CRYPTO-ENABLED ESPIONAGE: THE GROWING THREAT TO NATIONAL SECURITY

Oladipupo AbdulMalik Olalekan

Department of Politics and International, Lead City University, Ibadan.

Email: oladipupo.abdulmalik@lcu.edu.ng; Tel.: +2349163938209

Cite this article:

Oladipupo AbdulMalik Olalekan (2024), Crypto-Enabled Espionage: The Growing Threat to National Security. African Journal of Social Sciences and Humanities Research 7(4), 235-246. DOI: 10.52589/AJSSHR-Z73T57O2

Manuscript History

Received: 26 Aug 2024

Accepted: 3 Nov 2024

Published: 11 Nov 2024

ABSTRACT: *This paper examines the growing threat of crypto-enabled espionage and its impact on national security. The research addresses the central questions on how cryptocurrencies facilitate espionage, and what the implications for national security are. Using a qualitative approach, the study draws on existing literature, case studies, and intelligence reports to explore how cryptocurrencies are increasingly being leveraged by state and non-state actors for covert operations. The findings reveal that the key features of cryptocurrencies—such as anonymity, decentralization, and the lack of regulation make them highly attractive to espionage actors. Specific cases, including the use of cryptocurrencies by North Korean and Russian state sponsored espionage networks, demonstrate how these actors bypass financial surveillance systems. The study concludes that while cryptocurrencies offer significant advantages for espionage, they pose severe challenges for national security agencies, especially in terms of monitoring and preventing illicit activities. To address these threats, stronger international cooperation, regulatory reforms, and advancements in blockchain surveillance technology are necessary. The paper recommends further research into counterintelligence strategies that incorporate blockchain technology and artificial intelligence for monitoring crypto-enabled espionage.*

KEYWORDS: Crypto-Enabled Espionage, Cryptocurrency, Blockchain, National Security, Decentralization, Cyber Warfare.

Article DOI: 10.52589/AJSSHR-Z73T57O2
DOI URL: https://doi.org/10.52589/AJSSHR-Z73T57O2

INTRODUCTION

Espionage is one of the oldest threats to national security, customary from any user, with its members which include intelligence and spying, collecting and monitoring influential political, military and economic systems that are controlled by local as well as international players. Modern espionage, however, which over the last few decades has entered the information age, has become more high-tech, moving from combat officers and arms that sneak into houses and buildings to arms that penetrate computers and electronic networks and collect information from them. This shift has altered the coverage of intelligence with new methods of mass surveillance, data hunting, and tampering with structures in other nations. Today, cryptocurrencies have become an extra element of international clandestine operations mainly because they are decentralized and not easily traceable.

The new approach to cryptocurrencies like Bitcoin and Ethereum is that they provide an opportunity to work with money without the interference of government and financial systems dominating the world. Cryptocurrency is built on the blockchain technology that works on the principle of distributed ledger where every transaction gets recorded on the multiple nodes that are syntactically visible but not very much analytically accessible. To the worthy beneficiaries, the features are in fact an advantageous factor providing privacy and excluding banking charges. Nonetheless, these are the very things that also make cryptocurrencies fascinating to the black hats, more so, those in the espionage business. In the sphere of national security, it is worth noting that espionage actors are now successfully utilizing cryptocurrency as an anonymity instrument for their illicit actions. This includes all manner of transactions starting with the movement of funds to agents active in conspiracies as well as the acquisition of the equipment utilized in cyber crime. These actors can avoid the usual financial checks that institutions put in place to report any fishy activity to the authorities through cryptocurrencies. This was as seen in the current study conducted by Tahir et al. (2021) where they inferred that cryptocurrencies are now being used as sources of funding of intelligence as well as cyber attacks which could be sponsored by states or non-state actors.

