INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Facultyof Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

www.ijlra.com
Volume 2 Issue 7 | Jan 2024
ISSN: 2582-6433

CYBER PIRACY AND IT'S IMPACT ON GLOBAL SECURITY

AUTHORED BY - SHIVKANT SINHA
NEW LAW COLLEGE
BBALL.B (3RD YEAR)
DIVISON- C
ROLL NO- 27

ABSTRACT

The multifaceted nature of cyber piracy necessitates a comprehensive exploration of its intricacies, ranging from the methods employed by malicious actors to the motivations that drive their activities. This research paper aims to delve deep into this intricate phenomenon, shedding light on the evolving landscape of cyber piracy and its pervasive impact on individuals, businesses, and governments worldwide. To comprehend the complexity of cyber piracy, an in-depth analysis of the methods employed by cyber criminals is essential. Beyond the technical aspects, the paper will delve into the motivations that drive cyber piracy. Financial gain remains a significant motivator, but the landscape is also shaped by political and ideological motivations, cyber espionage, and hacktivism. By unravelling these motivations, the research seeks to provide insights into the underlying reasons behind cyber attacks, contributing to a more holistic understanding of the threat landscape. The far-reaching impact of cyber piracy extends to individuals who may fall victim to identity theft, businesses facing financial losses and operational disruptions, and governments dealing with national security threats. This research will systematically assess the consequences of cyber piracy on these different stakeholders, addressing issues such as financial losses, compromised personal data, reputational damage, business disruption, and national security vulnerabilities. Effectively combating cyber piracy requires an understanding of the challenges faced by cybersecurity professionals, law enforcement, and governments. The paper will explore challenges such as attribution difficulties, jurisdictional issues, the rapid evolution of attack tactics, and the lack of international cooperation. Identifying and acknowledging these challenges is crucial for developing targeted and effective countermeasures.

ISSN: 2582-6433

Keywords: - Cyber, Piracy, Pirates, Global, cyber security, Cyber warfare

INTRODUCTION

Cyber piracy, in the contemporary context, refers to the unauthorized and illicit activities conducted by individuals or groups in the digital realm with the intent to gain unauthorized access, control, or manipulate information systems, networks, and data for various purposes. This encompasses a wide range of malicious activities, including but not limited to hacking, data breaches, ransomware attacks, and other forms of cybercrime. The term is not limited to actions targeting a specific sector; rather, it encapsulates a broad spectrum of activities that exploit vulnerabilities in digital infrastructures. The scope of cyber piracy extends across various domains, impacting individuals, businesses, and governments alike. It is not confined to a particular geographic location or industry sector, making it a global challenge. As technology continues to advance, so do the methods employed by cyber pirates, necessitating a comprehensive understanding of the evolving nature of cyber threats. The evolution of cyber piracy is intrinsically tied to the rapid advancements in technology and the increasing interconnectedness of the digital world. Initially, cyber attacks were often opportunistic and unsophisticated, primarily driven by curiosity or a desire for notoriety[1]. However, over time, the motives behind cyber piracy have evolved to include financial gain, political motivations, espionage, and hacktivism. The methods employed by cyber pirates have also become more sophisticated, leveraging cutting-edge techniques such as malware, social engineering, and zero-day exploits. As the digital landscape continues to evolve, so too do the strategies of cyber pirates, posing significant challenges to cybersecurity experts and organizations tasked with defending against these threats. This introductory section sets the stage for a comprehensive exploration of cyber piracy, highlighting its broad scope and dynamic nature. Understanding the evolution of cyber space is crucial for developing effective strategies to combat and mitigate the impact of these ever-evolving digital threats[2].

CYBER SPACE THE SEA OF CYBER PIRATES

In our increasingly interconnected world, cyberspace has become an integral part of our daily lives, shaping how we communicate, conduct business, and interact with the digital realm.

