal of Social Science Research and Review*, 6/2023, 223–243.

online fraud[3], is a hazard to persons and institutions, underscoring the necessity for efficient legal and regulatory responses.

1.1. Methodology

This study adopts a qualitative research approach, analyzing Rwanda's existing legal framework, relevant laws, and policies on cybercrime and electronic evidence. The research involves a review of academic literature, legal texts, and case law to identify gaps and challenges in the current system. A comparative analysis of international best practices will also be conducted to propose feasible solutions adapted to Rwanda's legal and technological context. The study aims to comprehensively understand the obstacles in utilizing electronic evidence in Rwanda's cybercrime cases and suggest practical recommendations for strengthening the legal framework to address these challenges effectively.

1.2. Background of the study

Digital technology has brought globalization to all walks of life and presents opportunities for communication and criminal activities. Cybercrime, or computer-oriented crime, is a severe threat threatening a person or a nation's security and financial health[4]. Cybercrimes involve computers and networks, and their issues include hacking, copyright infringement, mass surveillance, sex extortion, child pornography, and child grooming. Privacy problems arise when confidential information is intercepted or disclosed. Cybercrimes cross international borders and involve governmental and non-state actors, including espionage, financial theft, and other cross-border crimes. Understanding cybercrime phenomena, including challenges in prosecution and punishment, aims to assist countries in understanding the legal aspects of cyber security and

[3] Hamid Jahankhani – Ameer Al-Nemrat – Amin Hosseinian-Far: Cybercrime Classification and Characteristics. In: Babak Akhgar – Andrew Staniforth – Francesca Bosco (eds.): *Cyber Crime and Cyber Terrorism Investigator's Handbook*. Waltham, Syngress, 2014. 149–164.

[4] Fidelis Chukwunenye Obodoeze: "Cyber Crimes. Effects of Information Technology and Globalization on World Economy." Paper presented at the UNESCO World Philosophy Day Celebration Workshop, Nnamdi Azikiwe University, Awka, Nigeria, November 21-23, 2011. https://www.researchgate.net/publication/340333512_CYBER_CRIMES_EFFECTS_OF_INFORMATION_TECHNOLOGY_AND_GLOBALIZATION_ON_WORLD_ECONOMY.

harmonizing legal frameworks[5]. Challenges faced by prosecution and punishment actors include data loss, location loss, lack of legal framework, public and private partnerships, international cooperation, and evolving threat landscape[6].

1.3. General overview of cybercrime

Cybercrime is a global issue affecting electronic activities and involves crimes committed online using computers as tools or victims[7]. Classifying crimes into distinct groups is challenging due to the constantly evolving nature of cybercrime. The main target of cybercrimes depends on the computer and the person behind it. The unity of international, regional, and local governments is crucial in fighting against cybercrime and preventing danger caused by the Internet, networks, and computer systems. Cybercrime is a social label, not an established term within criminal law, and includes traditional and coming crimes conducted through computers and the Internet[8].

2. Forms of cybercrime activities

The prevalence of cybercrime activities in contemporary society has escalated, posing significant threats to governments, individuals, and businesses globally. With the rapid advancement of communication technologies, the number of cybercrime victims has surged, leading to various forms of harm such as harassment, financial losses, and considerable economic costs.9 While some of the impacts of cybercrime can be quantified in monetary terms, the broader consequences extend far beyond financial figures.[10]

5 Anja P. Jakobi: Non-State Actors All Around. The Governance of Cybercrime. In: Anja P. Jakobi – Klaus Dieter Wolf: *The Transnational Governance of Violence and Crime. Non-State Actors in Security*. London, Palgrave Macmillan, 2013. 129–148.

6 Cameron Scott Doran Brown: Investigating and Prosecuting Cyber Crime. Forensic Dependencies and Barriers to Justice. *International Journal of Cyber Criminology*, 1/2015, 55–119. 55. Available at: https://cybercrimejournal.com/pdf/Brown2015vol9issue1.pdf.

7 Sumanjit Das – Tapaswini Nayak: Impact of Cyber Crime. Issues and Challenges. *International Journal of Engineering Sciences & Emerging Technologies*, 2/2013, 142–153. Available at: https://www.ijeset.com/media/0002/2N12-IJESET0602134A-v6-iss2-142-153.pdf.

8 Ibid.

9 Richard Anderson et al.: "Measuring the Changing Cost of Cybercrime". Paper presented at The 18th Annual Workshop on the Economics of Information Security (WEIS 2019), Boston, 2019. https://weis2019.econinfosec.org/program/agenda/.

10 Ibid.

– Intellectual property (IP) theft is a major form of cybercrime involving the unlawful appropriation of commercial trademarks, patents, and copyrighted works such as music, movies, and books.[11] Cybercriminals use advanced technological means to steal vast amounts of copyrighted material, severely impacting the businesses or individuals victimized by such acts. Online piracy is a widespread form of IP theft, targeting consumers seeking discounted yet genuine products.[12]

– Hacking refers to unauthorized access to computer systems and networks, typically by individuals possessing specialized knowledge in coding or programming.[13] These cybercriminals exploit vulnerabilities to steal sensitive data or engage in illicit activities on behalf of others. Hackers often manipulate system controls or install malware to gain entry into target networks and commit further cybercrimes.[14]

– Child grooming is another harmful activity that exploits the internet to facilitate illegal businesses, including child prostitution and the production of child pornography.[15] Grooming typically involves building an emotional connection with a minor to reduce their inhibitions and manipulate them into abusive situations.[16] This form of exploitation is often perpetrated by adults with a sexual attraction to children.

– Identity theft and the stealing of sensitive data occur when cybercriminals successfully acquire personally identifiable information (PII). This information is often used for financial gain or to inflict damage on the victim.[17] Identity theft can involve activities such as unauthorized credit card transactions, online purchases, or renting property, all facilitated through illicit access to an individual's personal data.

– Cyber-stalking is a growing concern, wherein offenders use digital communication methods such as email to harass or threaten their victims. Unlike offline stalking, which involves physical proximity, cyber-stalking can be especially insidious, as it allows the stalker to remain anonymous and unseen while

11 David S. Wall – Majid Yar: Intellectual Property Crime and the Internet. Cyber-Piracy and 'Stealing' Information Intangibles. In: Yvonne Jewkes – Majid Yar (eds.): *Handbook of Internet Crime*. 2nd ed., Oxford, Routledge, 2011. 230-255.