Here, it was cryptocurrency's involvement in espionage that initially attracted noteworthy consideration when ransomware culprits began to demand payment in Bitcoin. In recent years, state-sponsored espionage actors resorted to using cryptocurrencies to fund hacking operations with the challenges of tracking the movement of funds. Cryptocurrencies differ from conventional financial activities in that they cannot be facilitated through third parties of financial institutions. This makes it extremely difficult for national security agencies to prevent (Mirinda, 2021) or block these transactions in real time, as has been observed by Deshpande et al. (2020).

Cryptocurrencies are even more involved, not only in financing espionage but also in interaction between different actors of espionage. A few cryptocurrencies include anonymous aspects in their protocol, including Monero's, stealth addresses and hidden ring signatures. This makes it difficult for the Police to follow the cash flow associated with espionage activities. These tools are especially desirable to espionage groups that conduct operations in areas that are unfriendly to them or are involved in international espionage activities in which utilization of normal banking channels will lead to discovery. Furthermore, cryptocurrency can make the purchase of services from hackers involved in computer hacking, data theft, and sabotage. Chairs sanctioned by the state have especially transferred their funding for these purposes to crypto trances. For example, North Korea has been blamed for engaging in many cyber espionage attacks, out of which the revenue gotten from stolen crypto was used in financing the country's intelligence and its military (Tahir et al., 2021). Likewise, according to cybersecurity experts, Russian and Chinese spying networks are also said to have been utilizing cryptocurrency to launder the cash, thus making it almost impossible for Western spies to track down illicit funds (Casey & Vigna, 2021). The growth of such espionage has the following implications to national security agencies: Talent traditional intelligence to a large extent based on tracking funds, imagery and key loggers, and close-in on a target's social network. Cryptocurrencies thus negate these methods by offering an inheritance of secure and peer-to-peer methods of passing information and value. Compared to centralized banking systems where regulators can easily monitor transactions that they deem suspicious, financial crime operates within many of the decentralized and pseudonymous structures of many cryptocurrency platforms.

Further, the decentralized and global nature of cryptocurrency distorts enforcement even further. Numerous cryptocurrencies are cross-border, and because all the operations take place on distributed systems, no country can regulate them. This complicates the attempt to enact rules to put their regulations in place or monitor the cross-border movement of funds. Consequently, espionage actors can work in a very synchronized way, funding its operations in a particular geographical location through cryptocurrency while the proceeds are channeled to players in another region with negligible chances of being intercepted. Another paper published by the European Union Agency for Cybersecurity (ENISA) in 2020 noted that nation-states are expanding the use of cryptocurrency for espionage, cyberattacks, as well as other types of hybrid warfare; however, anonymity of cryptocurrency transactions is going to be a significant problem for the law enforcement officers of different countries. It has, therefore, raised the need to come up with new measures to monitor top secret actions that happen on the blockchain. The current type of espionage operations involves a complex of cyber operations, ransomware, information leak, manipulation of infrastructure systems of different countries. Cryptocurrencies are present in many of these operations – not only as the currency of the transactions, but also as enablers of secure and anonymous communication. This characteristic renders blockchain perfect for clandestine intelligence work as spies or hackers share sensitive data, or organize an attack on Blockchain without a fear of it being altered or hacked into.

Therefore, it can be concluded that change of landscape in national security is under consideration due to the use of Cryptocurrencies in espionage activities. It is for this reason that current conventional espionage and surveillance techniques are no longer in effect in the new world of technology. Cryptocurrencies and especially their markets have been rapidly growing, and at the same time, there are no sufficient regulatory measures, which is an essential weakness a nation state should not afford. To effectively deal with all these emerging threats, there is need for governments and security agencies to come up with surveillance techniques in blockchain besides addressing the international cooperation techniques of countering threats posed by crypto-enabled espionage (Deshpande et al., 2020; Tahir et al., 2021).

Article DOI: 10.52589/AJSSHR-Z73T57O2
DOI URL: https://doi.org/10.52589/AJSSHR-Z73T57O2

Research Objective

The main research question of this type of work is to find out the specifics of using cryptocurrencies in espionage and determining the increasing threats of crypto-espionage to national security. Specific objectives include:

i. To examine how cryptocurrencies have facilitated clandestine activities and espionage.

ii. To explore how cryptography affects national security agencies' ability to detect espionage actions.

iii. To be able to offer recommendations for the decrease of espionage threats associated with the utilisation of cryptocurrencies.