[1] Dana Dahlstrom, 'piracy in the digital age',December 2006 [last visited 22 january 2024] https://www.riaa.com/issues/piracy/default.asp

[2] Kumaran U., Thangam S., T.V. Nidhin Prabhakar, Jana Selvaganesan, Vishwas H.N.[Adversarial Defence: A GAN-IF Based Cyber-security Model for Intrusion Detection in Software Piracy]2023

ISSN: 2582-6433

However, this virtual landscape is not without its challenges, and one of the most pressing issues is the pervasive threat of cyber piracy. This essay aims to explore the multifaceted dimensions of cyberspace, particularly in relation to the research paper that delves into the methods, motivations, and impact of cyber piracy on individuals, businesses, and governments worldwide. Cyberspace is a dynamic and ever-evolving environment, constantly shaped by technological advancements and the innovative use of digital tools. It encompasses the vast network of interconnected computers, servers, and devices that facilitate the exchange of information across the globe. As we navigate this digital realm, we encounter both the immense opportunities it presents and the lurking threats that manifest in the form of cyber piracy. The research paper highlighted the intricate methods employed by cyber criminals, ranging from sophisticated malware and ransomware attacks to deceptive phishing schemes and supply chain vulnerabilities. In cyberspace, these methods find fertile ground to exploit the digital infrastructure that underpins our interconnected world. Cyberspace serves as both the battleground and the medium through which cyber pirates execute their attacks, emphasizing the critical importance of understanding the nuances of this virtual terrain[3].Cyberspace is not merely a neutral platform; it is a realm where various actors pursue divergent motivations. The research paper identified financial gain, political agendas, and hacktivism as driving forces behind cyber piracy. In cyberspace, these motivations manifest in the form of targeted attacks on financial systems, political institutions, and online platforms. The virtual realm provides a cloak of anonymity, empowering actors to pursue their objectives with relative impunity. The impact of cyber piracy extends across continents, as cyberspace knows no borders. Individuals face the risk of identity theft, while businesses grapple with financial losses, operational disruptions, and reputational damage. Governments find themselves vulnerable to national security threats and espionage. The interconnected nature of cyberspace means that an attack on one part of the world can have cascading effects globally, underscoring the need for international collaboration in addressing cyber threats. Navigating cyberspace comes with inherent challenges, as highlighted in the research paper. Attribution difficulties, jurisdictional issues, and the rapid evolution of attack tactics pose formidable obstacles. In response, effective countermeasures must be devised. Improved cybersecurity measures, international collaboration, robust legislative frameworks, and public awareness campaigns emerge as crucial components of a comprehensive strategy to safeguard cyberspace. As we continue to

[3] Michael D. Smith 'PIRACY AND COPYRIGHT ENFORCEMENT MECHANISMS'June 2013, https://www.nber.org/papers/w19150

ISSN: 2582-6433

immerse ourselves in the vast expanse of cyberspace, the intricate dance between innovation and threat becomes increasingly apparent. Understanding the complexities of this virtual landscape is paramount, and the research paper on cyber piracy serves as a guide to unraveling the multifaceted dimensions of cyberspace.[4] By acknowledging the challenges and proposing mitigation strategies, we can strive to create a secure and resilient digital environment for individuals, businesses, and governments worldwide. In this ongoing journey, staying vigilant and informed is key to navigating the complex web of cyberspace.

METHODS OF CYBER PIRACY

In the vast expanse of cyberspace, the nefarious activities of cyber pirates cast a looming shadow over the interconnected digital landscape. As technology advances, so do the methods employed by these malicious actors, creating an intricate web of threats that pose significant challenges to individuals, businesses, and governments worldwide. This section delves into the multifaceted nature of cyber piracy, exploring five prominent methods utilized by cyber criminals to infiltrate, disrupt, and exploit digital systems.

1) Malware and Ransomware Attacks:

Malware and ransomware attacks represent sophisticated and pervasive methods employed by cyber pirates to compromise digital systems. Malware, a collective term for malicious software, is designed to infiltrate, damage, or gain unauthorized access to computer systems. Ransomware, a subset of malware, encrypts files or entire systems, rendering them inaccessible until a ransom is paid. These tactics exploit vulnerabilities in software or human behavior, emphasizing the need for robust cybersecurity measures to detect, prevent, and mitigate such attacks.