12 Ibid.

13 Robert J. Sciglimpaglia, Jr.: Computer Hacking. A Global Offense. *Pace Yearbook of International Law*,1/1991, 199–266. 199. https://digitalcommons.pace.edu/pilr/vol3/iss1/.

14 Ibid.

15 Kim-Kwang Raymond Choo: *Online Child Grooming. A Literature Review on the Misuse of Social Networking Sites for Grooming Children for Sexual Offences*. Canberra, Australian Institute of Criminology, 2009. https://www.aic.gov.au/sites/default/files/2020-05/rpp103.pdf.

16 Ibid.

17 Clapper v. Amnesty International USA, 568 U.S. 398, 133 S. Ct. 1138, 185 L. Ed. 2d 264 (2013).

causing significant emotional distress.[18] This form of harassment often leads to victims fearing for their safety, with stalkers engaging in repeated and threatening behaviors.[19]

– Computer and internet fraud involves using computer systems to engage in deceptive practices that mislead others into making decisions that lead to financial loss.[20] Fraudsters may alter input data, manipulate stored information, or install malicious software to facilitate crimes.[21] For example, cybercriminals may rewrite software codes and infiltrate banking systems, enabling unauthorized transactions using stolen user credentials.

– Computer malware, including viruses and worms, is a form of malicious software designed to damage or disrupt computer systems. Malware is often spread through the internet, particularly via email attachments or downloadable files , and can cause significant harm by corrupting data, deleting files, or rendering systems inoperable.[22] Cybercriminals use malware to exploit vulnerabilities in computer systems, enabling them to carry out further malicious actions or steal sensitive information.[23] The widespread nature of these cybercrimes underscores the urgent need for robust cybersecurity measures and international cooperation to combat these threats.

3. The legal framework for addressing Cybercrimes in Rwandan legislation

Rwanda has developed a robust legal framework to combat cybercrimes, demonstrating its commitment to improving cybersecurity and safeguarding its citizens in the digital era. Legislation that tackles a wide range of cyber offenses is necessary because, as technology advances, so do the tactics used by hackers. The

[18] Michael Pittaro: Cyberstalking. An Analysis of Online Harassment and Intimidation. *International Journal of Cyber Criminology*, 2/2007, 180–197.

[19] John Reid Meloy: Stalking. An Old Behavior, A New Crime. *Psychiatric Clinics of North America*, 1/1999, 85–99. https://www.sciencedirect.com/science/article/abs/pii/S0193953X05700617.

[20] Samuel W. Buell: What Is Securities Fraud. *Duke Law Journal*, 3/2011, 511–581. 511.

[21] John Aycock: *Computer Viruses and Malware.* New York, Springer Science & Business Media, 2006. 1-8.

[22] Thomas M. Chen – Jean-Marc Robert: The Evolution of Viruses and Worms. In: William W.S. Chen (ed.): *Statistical Methods in Computer Security*. Boca Raton, CRC Press, 2004. 289-310. https://www.taylorfrancis.com/chapters/edit/10.1201/9781420030884-19/evolution-viruses-worms-thomas-chen-jean-marc-robert.

[23] Ibid.

Rwandan government has realized how critical it is to enact laws and rules that discourage cybercrime and offer channels for victim assistance and prosecution.

3.1. Law nº68/2018 of 30/08/2018 determining offences and penalties in general

According to the above law, which governs general principles governing offenses and penalties, article 160 regarding the Collection of individuals' personal information in computers states that "Any person who, in bad faith, records, collects an individual's personal information or who archives or uses other ways of keeping the personal information in computers and other specialized equipment in a manner that is likely to adversely affect the individual's honor or his/her privacy, commits an offense.[24] Upon conviction, he/she is liable to imprisonment for a term of not less than six (6) months and not more than one (1) year and a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than two million Rwandan francs (FRW 2,000,000)".[25] Acts referred to in Paragraph One of this article performed professionally or in the context of one's duty and legally recognized do not qualify as an offense.

3.2. Law n°24/2016 of 18/06/2016 governing information and communication technologies

This Law establishes a framework for Information and Communication Technologies (ICT) policy and regulation. Article 198, regarding access to a computer system with the intent to commit an offense, provides that "any person who causes a computer system to perform any function to secure access to any program or data held in any computer system with the intent to commit an offense is punished under the provisions of the penal code".[26] Any individual who, through any means, knowingly gains unauthorized access to a computer system to obtain, either directly or indirectly, any computer service, function, or data within the system, commits an offense. This is punishable by the provisions of the Penal Code. However, a person shall not be guilty of an offense if they

[24] Article 160 of Law n°68/2018 of 30/08/2018 determining offences and penalties in general, Officicial Gazette no special of 27/09/2018.

[25] Ibid.

[26] Article 198 of Law n°24/2016 of 18/06/2016 governing information and communication technologies, Official Gazette n°26 of 27/06/2016.

have obtained consent from the individual who sent the data and the intended recipient or is acting within the bounds of any statutory authority.[27]

In addition, any person knowingly engaging in activities that result in the unauthorized modification of data held within a computer system is committing an offense. This act is punishable under the relevant provisions of the penal code.[28] Furthermore, anyone without lawful authority or excuse who performs an act that directly or indirectly causes degradation, failure, interruption, or obstruction of a computer system's operation or denies access to or damages any program or data stored within the system is guilty of an offense. This, too, is punishable under the provisions of the Penal Code.[29]

The unlawful possession of computer systems, devices, and data constitutes a crime. A person who knowingly manufactures, sells, procures, imports, distributes, or otherwise makes available a computer system or any device while possessing data or programs intending to use them or enable others to commit an offense personally is guilty of an offense. This is punishable by the penal code.[30]

Similarly, any individual who, by means of a computer or electronic device, commits fraud or facilitates or causes forgery is committing an offense. This is punishable under the relevant provisions of the penal code.[31]

Additionally, the disclosure of passwords or access codes constitutes a criminal offense if it is made knowingly and to obtain wrongful gain or for an unlawful purpose and if it is likely to cause harm to another individual. According to the penal code's provisions, a person guilty of this offense will face punishment.[32] Finally, any individual who knowingly or willfully publishes or transmits indecent information in electronic form or causes such information to be published commits an offense, punishable under the relevant provisions of the penal code.