Research Questions

i. In what way do cryptocurrencies facilitate clandestine support and spying in espionage operations?

ii. What are the main problems that threaten the national security agencies when it comes to using cryptocurrencies in espionage detection and prevention?

iii. As we look at the nature of risks that are likely to be posed by crypto enabled espionage, what strategies and policies can effectively address these risks?

Significance of the Study

As cryptocurrencies deepen their usage in espionage activities, this has posed a significant threat to any nation around the globe. Various national security agencies are still in a process of facing threats of cyber warfare, and now have to deal with espionage actors and blockchain technologies. The importance of this study is anchored more on the fact that while there is growing literature on threats of national security, not much has been done on this potential threat of cryptocurrency in espionage activity. Tahir et al. (2021) have established that expansion of cryptocurrencies and the lack of sufficient regulation offer an environment for espionage operations to operate in, which would not be apparent in traditional financial surveillance. The best approach that the law enforcement agencies, intelligence agencies and policymakers must have is the knowledge on how cryptocurrencies are used in espionage. In addition, this research enriches the discussion on the relationship between new ICT and security cited by Casey and Vigna (2021) and indicates that the digital currencies have changed the approach to the modem crime like espionage in the age of the fourth industrial revolution.

Scope and Limitations

This paper examines crypto-enabled espionage and counterintelligence issues and uses secondary data sources, such as case studies, intelligence reports and academic materials. Despite the fact that the work presents a general description of the phenomenon, secret activities of spies allow receiving only indirect, current data. In addition, the study mainly focuses on the use of cryptocurrencies in spying activities while other blockchain applications in other unlawful engagements are not considered. This limitation suggests that future empirical studies that are existent can focus on concrete instances where cryptocurrencies have been associated with espionage actionable threats, giving a richer account of the emerging threat environment.

LITERATURE REVIEW

Blockchain Technology

Cryptocurrencies are built upon most blockchain technologies, and they offer the world a decentralized system for registration. This decentralization makes it extremely hard for anyone to interfere, modify and censor which is beneficial to espionage actors who want to be unseen and secure. As highlighted by Kshetri (2021), cryptographic properties such as secure hashing and consensus mechanisms facilitate immutability and the complex tracing of transaction records. By immutability, it means that in terms of spy craft, the participants can transact not only funds but also messages on the blockchain networks. Further, due to the distributed nature of the blockchain, there lies no single point at which the intelligence agencies can insert themselves to dismantle this sort of espionage effort.

Decentralization

Understanding decentralization is important when trying to explore why cryptocurrencies are so attractive to espionage actors. Unlike more conventional financial systems in which there exist centralized regulatory focal points [like banks or government], cryptocurrencies operate within decentralized networks in which no governing authority directs the dispensation of the funds. Dube and Vitkovski (2022) suggest that this decentralization enables espionage groups to perform their activities beyond regulation. Much of this decentralization is done beyond the regime of standard regulations, like those from international financial supervisory entities. Hence, there is less possibility of detection for spies as the exchanges cannot be easily intercepted or frozen by the government.

Anonymity and Pseudonymity

Another key benefit of cryptocurrencies as far as espionage activities are concerned is that they afford very high levels of identity anonymity or pseudonymity. Depending on the financial type, users have to identify themselves, while cryptocurrencies let actors perform transactions under some other name or even be fully anonymous. Other cryptocurrencies that do a better job in concealing the identity of users include Monero and Zcash, in that these post details like the sender, receiver, and the amount sent or received, which are all hidden. In their view, Broadhurst et al. (2020) attribute this kind of anonymity to make it vastly more complex for the intelligence as well as counterintelligence agencies to track espionage-connected financial operations. For instance, state-connected spy agencies can transact in these cryptocurrencies knowing fully well that they cannot be easily associated with specific states.