2) Phishing and Social Engineering:

Phishing, a deceptive technique, involves tricking individuals into divulging sensitive information such as usernames, passwords, or financial details. Social engineering, a related method, manipulates human psychology to gain access or extract confidential information. Cyber pirates often employ email, fake websites, or even phone calls to impersonate trusted entities, exploiting human trust to breach security defenses. Understanding these manipulative

[4] J. Barlow 'A Declaration of the Independence of Cyberspace' 2021 , https://www.eff.org/cyberspace-independence

ISSN: 2582-6433

tactics is crucial for fostering awareness and implementing preventive measures at both individual and organizational levels.[5]

3) Distributed Denial of Service (DDoS) Attacks:

DDoS attacks disrupt the normal functioning of a network or website by overwhelming it with a flood of traffic, rendering it inaccessible to users. Cyber pirates may deploy botnets, networks of compromised computers, to amplify the scale of such attacks. DDoS attacks can have severe consequences, causing financial losses and tarnishing the reputation of targeted entities. Effective DDoS mitigation strategies involve network monitoring, traffic filtering, and distributed infrastructure to absorb and mitigate the impact of the attack.

4) Supply Chain Attacks:

Supply chain attacks target vulnerabilities in the interconnected network of suppliers and service providers associated with a particular organization. By infiltrating a trusted supplier's network, cyber pirates can compromise the downstream systems and gain unauthorized access to the primary target. These attacks underscore the importance of securing the entire supply chain, with organizations needing to vet and monitor their suppliers' cybersecurity practices rigorously.

5) Zero-Day Exploits and Vulnerability Exploitation:

Zero-day exploits target software vulnerabilities that are unknown to the software vendor or security community. Cyber pirates capitalize on this gap to launch attacks before a fix or patch is available. Vulnerability exploitation involves identifying and taking advantage of weaknesses in software or hardware. Staying ahead of these exploits requires proactive security measures, including regular software updates, vulnerability assessments, and threat intelligence to anticipate potential avenues of attack.

Understanding these methods is essential for comprehending the dynamic and adaptive nature of cyber piracy. As the digital landscape evolves, cyber pirates continuously innovate their tactics, necessitating a proactive and multifaceted approach to cybersecurity. Organizations and individuals alike must stay informed about these methods and invest in resilient cybersecurity

[5] Esraa Alomari, R. R. Nuiaa, Z. Alyasseri, Husam Jasim Mohammed, N. Sani, Mohd Isrul Esa, Bashaer Abbuod Musawi[Malware Detection Using Deep Learning and Correlation-Based Feature Selection], 2023.

ISSN: 2582-6433

measures to safeguard against the ever-evolving threat landscape.[6]

IMPACT ON GLOBAL SECURITY

Cyber piracy, with its intricate methods and motivations, extends its tendrils far beyond the realms of individual victims or targeted organizations. Its repercussions reverberate globally, posing substantial threats to the overarching fabric of global security. Understanding the implications on a global scale is paramount for devising comprehensive strategies to safeguard the interconnected digital landscape.

1)Cyber Warfare: The evolution of cyber piracy has given rise to a new frontier in warfare – cyber warfare. Nations are increasingly leveraging cyber capabilities as tools of aggression, using sophisticated attacks to compromise critical infrastructure, disrupt essential services, and gain strategic advantages. The interconnectedness of digital systems across borders means that an attack on one nation can have cascading effects, creating a web of vulnerabilities that challenge the traditional paradigms of national security.

2) Critical Infrastructure Vulnerabilities: Critical infrastructure, ranging from power grids to financial systems, is a prime target for cyber pirates seeking to destabilize nations. The interconnected nature of these systems amplifies the impact of cyber attacks, potentially leading to widespread disruptions that transcend geographic boundaries. The vulnerabilities in critical infrastructure underscore the need for robust cybersecurity measures and international collaboration to fortify these vital components of global security.[7]

3) Espionage and National Security Threats: Cyber espionage, driven by state-sponsored actors or malicious entities, poses a significant threat to national security. The theft of sensitive information, intelligence, and classified data through cyber means can compromise the strategic interests of nations. As governments become increasingly reliant on digital communication and storage, the stakes in cyberspace escalate, necessitating collaborative efforts to detect, deter, and respond to cyber threats on a global scale.