3.3. Law nº18/2010 of 12/05/2010 relating to electronic messages, electronic signatures, and electronic transactions

To create a thorough legal framework that encourages and governs the use of electronic communications and digital transactions in Rwanda, Law No. 18/2010 of 12/05/2010 was passed. This law deals with electronic messages,

27 Article 199, Law n°24/2016 of 18/06/2016, 24.
28 Article 200, Law n°24/2016 of 18/06/2016, 23.
29 Article 201, Law n°24/2016 of 18/06/2016, 23.
30 Article 202, Law n°24/2016 of 18/06/2016, 23.
31 Article 203, Law n°24/2016 of 18/06/2016, 23.
32 Article 204, Law n°24/2016 of 18/06/2016, 23.

electronic signatures, and electronic transactions. With the nation increasingly incorporating digital technologies into its economic and social structure, this law seeks to guarantee electronic transactions' legitimacy, security, and dependability. It creates explicit rules for digital signatures, electronic messaging, and general online business conduct, which promotes confidence and helps expand digital services and e-commerce while guarding against fraud and other online hazards.

3.3.1. Unauthorized access to computer data

Access by a person to a computer system is unauthorized where the person is not entitled to control and access the computer system; does not have consent to access by him/her of the kind in question from any person who is so entitled[33]. Any person who causes a computer system to perform a function, knowing that the access he/she intends to secure is unauthorized, shall commit an offense but shall not be liable under this provision where he/she is a person entitled to control the operation or use of the computer system and exercises such right in good faith. He/she has the express or implied consent of the person empowered to authorize him/her to have such access; he/she is acting in reliance of any statutory power arising under any enactment to obtain information or take possession of any document or other property.[34] For this section, any access not directed at any particular program or data, a program or data of any kind, or a program or data held in any specific computer system shall be immaterial.

3.3.2. Access to a computer system with the intent to commit offenses

Any person who causes a computer system to perform any function to secure access to any program or data held in any computer system, with intent to commit an offense under any law, commits an offense.[35]

3.3.3. Unauthorized access to and interception of computer service

Any person who, by any means, knowingly has unauthorized access to any computer system to obtain, directly or indirectly, any computer service or intercepts or causes to be intercepted, directly or indirectly, any function or any data within a computer system commits an offense.[36]

[33] Peter A. Winn: The guilty eye. Unauthorized access, trespass, and privacy. *The Business Lawyer*, 4/2007, 1395–1437.

[34] Article 58 of Law nº 18/2010 of 12/05/2010 relating to electronic messages, electronic signatures, and electronic transactions, *O.G n° 20 of 17/05/2010.*

[35] Ibid. Article 59.

[36] Ibid.

Institutional framework

The institutional framework for addressing cybercrime in Rwanda is designed to combat and prevent digital offenses through a coordinated approach involving various government agencies and regulatory bodies. Rwanda's National Cyber Security Authority (NCSA) plays a central role in safeguarding the country's digital infrastructure and implementing robust security measures. Established under Law No.26/2017 of May 31, 2017, the NCSA is mandated to protect national interests and combat the growing threat of cybercrime.[37] Its responsibilities include developing and executing comprehensive cybersecurity plans, conducting response exercises, and promoting industry best practices. The institutional framework of the NCSA also encompasses public awareness campaigns, threat intelligence, policy formulation, and incident response, all of which significantly enhance Rwanda's cyber defenses and security posture.[38]

According to Article 4 of Law No.26/2017 of May 31, 2017, the NCSA's mission focuses on building skills and capacities in cybersecurity to protect national integrity and security while supporting economic and social development. To achieve these goals, the NCSA advises the President of the Republic and other public and private institutions on strategies to protect Rwanda's interests in cyberspace. It conducts cyber intelligence to identify threats to national security, shares intelligence with appropriate organs, establishes guidelines based on national and international ICT security principles, and coordinates the implementation of a national ICT security policy and strategy.[39]

The NCSA is also responsible for developing plans to secure electronic operations, monitoring national ICT security programs, preventing cyber-attacks, and protecting critical ICT infrastructure. Additionally, the authority fosters national cybersecurity education, promotes research and industry development in the ICT sector, raises public awareness about cybersecurity, and collaborates with regional and international bodies to enhance ICT security. It supports national defense and security organs in cyberspace and performs other duties the President assigns.[40]

As stipulated by Law No.26/2017, the powers granted to the NCSA include setting guidelines for cyberspace protection and ICT security, conducting critical

37 Article 4 of law no 26/2017 of 31/05/2017 establishing the national cyber security authority and determining its mission, organization, and functioning, *O.G nº 27 of 03 July 2017.*

38 Ibid.

39 Roger Généreux Ishimwe: *Critical analysis on the impact of cybercrimes on intellectual property rights under Rwanda legal framework*. Kigali Independent University ULK, 2024. http://drepository.ulk.ac.rw:8080/xmlui/bitstream/handle/123456789/362/CRITICAL%20ANALYSIS%20ON%20THE%20IMPACT%20OF%20CYBERCRIMES.pdf?sequence=1&isAllowed=y.

40 Article 9 of law nº 26/2017 of 31/05/2017, 37.

infrastructure audits, investigating cyber threats, and collaborating with other organizations to combat cybercrime. Despite these efforts, Rwanda continues to face challenges in addressing cybercrime, including limited cooperation, inadequate electronic evidence gathering, and logistical hurdles that impede the immediate prosecution and punishment of cybercrimes.[41]

Complementing the NCSA's efforts, the Rwanda National Police (RNP) is pivotal in combating cybercrime. The RNP's strategic plan includes infrastructure development, enhancing equipment capabilities, improving communication systems, fostering police discipline, and developing anti-corruption strategies. With the increasing use of the internet and digital technologies, the RNP has focused on implementing systems to prevent and fight against cybercrimes in collaboration with various stakeholders.[42] Criminals increasingly exploit cyberspace to access personal information, steal intellectual property, and compromise sensitive government-held data for financial, political, or other malicious purposes, necessitating a proactive response by law enforcement.[43]

The Rwanda Investigation Bureau (RIB) is another critical institution in the fight against cybercrime. Established by Law No.12/2017 of April 7, 2017, the RIB operates under the Ministry of Justice and is tasked with investigating various crimes, including cybercrime. Its responsibilities include receiving complaints on criminal behavior, gathering and assembling criminal evidence for prosecution, and ensuring the prompt and efficient disposal of cases.[44] The RIB also provides forensic services, collects and disseminates information on criminals, and develops and implements strategies to enhance cybersecurity. These roles are vital in improving Rwanda's public order, safety, and crime prevention.

The obstacles hindering Rwanda's efforts to prosecute and suppress cybercrime.