Cryptographic Security

Cryptography is a fundamental part of blockchain and of all the financial transactions which are made using cryptocurrencies. It also guarantees that data shared over the block chains are purely safe and secure through the employment of enhanced cryptographic methods. In their current form, Lindström (2020) observes that espionage actors leverage blockchain's cryptographic security to protect their financial operations and messages. For example, elliptic

Article DOI: 10.52589/AJSSHR-Z73T57O2
DOI URL: https://doi.org/10.52589/AJSSHR-Z73T57O2

curve cryptography, hashing help to prevent espionage connected operations from being intercepted or decrypted by those not authorized. This degree of secession makes it easier for espionage agents to perform secret operations in the course of duty, without the concern of fixed observation.

Underpinning Theories

Asymmetric Warfare Theory

Asymmetric warfare theory explains how smaller, less powerful actors can challenge more dominant adversaries by using unconventional tactics. In the context of crypto-enabled espionage, this theory is relevant because it shows how non-state actors, small rogue states, or even hacktivist groups can use cryptocurrency to conduct covert operations against major national powers. The decentralized and anonymous nature of cryptocurrency allows these actors to bypass traditional financial systems, making it difficult for larger intelligence and counterintelligence agencies to track or disrupt their operations. Asymmetric warfare highlights the idea that technologically weaker adversaries can exploit vulnerabilities within advanced systems, such as national security frameworks, through means like cryptocurrency.

Cyber Warfare Theory

Cyber warfare theory focuses on the use of digital tools and techniques to conduct espionage, sabotage, or other hostile actions against state or non-state actors. This theory is particularly relevant to crypto-enabled espionage, where cryptocurrencies act as both a financial tool and a medium for covert communication. Cyber warfare encompasses a broad range of digital activities, including hacking, malware deployment, and data breaches, which can be funded or facilitated using cryptocurrencies. The rise of blockchain technology has added a new dimension to cyber warfare, as it provides a secure platform for espionage actors to transmit sensitive information or pay operatives without detection.

Financial Anonymity and Cryptocurrencies

The concept of financial anonymity is critical in understanding the appeal of cryptocurrency in espionage activities. Traditional financial systems, such as banks or wire transfers, are subject to government regulations and surveillance, making them unsuitable for covert operations. Cryptocurrencies like Bitcoin, Monero, and Zcash offer pseudonymity or full anonymity, allowing espionage agents to move funds without revealing their identity. This financial anonymity makes cryptocurrency ideal for funding espionage missions, paying hackers, or transferring value across borders without leaving a trace. As a result, intelligence and counterintelligence agencies find it much harder to track financial flows linked to espionage activities.

Empirical Research

Some works focus on the relationship that cryptocurrency has with crime to include cybercrime, money laundering, and terrorism financing. One major interest in recent literature is on how these activities can be facilitated by cryptocurrencies in that users acquire a safe means of transacting anonymously. For example, Broadhurst et al. (2020) discovered that criminals use cryptocurrencies because of their decentralization and cross-border transactions; the same is valued for espionage. As for spying, the scientific publications have focused on

Article DOI: 10.52589/AJSSHR-Z73T57O2
DOI URL: https://doi.org/10.52589/AJSSHR-Z73T57O2

nation-state attributes of cyberspace and their application of cryptocurrencies for ulterior motives. As Kshetri reported in 2021, state-backed spy agencies have notably recently started using cryptocurrencies as a means of funding cyber operations and collection. According to Kshetri, cryptocurrencies assist these groups in executing their espionage activities because they are opaque, which makes it difficult for these bodies to monitor them due to evasion of international sanctions. Moreover, Lindström (2020) speaks about cryptocurrencies as the basis for secure financial transactions for an intelligence operation with an emphasis on hacking and cyber-attacks.

Another example is a work from Dube and Vitkovski (2022) that examines how the technology underlying this type of organizational system has been weaponized. In their research, they present various aspects on how espionage groups have exploited these characteristics of blockchain technology to store and transfer sensitive information and render them inaccessible for any counterintelligence agency to intercept or decode the message.