[6] Nicolas Dejon, David J. Caputo, Luca Verderame, A. Armando, A. Merlo[Automated Security Analysis of IoT Software Updates] 2019.
[7] Richard E. Wilson, Alexia Fitz[Nuclear Weapons, Cyber Warfare, and Cyber Security: Ethical and Anticipated Ethical Issues]2023

ISSN: 2582-6433

CHALLENGES IN COMBATING CYBER PIRACY

As the digital landscape continues to evolve, the phenomenon of cyber piracy presents a complex and multifaceted challenge that transcends geographic boundaries. Effectively combating this pervasive threat demands a nuanced understanding of the intricate challenges that arise in the realms of attribution, jurisdiction, rapid technological evolution, and international cooperation. This section explores the formidable obstacles encountered in the global effort to counter cyber piracy, shedding light on the complexities that governments, cybersecurity professionals, and international entities must navigate to secure the interconnected digital realm. From the elusive nature of attribution to the legal intricacies of jurisdictional issues, the rapid evolution of tactics, and the imperative need for enhanced international cooperation, these challenges underscore the necessity for a unified and proactive approach to fortify global cybersecurity defenses.[8]

- Attribution Difficulties: One of the foremost challenges in combating cyber piracy on a global scale lies in attribution difficulties. Determining the origin of a cyber attack is intricate, with perpetrators often concealing their identities through various means. This lack of clear attribution complicates diplomatic responses and international cooperation in holding responsible parties accountable.
- Jurisdictional Issues: Cyber attacks can traverse international borders effortlessly, leading to jurisdictional challenges in prosecuting cyber criminals. The misalignment of legal frameworks and the absence of standardized international laws for cybercrime hinder the effective pursuit and apprehension of perpetrators, contributing to the impunity with which cyber pirates operate.
- Rapidly Evolving Tactics: The fast-paced evolution of cyber tactics presents an ongoing challenge for global security efforts. Cyber pirates adapt swiftly to advancements in cybersecurity measures, exploiting emerging technologies and vulnerabilities. This constant evolution demands a proactive and collaborative approach to stay ahead of the curve in countering cyber threats.
- Lack of International Cooperation: Effective mitigation of cyber piracy requires robust international cooperation, information sharing, and coordinated responses. However, geopolitical tensions and varying national interests can impede collaborative efforts.

[8] Mukund Sundararajan, Ankur Taly, Qiqi Yan[Axiomatic Attribution for Deep Networks],2017.

ISSN: 2582-6433

Bridging these gaps and fostering a united front against cyber threats is imperative for strengthening global security in the face of an ever-evolving cyber landscape.[9]

In summary, the impact of cyber piracy on global security is profound, encompassing the realms of cyber warfare, critical infrastructure vulnerabilities, and espionage. Addressing the associated challenges requires a united and concerted effort on an international scale, involving governments, organizations, and cybersecurity experts working collaboratively to fortify the digital defenses that underpin the security of nations worldwide.

ANTI-PIRACY INTERVENTIONS

In response to the escalating threat of cyber piracy, a myriad of interventions has been devised to counteract and mitigate its adverse impacts. One crucial facet of these interventions involves the development and implementation of robust cybersecurity measures. These measures span from the deployment of advanced intrusion detection systems to the regular updating and patching of software vulnerabilities, forming a digital fortress against the ever-evolving tactics of cyber pirates. International collaboration and information sharing stand out as key pillars in the collective effort to combat cyber piracy. Given the borderless nature of the digital landscape, effective intervention requires nations to transcend geopolitical boundaries and pool their resources. Collaborative initiatives facilitate the exchange of threat intelligence, best practices, and technological innovations, enabling a unified response against cyber threats on a global scale. Legislative and regulatory frameworks play an instrumental role in anti-piracy intervention. Governments worldwide are increasingly recognizing the need for comprehensive cyber laws that define and penalize cybercrimes. [10]These legal instruments not only act as deterrents but also provide the necessary legal basis for prosecuting cyber pirates. Additionally, fostering international cooperation in harmonizing cyber laws ensures a consistent and effective legal landscape for combating cybercrime. Public awareness and education form another critical component of anti-piracy interventions. Empowering individuals and organizations with the knowledge to recognize and respond to cyber threats is pivotal. Education campaigns aim to cultivate a culture of cybersecurity consciousness, encouraging proactive measures such as secure online practices, the use of robust passwords, and the recognition of phishing attempts. The multidimensional nature of cyber piracy demands a