While Rwanda has advanced significantly in technology and digital transformation, the country still has a long way to go before it can prosecute and suppress cybercrime. The emergence of cyber attacks presents a significant risk to the nation's economic growth and national security as it embraces digitalization.

41 John Gacinya: *Criminal Justice System as an Instrument of Internal Security. A Case Study of Rwanda. Master's thesis*. Institute of Diplomacy and International Studies (IDIS), University of Nairobi, 2013. 75-159. https://erepository.uonbi.ac.ke/bitstream/handle/11295/166148/Criminal%20Justice%20System%20as%20an%20Instrument%20of%20Internal%20Security%20a%20Case%20Study%20of%20Rwanda.pdf?sequence=1.

42 RNP, *Strategic plan 2013-2018*, Kigali Rwanda, 1-47, Available at: https://police.gov.rw/uploads/tx_download/RNP_A5_Booklet_FINAL_2015.pdf.

43 Ibid.

44 Law n°12/2017 of April 7, 2017 establishing the Rwanda Investigation Bureau and determining, its mission, powers, organization and functioning, Official gazette no Special of 20/04/2017.

It is essential to comprehend the barriers preventing Rwanda from progressing in this area to create tactics that effectively tackle cybercrime.

4. Challenges relating to the identification of cybercriminals

This paper believes that the anonymity of cybercriminals' identities continues to be one of the most significant barriers to international attempts to curb the spiraling incidence of cybercrimes. The anonymity of cybercriminals' identities remains a substantial barrier to international efforts to combat cybercrimes.[45] The global information system's freedom allows cybercriminals to hide their identities using various telecommunications gadgets, making it impossible to trace their online IP addresses. This makes it difficult to enforce laws, as they are not meant to work in a vacuum. Cybercrime laws were primarily enacted to apprehend and prosecute cybercriminals, making investigations and punishments difficult due to the lack of physical presence.

4.1. The challenges related to jurisdiction

Jurisdiction is a crucial issue in enforcing cybercrime laws, as it affects the power of a court to entertain an action, petition, or proceeding[46]. A court needs jurisdiction to try a case, as a defect in competence can render proceedings null and void. Jurisdiction is used in intra-territorial and extra-territorial situations, with extra-territorial jurisdiction being crucial when a court's judgment is sought to be enforced outside the forum. A jurisdictional challenge to enforcing cybercrime laws reduces the hurdle of anonymity, as a court cannot effectively try a cybercriminal if they are located in another country[47]. Extradition is a solution, but it faces challenges, including double criminality requirements and the absence of extradition treaties or mutual legal assistance treaties between the requesting and custody states.

[45] Zunaira Sattar et al.: "Challenges of Cybercrimes to Implementation of Legal Framework." Paper presented at the International Conference on Emerging Technologies, November 1, 2018. https://www.semanticscholar.org/paper/Challenges-of-Cybercrimes-to-Implementation-of-Sattar-.

[46] Emmanuel Ajayi: Challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems*, 1/2016, 1–12. https://www.researchgate.net/publication/307528405_Challenges_to_enforcement_of_cybercrimes_laws_and_policy.

[47] Idem.

4.2. The barriers relating to the processes of extradition of a suspect

Extradition is returning somebody accused of a crime to a different legal authority for trial or punishment[48]. Extradition has also been defined as the surrender by one state to another of a person accused of committing an offense in the latter[49]. A casual glance at the definition of extradition as above would ordinarily raise the hope that if a person is alleged to have committed a cybercrime in one jurisdiction and escapes to another country, all that needs to be done by the country where the cybercriminal is domiciled is expeditiously return the said criminal to the requesting country, to face trial, however, in practice, this is not so because of the principle of state independence and sovereignty earlier stated before now.[50] Under international law, no instrument obligates sovereign nations to return cybercriminals for trial automatically. In effect, countries where Cybercriminals are situated, for different reasons, more often than not refuse to extradite them, and this development presents an insurmountable challenge to the enforcement of cybercrime laws across the globe.

To address the lacuna created as a result of the lack of international law not making it mandatory to deport criminals, extradition treaties fill the void; thus, if there is a treaty between two states, criminals may be deported, and even at that, there are many exceptions to extradition processes. One of the biggest hurdles to the extradition of criminals to requesting states is the "unruly legal horse" called jurisdiction; countries often invoke jurisdiction to deny extradition[51], especially if the requested state has jurisdiction to try criminals who are nationals of the requested state; as such, the requesting state has no choice but to abide by that decision not to commence extradition.

[48] Craig R. Roecks: Extradition, Human Rights, and the Death Penalty. When Nations Must Refuse to Extradite a Person Charged with a Capital Crime. *California Western International Law Journal*, 1/1994, 189. https://heinonline.org/HOL/LandingPage?handle=hein.journals/calwi25&div=10&id=&page=.

[49] Ibid.

[50] M. Cherif Bassiouni: *The Sources and Content of International Criminal Law. A Theoretical Framework*. Leiden, Martinus Nijhoff Publishers, 1999. 353-356.

[51] Emmanuel O. C. Obidimma – Richard Onyekachi Ishiguzo: Cybercrime Investigation and Prosecution in Nigeria. The Critical Challenges. *African Journal Of Criminal Law And Jurisprudence*, 8/2023, 30–36. 30.

4.3. The challenge regarding the nature of evidence

The enforcement of cybercrime laws is hindered by the nature of the evidence available in prosecution custody and its admissibility in cybercriminals' trials[52]. Evidence can take various forms, including testimony, documentary, and tangible evidence. In criminal prosecution, it is crucial to prove the case beyond a reasonable doubt before a conviction can be obtained. However, the evidence available in cybercrime prosecution is often tenuous and needs more evidential value. Physical evidence is rare, and investigators rely on footprints on computers and internet traces, which have little evidential value and are costly to gather.

4.4. Lack of effective reporting and lack of data

Many countries have laws and policies against cybercrime, but enforcing them is challenging due to inadequate reporting and lack of cooperation between victims, stakeholders, and police. Reasons for reluctance include costs, reputation damage, lengthy investigations, and difficulty in diligent investigation. The lack of cooperation and the damage caused by cybercrimes can hinder global attention and appreciation of the menace. Addressing these issues is crucial for a more practical approach to cybercrime.