Critical Analysis of the Literature

Although a significant body of literature already exists in the areas related to cryptocurrencies and crime, relatively few dedicated to the utilization of cryptocurrencies for spying has been published. Some of the findings of the studies considered in this work affect the anonymity and decentralized use of cryptocurrencies, but none of those looked at how such properties make use of cryptocurrencies ideal for intelligence gathering and other sneak operations. For example, Broadhurst et al. (2020) and Lindström (2020) offer a general background of the use of cryptocurrency in the crime, attributing it to espionage, but they are not exhaustive in case descriptions of espionage or empirical data. However, Like Kshetri (2021) work, it also generalizes the use of cryptocurrencies by state actors or lumps different forms of cybercrime with espionage. However, there is still a significant shortage of detailed information regarding how precisely intelligence agencies, or other villains, perform spying operations using cryptocurrencies. As mentioned, there is a lack of discussions about the non-financial aspects of blockchain in espionage; however, even Dube and Vitkovski (2022) do not explore the real-life cases of such grotesque incidents, which are potentially useful for identifying potential solutions to these threats.

To fill these gaps, further research should qualify concrete examples of crypto-enabled spy operations, with an emphasis on certain states – North Korea, Russia, Iran and others – that are reputed for their highly developed information warfare potentialities. Furthermore, there is a requirement of more interdisciplinary works which focus on cyber warfare, intelligence studies, and blockchain technology in order to gain a more newborn’s picture of how cryptocurrencies are being used as tools for spying. Due to the realization by governments and international organizations of the nature of threats posed by crypto-enabled espionage to any nation, there has been a push for regulation. For example, the Financial Action Task Force (FATF) has provided recommendations on how to control the reuse of cryptocurrency trading techniques for money laundering and funding of terrorism (FATF, 2019). However, the enforcement of such regulations has been a slow process especially due to its application in spying where many individuals act beyond police apprehension abilities. Lusthaus and Varese (2021) suggest that while there is no stopping individuals who seek to use crypto for espionage, more stringent regulations as well as blockchain forensic analysis instruments could go a long way in reducing the risk, or rather likelihood, of such use of crypto. But they also warn that the tremendously

Article DOI: 10.52589/AJSSHR-Z73T57O2
DOI URL: https://doi.org/10.52589/AJSSHR-Z73T57O2

distributed nature of the blockchain aggravates the problem of regulation because both cryptocurrencies and espionage efforts are equally global.

METHODOLOGY

This research utilizes a qualitative research method and only secondary sources of information sourced from refereed academic journals, key cybersecurity reports, and cases. The research design focuses on following key themes for content analysis, mainly, pattern of using cryptocurrencies in spying. Because of the design of the study, there were no primary participants used in the study. However, archival data were obtained from documents like government publications and intelligence archives which specifically targeted incidents related to cryptocurrencies and espionage. The information was obtained from scholarly journals and articles, cybersecurity reports and case studies. Data treatment included identifying and sorting the material according to significant topics such as anonymity, use of the blockchain, and state spying.

RESULTS

Anonymity

In this research, the author discovered that cryptocurrencies offer fairly good anonymity, which is desirable to spy practitioners. Other cryptocurrencies such as Monero and Zcash are even built to have higher privacy mechanisms than Bitcoin. This untraceability enables espionage agents to transfer money, purchase information and stage clandestine operations since these activities do not raise any alarm for security departments over the financial sector.

Decentralization and Related Regulatory Problems

Cryptocurrencies refer to digital currencies whose operations are based on shared databases referred to as blockchains, where there is no authoritative third party in charge of the transactions. This decentralization presents enormous regulatory problems for governments that want to ban their use in spying operations. Since no single person or organization owns the blockchain, the various police agencies may have problems with tapping on the transactions or even closing down the businesses; this is a clear benefit for those involved in espionage.