[9] Y. Razmetaeva, H. Ponomarova, Iryna Bylya-Sabadash[Jurisdictional Issues in the Digital Age],2021.
[10] M. Zipperle, F. Gottwalt, Elizabeth Chang, T. Dillon[Provenance-based Intrusion Detection Systems: A Survey]2022.

ISSN: 2582-6433

holistic approach to intervention. Anti-piracy efforts must evolve in tandem with the dynamic threat landscape, adapting to emerging technologies and tactics. Through the concerted implementation of cybersecurity measures, international collaboration, legislative frameworks, and educational initiatives, stakeholders can collectively fortify the digital realm against the pervasive threat of cyber piracy.[11]

EMERGING THREATS IN CYBER PIRACY

As the digital landscape evolves, the horizon of cyber piracy widens, presenting a continuum of challenges and potential threats. This section scrutinizes the future trends and emerging threats that are poised to shape the landscape of cyber piracy, requiring proactive measures to fortify global cybersecurity defenses.

- Artificial Intelligence and Machine Learning in Cyber Piracy: The integration of artificial intelligence (AI) and machine learning (ML) into cyber piracy tactics marks a paradigm shift. Cyber pirates are leveraging AI and ML to enhance the sophistication of their attacks, enabling automated and adaptive strategies. This subsection explores the implications of AI-driven cyber piracy, assessing the potential for more potent and evasive threats that can dynamically respond to security measures[12].
- Internet of Things (IoT) Vulnerabilities: The proliferation of Internet of Things (IoT) devices introduces a myriad of entry points for cyber pirates. Insecure IoT devices can become vectors for cyber attacks, contributing to the expansion of botnets and creating vulnerabilities in interconnected systems. This exploration delves into the emerging threats stemming from IoT devices and the imperative need for robust security measures to safeguard against potential exploitation.
- Quantum Computing and Cryptographic Risks: As quantum computing advances, the cryptographic algorithms that underpin current cybersecurity protocols face potential vulnerabilities. Quantum computers have the capability to break traditional encryption methods, posing a unique challenge for securing digital communications. This subsection examines the cryptographic risks associated with quantum computing and explores strategies to develop quantum-resistant cryptographic solutions.

[11] Dawit Tolossa[IMPORTANCE OF CYBERSECURITY AWARENESS TRAINING FOR EMPLOYEES IN BUSINESS],2023.
[12] Ranu Sewada, Ashwani Jangid, Piyush Kumar, Neha Mishra[Explainable Artificial Intelligence],2023.

ISSN: 2582-6433

Anticipating these future trends and emerging threats is paramount for staying ahead of the cyber piracy curve. By understanding the potential trajectories of technological advancements and the associated risks, stakeholders can proactively adapt their cybersecurity strategies to address the evolving challenges in the digital landscape. The insights garnered from this exploration provide a foundation for the ongoing efforts to bolster cybersecurity and ensure the resilience of global digital infrastructures.[13]

CONCLUSION

Piracy has been a major problem since the dawn of digital age and the explosion of WWW (World Wide Web). The fast adoption of the Internet and the digitization of information products have led an increasing number of consumers to copy and distribute digital products without the authorization of their legal owner. A lot of adults and youths delight in sharing software, games, music, e-books, pictures, etc. They do not perceive digital piracy to be an ethical issue. They see it as a way of helping and being nice to others. Pirates will always find a way. They have found various ways to bypass the Internet giant's and keep their videos online for millions to watch. Technology has expanded many people's ability to access pirated material and store it with ease. When it comes to piracy, everyone is involved, one way or another.

[13] Kevin M. Stine[Framework for Improving Critical Infrastructure Cybersecurity],2021.