4.5. Cost, time, and efforts incurred in investigation and prosecution

The cost of using a scientific approach to solving crimes is significantly higher than traditional evidence gathering in terrestrial crimes, mainly due to the forensic evidence required for prosecuting cybercrimes.[53] This approach also demands high-tech equipment, specialized materials, and expertise to conduct investigations. In the context of business and social interactions, the rise of technology has had two main effects. On the one hand, it has brought numerous advantages, such as faster and more accurate information and communication, making the world feel like a global village. On the other hand, it has led to the rise

[52] Susan W. Brenner – Joseph J. Schwerha: Transnational Evidence Gathering and Local Prosecution of International Cybercrime. *Journal of Computer & Information Law*, 3/2002). 347.

[53] Mohamed Chawki et al.: *Cybercrime, Digital Forensics and Jurisdiction*. Springer, Cham, 2015. https://link.springer.com/book/10.1007/978-3-319-15150-2#publish-with-us.

of cybercrimes, often called the "dark side" of technology.[54] These crimes present a significant challenge for investigators and law enforcement agencies, as they must sift through vast amounts of information that require scientific analysis, such as decrypting files and breaking encrypted codes. Uncovering hidden or destroyed evidence often involves high costs and significant time and effort from expert resources that could otherwise be used more effectively in other areas.

4.6. Lack of adequate legislation and ineffectiveness where extant

Cybercrime law enforcement is hindered by inadequate legislation and ineffectiveness[55]. Out of 201 countries, only 79 have laws specifically for cybercrimes, with Western Europe being the majority[56]. This lack of laws gives cybercriminals a license to operate freely without fear. The absence of requisite laws is more prevalent in Africa, where only four countries have criminalized cybercrimes.[57] Even with existing legislation, these provisions are not severe enough to deter cybercriminals from their illegal acts[58]. Examples include Australia's Cybercrime Act 2001, Criminal Code Act 1995, and Telecommunications (Interception and Access) Act 1979.

4.7. Lack of enforcement mechanisms under international law

The paper argues that international law is not a law in practice due to its lack of enforcement mechanisms. It suggests that independence, sovereignty, and territorial bounds preserve state equality. However, the strength of nations is evident in their relations. Enforcement methods include sanctions, reciprocity, collective action, and shaming. The Budapest Convention on Cybercrime, a treaty, is an example. The non-binding nature of international law has stifled the enforcement of cybercrime laws, as states refuse to enforce provisions in their territory.

54 Richard A. Posner: *An Economic Approach to the Law of Evidence*. University of Chicago Law School, John M. Olin Law & Economics Working Paper No. 66. https://heinonline.org/HOL/LandingPage?handle=hein.journals/stflr51&div=55&id=&page=.

55 Ajayi 2016.

56 Ibid.

57 Ibid.

58 Christopher Hooper et al.: Cloud Computing and Its Implications for Cybercrime Investigations in Australia. *Computer Law & Security Review*, 2/2013, 152–163.

4.8. Weakly trained, poorly paid, and lack of protection for law enforcement agencies

This study believes that cybercriminals are crass opportunists always looking for avenues to make unlawful wealth or, in rare cases, wreak havoc on computer systems; they have been described as professional thieves and soldiers of fortune; above all, cybercriminals are experts in computers and cyberspace issues. Thus, the expertise of cyber criminals cannot be juxtaposed with law enforcement agencies, which are mere government officials who are ill-trained, poorly remunerated, and who offer their services without proper security and protection[59]. The preceding factors make efforts to investigate and enforce cybercrime laws puerile because cyber criminals are far ahead of law enforcement agencies regarding access to funds and the necessary acquisition of skills in computers and cyberspace-related issues.

4.9. Absence of one universal law governing cybercrimes

The only law explicitly dealing with international cybercrimes is the Budapest Convention, hampered by difficulties associated with international laws, an already copiously discussed issue.[60] This paper emphasizes the lack of a universal law governing cybercrimes, as they are borderless, transnational, and international crimes committed in cyberspace. Current laws and policies are fragmented due to issues such as lack of consensus on cybercrime types, definitions of criminal conduct, insufficient legal powers for investigation, lack of uniformity between national procedural laws, and absence of extradition and mutual legal assistance treaties. A universal law is needed to address these challenges.

5. Practical cases of cybercrime and electronic mail forgery that occurred in Rwanda

Cybercrime has emerged as a significant challenge in Rwanda's rapidly growing digital economy. The increasing reliance on technology in communication, business transactions, and public administration has created opportunities for cybercriminals to exploit vulnerabilities in electronic systems. Among the

[59] Ibid.
[60] Ibid.

various forms of cybercrime, electronic mail forgery is prevalent, manipulating email content, headers, or sender information to deceive recipients for financial, reputational, or other illicit gains. This section explores notable instances of cybercrime and electronic mail forgery in Rwanda, highlighting their modus operandi, legal implications, and the efforts undertaken by authorities to address these offenses. By examining these cases, the aim is to provide practical insights into the challenges of combating cybercrime and the critical role of electronic evidence in ensuring accountability and justice.

5.1. Case 1: Cyber fraud ring targeting Equity Bank

In 2020, Rwandan authorities dismantled a cybercrime syndicate attempting to infiltrate Equity Bank's systems. The group, comprising eight Kenyans, three Rwandans, and one Ugandan, sought unauthorized access to the bank's digital infrastructure to transfer funds illicitly. The Rwanda Investigation Bureau (RIB) apprehended the suspects before they could execute the heist, preventing potential financial losses and reinforcing the importance of robust cybersecurity measures in the banking sector.[61]

5.2. Case 2: Surge in cyber-fraud during COVID-19 lockdown

Between January and September 2020, Rwanda experienced a significant increase in cyber-fraud cases, with 141 incidents reported involving approximately RWF 371 million. The Rwanda Investigation Bureau (RIB) successfully recovered RWF 89 million and arrested several individuals connected to these crimes. This surge in cyber fraud, particularly during the COVID-19 lockdown, underscores the need for enhanced cybersecurity awareness and strengthened legal frameworks to combat electronic fraud effectively.[62]

[61] Rwanda Investigation Bureau, Cyber fraud scammers steal over RWF 280M in 2020. Online: https://cyber.gov.rw/updates/article/cyber-fraud-scammers-steal-over-rwf-280m-in-2020-1/.

[62] Ibid.

6. Effective Legal strategies for prosecuting and punishing cybercrime in Rwanda

This study examines various legal strategies as potential solutions to the abovementioned difficulties. Among those tactics are criminality, applying current laws, investigation, evidence gathering, prevention, and international collaboration.