State-Sponsored Crypto-Espionage

Another important finding is the increasing involvement of state-sponsored actors in crypto-enabled espionage. Several cases have linked cryptocurrency use to nation-state actors conducting cyber espionage. For example, North Korea has been documented to use cryptocurrencies to bypass international sanctions and fund intelligence operations. Cryptocurrencies enable these actors to remain financially independent, while also concealing the origins of their transactions, making it more difficult to trace their activities back to the sponsoring state.

Article DOI: 10.52589/AJSSHR-Z73T57O2
DOI URL: https://doi.org/10.52589/AJSSHR-Z73T57O2

DISCUSSION

The anonymity of cryptocurrencies is one of the key elements making them an attractive tool for espionage. Cryptocurrencies like Monero, Zcash, and Bitcoin allow for the transfer of funds without disclosing personal identities, making them a natural fit for covert operations. As noted by Li and Wang (2021), the pseudonymity of cryptocurrencies makes it difficult for regulatory bodies to trace the parties involved in transactions, posing a risk to national security as it provides a means for malicious actors to avoid detection. Moreover, decentralized blockchain networks operate without the oversight of centralized financial institutions, creating further regulatory challenges for governments and security agencies, as observed by Foley, Karlsen, and Putniņš (2019).

Furthermore, research reveals that state-sponsored actors, particularly those involved in cyber espionage, are exploiting cryptocurrency as a financial tool. Reports suggest that North Korea, through its Lazarus Group, has increasingly utilized cryptocurrency to fund illicit programs, including missile development and espionage activities (Perkins, 2020). The decentralized nature of blockchain, coupled with the absence of international regulatory frameworks, exacerbates the risks, making cryptocurrencies a potent tool in modern intelligence operations.

Broader Implications for National Security

The growing use of cryptocurrencies in espionage introduces several national security challenges. Traditional methods of tracing financial transactions through centralized banks or international financial systems are ineffective against cryptocurrencies, which operate independently of governmental oversight. This, in turn, complicates efforts by intelligence agencies to monitor and disrupt espionage activities. As noted by Kshetri (2021), the use of blockchain and cryptocurrency in cybercrime, particularly in espionage and ransomware, is creating a significant gap in the counterintelligence capabilities of many nations.

This situation not only complicates efforts to trace state-sponsored activities but also opens the door for non-state actors to engage in espionage more effectively. Smaller nations or technologically weaker states can exploit these technological tools to level the playing field against larger powers. This is particularly evident in asymmetric warfare, where cryptocurrencies can be used to disrupt traditional intelligence gathering or covert operations, as discussed by Chen and Xu (2020). The implications extend beyond national borders, as the decentralized nature of cryptocurrencies poses challenges for international law and security. As global tensions rise, state actors can use cryptocurrencies to finance espionage without fearing immediate consequences. Cryptocurrencies allow for a new type of covert operation that circumvents traditional sanctions or financial monitoring systems, raising geopolitical risks, as highlighted by Kethineni and Cao (2020).

Comparison with Previous Research

In contrast to previous research concentrating on the use of cryptocurrency to facilitate cybercrime, money laundering, and terrorism financing, this analysis solely examines the increasing problem of crypto-based espionage. Some past works like Foley et al. (2019) analysed how criminals use cryptocurrency for more nefarious endeavours. Although such studies measured the potential danger of anonymity of transactions, such scholarship did not directly speak to how state-sponsored espionage is enabled by cryptocurrencies. This paper

Article DOI: 10.52589/AJSSHR-Z73T57O2
DOI URL: https://doi.org/10.52589/AJSSHR-Z73T57O2

extends from those findings by addressing this specific application as well as revealing these distinctive patterns of cryptocurrencies in espionage.