6.1. Enforcement of the existing laws and conducting investigation

The United Nations code of conduct for law enforcement officials emphasizes the duty of law enforcement to serve the community and protect against illegal acts[63]. As cybercrime becomes more prevalent, law enforcement agencies must balance serving and protecting global crimes. Local police stations often transfer cases to specialized national-level leads, but electronic evidence is expected to revolutionize policing techniques. The capacity of police forces to investigate cybercrime varies between countries, with some having well-organized units and others needing more trained officers.

6.2. Increasing the power of investigation

Cybercrime evidence is typically electronic or digital, requiring a combination of traditional and new policing techniques. Law enforcement may use conventional methods, such as interviewing victims or undercover surveillance, but may also use computer-specific approaches[64]. Legal frameworks for cybercrime investigations require a clear scope of application and sufficient authority for data preservation and collection. Specialized procedural frameworks define concepts like computer data, data at rest, and data in transit and differentiate between data types like subscriber, traffic, and content data.

[63] Gerhard O. W. Mueller: The United Nations Draft Code of Conduct for Law Enforcement Officials. *Police Studies*, 2/1978.

[64] Kanae Kanki – Alexander Resch: Strengthening International Law Enforcement Cooperation. INTERPOL and Its Global Fight Against Economic and Financial Crime. In: Michala Meiselles – Nicholas Ryder – Arianna Visconti (eds.): *Corporate Criminal Liability and Sanctions*. Routledge, 2024. eBook, https://www.taylorfrancis.com/chapters/edit/10.4324/9781003324829-9/strengthening-international-law-enforcement-cooperation-kanae-kanki-alexander-resch.

6.3. Empowering Law Enforcement Capacity

This point presents information gathered on the capacity of law enforcement authorities to prevent and combat cybercrime. Institutional capacity in policing has several elements, including strategic and operational capabilities, personnel technical skills, and sufficiency of officers and resources. Another essential element of capacity is the degree of specialization. Crimes that require a specialized response typically present specific challenges in terms of offense definitions, the applicability of laws, or evidence gathering and analysis.[65] Cybercrime shows all of these characteristics, and a degree of law enforcement specialization is critical to an effective crime prevention and criminal justice response. Law enforcement specialization can occur at the organizational and personnel levels, often overlapping. While specialization will likely always be required in cybercrime and electronic evidence, it is also the case that as the world advances towards hyper-connectivity, all law enforcement officers will increasingly be expected to handle and collect electronic evidence routinely.

6.4. Increasing criminalization and respect for human rights

The increasing use of social media and user-generated internet content has resulted in regulatory responses from the government, including criminal law, and calls for respect for the right to freedom of expression[66]. International human rights law acts as a sword and a shield, requiring the criminalization of (limited) extreme forms of expression while protecting others. Some prohibitions on freedom of expression, including incitement to genocide, hatred constituting incitement to discrimination, hostility or violence, incitement to terrorism, and propaganda for war, are therefore required for states that are party to relevant international human rights instruments. The international human rights law both prescribes and prohibits criminalization in the area of cybercrime. Jurisprudence around freedom of speech is mainly developed in assisting countries to place boundaries around the criminalization of expression in areas as diverse as hate speech, incitement to terrorism, defamation, obscenity, and insult.

[65] Richard Mace: *Prosecution Organizations and the Network of Computer Crime Control. Doctoral dissertation*. 1999. AAT 9920188.

[66] Lorna Woods: User-generated content. Freedom of expression and the role of the media in a digital age. In: Merris Amos – Jackie Harrison – Lorna Woods (eds.): *Freedom of Expression and the Media*. Leiden, Martinus Nijhoff Publishers, 2012. 141-159.

A state that is a party to human rights treaties must establish criminal law and systems sufficient to deter and respond to attacks on individuals; it must not deny individual rights by criminalizing particular conduct.[67] In undertaking this assessment, the criminal law provision must be assessed on a 'right-by-right' basis to test whether its contents infringe a range of individual rights, such as the right not to be subjected to arbitrary or unlawful interference with privacy, family, home or correspondence[68], the right to freedom of thought, conscience, and religion[69], or the right of peaceful assembly.[70] International human rights law applies equally to the criminalization of cybercrime. Cybercrime represents a broad area of criminalization, including acts against the confidentiality, integrity, and availability of computer data or systems, computer-related acts for personal or financial gain or harm, and computer content-related acts. Some criminal provisions may engage international human rights law obligations more than others.

6.5. Collecting and analyzing electronic evidence through digital forensics

This point considers the criminal justice process in cybercrime cases, starting from the need to identify, collect, and analyze electronic evidence through digital forensics. It examines the admissibility and use of electronic evidence in criminal trials and demonstrates how prosecutorial challenges can impact criminal justice system performance. It links law enforcement and criminal justice capacity needs with a view of delivered and required technical assistance activities.

6.6. Increasing criminal justice capacity

Cybercrime and electronic evidence-based investigations require specialization within law enforcement; the prosecution and adjudication of cybercrime cases

67 United Nations Commission on Narcotic Drugs and Crime Prevention and Criminal Justice, 2010. Drug control crime prevention and criminal justice: A Human Rights perspective. Note by the Executive Director. E/CN.7/2010/CRP.6 – E/CN.15/2010/CRP.1. 3 March 2010.

68 ICCPR, Art. 17: International Covenant on Civil and Political Rights, Article 17 – Protection against arbitrary interference with privacy, family, home, or correspondence, and protection of honor and reputation.

69 Ibid. Art. 18.

70 Ibid. Art. 21.

also call for specialization within the criminal justice system.[71] Such specialization requires personnel who understand computing and the Internet, know cybercrime legislative frameworks, and can present and understand electronic evidence in court.

6.7. Raising cybercrime awareness

Surveys, including in developing countries, demonstrate that most individual internet users now take basic security precautions. All stakeholders highlight the continued importance of public awareness-raising campaigns, including those covering emerging threats and those targeted at specific audiences, such as children.[72] User education is most effective when combined with systems that help users securely achieve their goals.

The United Nations Guidelines for the Prevention of Crime highlight the importance of public education and awareness.[73] Increased public awareness of victimization risks and protective measures is an important strategy in preventing any crime.[74] In addition to governments, during information gathering for the Study, private sector organizations also highlighted the importance of public and corporate awareness regarding cybercrime.

6.8. International cooperation with states

A transnational dimension to a cybercrime offense arises where an element or substantial effect of the offense is in another territory or part of the modus operandi of the offense is in another territory[75]. This engages issues of sovereignty, jurisdiction, transnational investigations, extraterritorial evidence, and international cooperation requirements. Cybercrime is not the first 'new'

[71] Council of Europe, Guideline for Prosecutors and Law Enforcement in Cybercrime Investigations in Turkey, prepared by Dr. Michael Jameison and Kemal Kumkumoglu, October 2023. Available at: https://rm.coe.int/guide-on-fight-against-cybercrime/1680ae6859.

[72] Breana C. Smith – Don Ly – Mary Schmiedel: Intellectual Property Crimes. *American Criminal Law Review*, 2/2006).

[73] United Nations Guidelines for the Prevention of Crime. 2002. Economic and Security Council resolution 2002/13, Annex. Para.6 and 25.

[74] UNODC, *Handbook on the crime prevention guidelines. Making them work*. United Nations, New York, 2010. 65.

[75] UNODC, *Transnational Cybercrime: A Global Perspective*, 2020. https://www.unodc.org/documents/organized-crime/Transnational_Cybercrime_A_Global_Perspective.pdf.

crime to demand a global response. Over the past decades, global action has been required to address challenges such as illicit drug trafficking and transnational organized crime, including through the development of international agreements. Nonetheless, it has become a truism that cybercrime today presents unique international cooperation challenges.

Rules of customary public international law protect states' sovereign equality. These include states' obligations not to interfere in the internal and external affairs of other states in any form or for any reason whatsoever.[76] Law enforcement and criminal justice matters fall within the exclusive domain of the sovereign state because criminal jurisdiction has traditionally been linked to geographical territory. States must, therefore, refrain from exerting pressure on other states regarding the behavior of specific national bodies, such as law enforcement agencies or the judiciary. Persons may not be arrested, a summons may not be served, and police or tax investigations may not be mounted on the territory of another state except under the terms of a treaty or other consent given.[77] Of course, not all crimes occur neatly within the territorial jurisdiction. Where this is the case, international law has recognized several bases of extra-territorial jurisdiction in criminal matters.[78] The international cooperation of states may include cooperation through bilateral and multilateral agreements, cooperation through Jurisdiction, cooperation for gathering electronic evidence, and collaboration on extra-territorial evidence from service providers.

7. Conclusion

Cybercrime, as a phenomenon that involves the use of computers and networks to commit or facilitate offenses, presents multifaceted challenges that threaten individual, organizational, and national security. These crimes, ranging from hacking and copyright infringement to child exploitation and financial fraud, exploit modern telecommunication networks and mobile technologies to cause harm. While the global community has taken strides to address cybercrime,

[76] Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States, annex to GA resolution A/RES/20/2131 (XX), 21 December 1965. Please also refer to the Corfu Channel case, ICJ Reports 1949, 35, the Military and Paramilitary Activities case, ICJ Reports 1986, 202, and the Nicaragua case, ICJ Reports 1986, 14, 109-10.

[77] Ian Brownlie: *Principles of Public International Law*. 6th ed. Oxford, Oxford University Press, 2003. 306.

[78] Hans-Heinrich Jeschek – Thomas Weigend: *Lehrbuch des Strafrechts. Allgemeiner Teil.* 5th ed. Berlin, Duncker & Humblot, 1996. 167 et seq.

significant gaps in effective prosecution, enforcement, and prevention remain pervasive. One of the critical barriers to progress lies in the disproportionate focus on nation-state actors and their implications for national security. While these concerns are valid, this approach overshadows the increasing prevalence of financially motivated cybercrime, which affects most individuals and institutions globally. The current enforcement gap reflects insufficient attention to transnational organized cybercrime and the lack of comprehensive mechanisms for attribution, legal enforcement, and international cooperation.

Rwanda's case is emblematic of the broader challenges nations face navigating the complexities of cybercrime control in an evolving digital landscape. This paper has examined Rwanda's legal framework and enforcement mechanisms, uncovering gaps in prosecutorial effectiveness and institutional capacities. The findings underscore the urgent need for reform to strengthen legal provisions, enhance investigative tools, and foster capacity-building initiatives for law enforcement agencies.

To reverse the enforcement gap, a unified approach that aligns national and international stakeholders on shared priorities is required. This includes establishing frameworks to tackle transnational cybercrime networks, eliminating safe havens for perpetrators, and fostering collaboration between governments, corporations, and international organizations. Investing in technological capabilities, harmonizing legal standards with international conventions, and fostering judicial and law enforcement expertise will be critical steps forward for Rwanda and other nations.

As technology evolves, emerging threats will further test the resilience of national and global cybercrime control mechanisms. Rwanda's experience highlights the importance of proactive legal and institutional responses to prevent cybercrime from reaching epidemic proportions. By integrating lessons learned through comparative analysis and collaboration with international partners, Rwanda can position itself as a model for addressing cybercrime in developing contexts.

Addressing cybercrime requires a long-term vision emphasizing prevention, cooperation, and adaptability to technological advancements. The global community must embrace shared values and principles to reduce the enforcement gap and ensure the digital landscape remains secure for all. For Rwanda, leveraging its unique context and experiences can drive impactful reforms contributing to national security and regional and global cybersecurity resilience.

Bibliography

Richard Anderson et al.: "Measuring the Changing Cost of Cybercrime". Paper presented at The 18th Annual Workshop on the Economics of Information Security (WEIS 2019), Boston, 2019. https://weis2019.econinfosec.org/program/agenda/.

John Aycock: *Computer Viruses and Malware.* New York, Springer Science & Business Media, 2006.

M. Cherif Bassiouni: *The Sources and Content of International Criminal Law. A Theoretical Framework*. Leiden, Martinus Nijhoff Publishers, 1999.

Cameron Scott Doran Brown: Investigating and Prosecuting Cyber Crime. Forensic Dependencies and Barriers to Justice. *International Journal of Cyber Criminology*, 1/2015, 55–119. Available at: https://cybercrimejournal.com/pdf/Brown2015vol9issue1.pdf.

Samuel W. Buell: What Is Securities Fraud. *Duke Law Journal*, 3/2011, 511–581.

Thomas M. Chen – Jean-Marc Robert: The Evolution of Viruses and Worms. In: William W.S. Chen (ed.): *Statistical Methods in Computer Security*. Boca Raton, CRC Press, 2004. 289-310. https://www.taylorfrancis.com/chapters/edit/10.1201/9781420030884-19/evolution-viruses-worms-thomas-chen-jean-marc-robert.