Li and Wang (2021) have also reviewed the relation of cryptocurrency to cybercrime, but more on the technological lens, that is, anonymity. This study builds on their work by identifying those features as the reason why cryptocurrency is perfect for espionage, hence adding yet another layer of complexity to the problem which already occupies national security agencies that seek to monitor such activities. Furthermore, unlike Kshetri's (2021) prior work that analyzed blockchain's effect on cybersecurity in general, this paper establishes an emerging trend in which state actors alongside individual cybercriminals use cryptocurrencies for espionage and clandestine operations. This is a deviation from previous research works most of which have concentrated on actors in the global periphery and fraudsters who employ cryptocurrency to fund cross-border crimes. Kethineni and Cao (2020) investigated cryptocurrency usage for terrorism financing, all through giving a brief consideration to the ability of state actors to harness it for their own gain. However, they did not pay much attention to the specifics of applying cryptocurrencies to spy activities, and this work aims to cover this gap.

Consequently, whereas prior studies have discussed the difficulties of combating cryptocurrency in legal terms for police and the regulation authorities, this paper aims to present a narrow analysis of crypto-based espionage. Expanding on traditional cybercrime discourses, this research focuses on state-led espionage and the exact processes through which cryptocurrencies can be used to enable clandestine actions. It therefore frames crypto-espionage as the novel and potent threat that it is for the world.

CONCLUSION

Cryptographic black operations are a major and increasing threat to the security of nations as we speak. As the findings of this research show, technology underpinning the cryptocurrency, which includes anonymity of transactions, decentralisation and unrestricted nature of exchange creates a welcoming environment for espionage actors. Current digital coins such as Bitcoin, Monero, and Zcash are also proving crucial in espionage as state and non-state actors perform secret operations without the possibility of being traced financially. Cryptocurrency in espionage evades intelligence as well as counterintelligence procedures; thus, it becomes challenging for governments and security agencies to unravel and counterintelligence conspiracies. Moreover, the paper investigates sections of the state that are using blockchain for assistance in circumventing and sanction bypass, financing attacks, and geopolitical interference.

Application for Practice and Policy

Cryptocurrency driven espionage poses new and complex threats and risks to existing institutions of national security, intelligence services, and regulating authorities. Currently, authorities of states and the international community must shift their focus towards the modernization of cybersecurity vectors and apply blockchain analysis tools as well as develop cross-state cooperation for tracking and monitoring suspicious cryptocurrency activities. Counterintelligence planning by the intelligence agencies will have to be redesigned to focus on new technological approaches to Machine Learning and AI Blockchain surveillance.

Article DOI: 10.52589/AJSSHR-Z73T57O2
DOI URL: https://doi.org/10.52589/AJSSHR-Z73T57O2

Furthermore, there is the need for the modern authorities to establish suitable legal standards that can effectively address the impermissible uses of cryptocurrencies while at the same time allowing for proper decentralized blockchain technology advancement.

To address these challenges, several actions are necessary:

1. Strengthening International Cooperation: Since cryptocurrencies are rather international in nature, espionage plans are frequently implemented across international lines. Global organizations like the United Nations and FATF and INTERPOL have to increase promotion of universal guidelines governing the use of cryptocurrencies and also improve intelligence sharing of espionage involving the cryptocurrencies.

2. Blockchain Forensics and Monitoring: Government and various agencies need to focus on buying software that can audit the movement of money through the various blockchains. While many cryptos currently place emphasis on anonymity, it is now possible to trace transactions at least to some extent even on the most anonymous cryptocurrencies. The further development in this area will improve the counter espionage activities that are already in existence.

3. Legislative Reforms: Government needs to come with new legal guidelines setting to curb the use of the cryptocurrencies in espionage and other unlawful incidences. Such regulations should force cryptocurrency exchanges and wallet providers to adhere to Know Your Customer (KYC) and Anti-Money Laundering (AML) policies in a bid to check those who wish to use digital currencies for unlawful activities.

SUGGESTIONS FOR FURTHER RESEARCH

This work was somehow restricted by the nature of espionage, which is quite concealed; by this, this study could not obtain specific and proximate samples of crypto-enabled espionage. In addition, due to an exponential growth of blockchain technology and introducing novel privacy coins, it is challenging to embrace all the aspects of this threat within the scope of the singular paper. The authors recommend that subsequent studies should incorporate detailed examinations of actual crypto-enabled espionage campaigns so as to accrue qualitative evidence on the utilization of cryptocurrencies in actual intelligence processes. Furthermore, research is necessary regarding how the relatively new advanced technology such as quantum computing can pose a threat or boost blockchain security in the future of crypto-enabled espionage.