Christopher, Rocks. „Extradition, Human Rights, and the Death Penalty: When Nations Must Refuse to Extradite a Person Charged with a Capital Crime." California Western International Law Journal, 25 (1994): 189. https://heinonline.org/HOL/LandingPage?handle=hein.journals/calwi25&div=10&id=&page=

Craig R. Roecks: Extradition, Human Rights, and the Death Penalty. When Nations Must Refuse to Extradite a Person Charged with a Capital Crime. *California Western International Law Journal*, 1/1994. https://heinonline.org/HOL/LandingPage?handle=hein.journals/calwi25&div=10&id=&page=.

Choo, Kim-Kwang Raymond. „Online Child Grooming: A Literature Review on the Misuse of Social Networking Sites for Grooming Children for Sexual Offences." Australian Institute of Criminology (2009). https://www.aic.gov.au/sites/default/files/2020-05/rpp103.pdf.

Kim-Kwang Raymond Choo: *Online Child Grooming. A Literature Review on the Misuse of Social Networking Sites for Grooming Children for Sexual Offences*. Canberra, Australian Institute of Criminology, 2009. https://www.aic.gov.au/sites/default/files/2020-05/rpp103.pdf.

Sumanjit Das – Tapaswini Nayak: Impact of Cyber Crime. Issues and Challenges. *International Journal of Engineering Sciences & Emerging Technologies*, 2/2013, 142–153. Available at: https://www.ijeset.com/media/0002/2N12-IJESET0602134A-v6-iss2-142-153.pdf.

Emmanuel Ajayi: Challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems*, 1/2016, 1–12. https://www.researchgate.net/

publication/307528405_Challenges_to_enforcement_of_cybercrimes_laws_and_policy.

John Gacinya: *Criminal Justice System as an Instrument of Internal Security. A Case Study of Rwanda. Master's thesis*. Institute of Diplomacy and International Studies (IDIS), University of Nairobi, 2013. 75-159. https://erepository.uonbi.ac.ke/bitstream/handle/11295/166148/Criminal%20Justice%20System%20as%20an%20Instrument%20of%20Internal%20Security%20a%20Case%20Study%20of%20Rwanda.pdf?sequence=1.

Roger Généreux Ishimwe: *Critical analysis on the impact of cybercrimes on intellectual property rights under Rwanda legal framework*. Kigali Independent University ULK, 2024. http://drepository.ulk.ac.rw:8080/xmlui/bitstream/handle/123456789/362/CRITICAL%20ANALYSIS%20ON%20THE%20IMPACT%20OF%20CYBERCRIMES.pdf?sequence=1&isAllowed=y.

Hamid Jahankhani – Ameer Al-Nemrat – Amin Hosseinian-Far: Cybercrime Classification and Characteristics. In: Babak Akhgar – Andrew Staniforth – Francesca Bosco (eds.): *Cyber Crime and Cyber Terrorism Investigator's Handbook*. Waltham, Syngress, 2014. 149–164.

Anja P. Jakobi: Non-State Actors All Around. The Governance of Cybercrime. In: Anja P. Jakobi – Klaus Dieter Wolf: *The Transnational Governance of Violence and Crime. Non-State Actors in Security*. London, Palgrave Macmillan, 2013. 129–148.

Kanae Kanki – Alexander Resch: Strengthening International Law Enforcement Cooperation. INTERPOL and Its Global Fight Against Economic and Financial Crime. In: Michala Meiselles – Nicholas Ryder – Arianna Visconti (eds.): *Corporate Criminal Liability and Sanctions*. Routledge, 2024. eBook, https://www.taylorfrancis.com/chapters/edit/10.4324/9781003324829-9/strengthening-international-law-enforcement-cooperation-kanae-kanki-alexander-resch.

Mace, Richard. Prosecution Organizations and the Network of Computer Crime Control. Doctoral dissertation, 1999.

Richard Mace: *Prosecution Organizations and the Network of Computer Crime Control. Doctoral dissertation*. 1999. AAT 9920188.

William Maluleke: Exploring Cybercrime. An Emerging Phenomenon and Associated Challenges in Africa. *International Journal of Social Science Research and Review*, 6/2023, 223–243.

John Reid Meloy: Stalking. An Old Behavior, A New Crime. *Psychiatric Clinics of North America*, 1/1999, 85–99. https://www.sciencedirect.com/science/article/abs/pii/S0193953X05700617.

Fidelis Chukwunenye Obodoeze: "Cyber Crimes. Effects of Information Technology and Globalization on World Economy." Paper presented at the UNESCO World Philosophy Day Celebration Workshop, Nnamdi Azikiwe University, Awka, Nigeria,

November 21-23, 2011. https://www.researchgate.net/publication/340333512_CYBER_CRIMES_EFFECTS_OF_INFORMATION_TECHNOLOGY_AND_GLOBALIZATION_ON_WORLD_ECONOMY.

Emmanuel O. C. Obidimma – Richard Onyekachi Ishiguzo: Cybercrime Investigation and Prosecution in Nigeria. The Critical Challenges. *African Journal Of Criminal Law And Jurisprudence*, 8/2023, 30–36.

Michael Pittaro: Cyberstalking. An Analysis of Online Harassment and Intimidation. *International Journal of Cyber Criminology*, 2/2007, 180–197.

Richard A. Posner: *An Economic Approach to the Law of Evidence*. University of Chicago Law School, John M. Olin Law & Economics Working Paper No. 66. https://heinonline.org/HOL/LandingPage?handle=hein.journals/stflr51&div=55&id=&page=.

Robert J. Sciglimpaglia, Jr.: Computer Hacking. A Global Offense. *Pace Yearbook of International Law*, 1/1991, 199–266. https://digitalcommons.pace.edu/pilr/vol3/iss1/.

Zunaira Sattar et al.: "Challenges of Cybercrimes to Implementation of Legal Framework." Paper presented at the International Conference on Emerging Technologies, November 1, 2018. https://www.semanticscholar.org/paper/Challenges-of-Cybercrimes-to-Implementation-of-Sattar-.

David S. Wall – Majid Yar: Intellectual Property Crime and the Internet. Cyber-Piracy and 'Stealing' Information Intangibles. In: Yvonne Jewkes – Majid Yar (eds.): *Handbook of Internet Crime*. 2nd ed., Oxford, Routledge, 2011. 230-255.

Peter A. Winn: The guilty eye. Unauthorized access, trespass, and privacy. *The Business Lawyer*, 4/2007, 1395–1437.