The future research may also look into more detailed countermeasures that would help to prevent crypto-enabled espionage. Such topics involve artificial intelligence and blockchain: national security threats, and private blockchain solutions which could protect state level information from espionage by foreign powers. Consequently, the crypto-enabled espionage is the modern growing and complex threat obligating and initiating international cooperation in its counteraction. It is a reality that intelligence agencies and policymakers need to consider this type of covert operations; thus, agencies have to change their approaches by combining their existing tactics with new technology, while policymakers have to establish progressive regulations that can respond to new technologies. When these challenges are met, nations will

Article DOI: 10.52589/AJSSHR-Z73T57O2
DOI URL: https://doi.org/10.52589/AJSSHR-Z73T57O2

be better placed in protecting against malicious use of crypto-enabled espionage and hence a safer cyberspace to look forward to.

REFERENCES

1. Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2020). **Cybercrime and cryptocurrency: Crime, criminology and system capacity.** *Journal of Cybersecurity*, 6(1), 1-10.
2. Casey, M., & Vigna, P. (2021). *Cryptocurrency and its Role in Espionage: Evolving Threats to Global Security*. *Journal of Security Studies*, 7(2), 102-118.
3. Chen, Y., & Xu, C. (2020). Cryptocurrency in asymmetric warfare: A new paradigm for financial disruption. *Journal of Digital Security and Law*, 8(1), 45-67.
4. Deshpande, R., Woodside, J. M., & Yadav, V. (2020). Cryptocurrencies, Blockchain, and Cybersecurity: Challenges and Implications for National Security. *Journal of Strategic Security*, 13(3), 45-66.
5. Dube, P., & Vitkovski, M. (2022). **Blockchain espionage: How cryptography and decentralized finance are reshaping covert operations.** *Cyber Intelligence Journal*, 5(3), 120-135.
6. European Union Agency for Cybersecurity (ENISA). (2020). *Threat Landscape Report*. Brussels: ENISA.
7. FATF. (2019). **Guidance for a risk-based approach to virtual assets and virtual asset service providers.** Financial Action Task Force.
8. Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? *Review of Financial Studies*, 32(5), 1798-1853.
9. Kethineni, S., & Cao, Y. (2020). The rise of cryptocurrency and its criminal implications. *Crime, Law and Social Change*, 73, 239-260.
10. Kshetri, N. (2021). Blockchain and cybersecurity: A comprehensive study. *Journal of Cybersecurity Studies*, 9(2), 98-113.
11. Kshetri, N. (2021). **Cryptocurrency and cybersecurity: An evolving threat.** *Journal of Strategic Security*, 14(2), 89-110.
12. Li, Y., & Wang, X. (2021). Cryptocurrency and financial anonymity: Implications for crime and law enforcement. *Journal of Financial Technology*, 12(3), 121-139.
13. Lindström, T. (2020). **The rise of cryptocurrency in espionage operations.** *Digital Espionage and Global Security Review*, 12(4), 100-115.
14. Lusthaus, J., & Varese, F. (2021). **The regulatory response to crypto-enabled cybercrime: Policy options and challenges.** *International Journal of Cybersecurity*, 8(3), 180-195.
15. Perkins, C. (2020). Cybersecurity and national security threats posed by cryptocurrencies. *Defense Intelligence Journal*, 14(4), 67-78.
16. Tahir, F., Batool, S., & Nadeem, M. (2021). Crypto-Enabled Threats to National Security: A Critical Examination. *International Journal of Cybersecurity Research*, 9(4), 89-104.

Article DOI: 10.52589/AJSSHR-Z73T57O2
DOI URL: https://doi.org/10.52589/AJSSHR-Z73T57O2