

VIRTUAL CURRENCIES: RISKS AND IMPLICATIONS FOR CSDP

*General (ret.) Professor Teodor FRUNZETI, Ph.D**
(Academy of Romanian Scientists, 3 Ilfov, 050044, Bucharest, Romania)
*Alexandru-Cosmin DUMITRU, Ph.D Candidate***

Abstract: *The present paper investigates the influence of virtual currencies on the financial security of the European Union (EU) and the consequences for the Common Security and Defence Policy (CSDP). With the increasing popularity of virtual currencies, the EU's financial ecosystem and defensive capabilities are faced with both opportunities and challenges. The paper examines the relationship between the financial stability required for CSDP efforts and the unpredictable nature of virtual currencies markets, while it explores potential risks linked to the utilization of virtual currencies, such as their capacity to disturb financial stability and enable unlawful actions. It also examines the cybersecurity risks that pose a danger to the European Union's financial infrastructure and the potential impact of hacks on virtual currencies' platforms. Using the perspective of securitization theory, this study examines the level of coordination necessary among European Union member states to effectively handle the intricacies of digital currencies and the importance of flexible policy frameworks. The results emphasize the significance of taking a proactive and cooperative approach to incorporating virtual currencies into the European Union's financial regulatory framework. This will ensure that the operations of the Common Security and Defence Policy (CSDP) remain strong and effective in dealing with rising digital risks.*

Keywords: *Financial security, virtual currencies, financial stability, cybersecurity, CSDP.*

1. Introduction

The Common Security and Defence Policy (CSDP) is the central element of the European Union's (EU) strategic framework. Its purpose is to enhance the EU's collective defence capabilities, address external security challenges, and promote stability inside its geopolitical area. With the increasing presence of digital financial technology, virtual currencies have become a powerful force that has the ability to reshape economic transactions and, consequently, influence the financial foundations of security policy.¹ This paper explores the complex relationship between virtual currencies and the EU's Common Security and Defence Policy (CSDP), analysing how the emergence and integration of virtual currencies could either strengthen or

* Full member of the Academy of Romanian Scientists, President of the Military Sciences Section of the Academy of Romanian Scientists, tfrunzeti@gmail.com.

** National Defence University 'Carol I', Bucharest, Romania, email: a.co.dumitru@gmail.com.

¹ Biscop, Sven, and Richard G. Whitman, eds. "The Routledge Handbook of European Security." Routledge, 2013.

weaken the EU's financial security, which is a fundamental pillar of the CSDP.

In light of the decentralized and transnational character of virtual currencies, this paper aims to examine the various implications these digital assets have for the CSDP in the financial environment. We will analyse the relationship between financial stability and defence policy, examine the hazards linked to virtual currencies usage, and evaluate the cybersecurity concerns that directly impact the EU's financial infrastructure and readiness for defence.

The present study is designed to offer a thorough comprehension of the possible ramifications that virtual currencies could have on the European Union's strategic defence activities. By presenting empirical case studies, this paper will offer insights into fictional scenarios where the volatility and regulatory challenges of virtual currencies have intersected with the objectives of the CSDP, thereby shaping the EU's approach to maintaining financial security in a digital era.

2. Financial stability and CSDP

The interaction between virtual currencies and the financial security of the European Union (EU) poses a complex challenge that affects both economic and security aspects. Given the intricate nature of virtual currencies, it is crucial for the EU to prioritize the maintenance of financial stability, especially in relation to the Common Security and Defence Policy (CSDP). This section explores the complex relationship between financial stability and the effective implementation of CSDP activities, emphasizing the possible influence of virtual currencies on the EU's capacity to achieve its security goals.

The Common Security and Defence Policy (CSDP) functions as the European Union's structure for tackling security concerns, maintaining international stability, and promoting cooperation in security matters. A strong and stable financial environment is crucial for the successful implementation of CSDP programs. Sufficient financial support and the allocation of resources are essential to facilitate the management of crises, peacekeeping operations, and attempts to increase security. If the EU does not have a strong financial base, its ability to deal with security concerns may be weakened.²

The emergence of virtual currencies, such as Bitcoin and Ethereum, has significantly transformed financial transactions and global trade in recent years. Although digital currencies provide advantages such as improved transaction speed and lower expenses, they also bring up new hazards that

² Mölling, Christian, and Sophie-Charlotte Brune. "Funding EU Military Operations: The Athena Mechanism." EU Institute for Security Studies, 2011.

require careful consideration. The inherent instability and lack of clear regulations around virtual currencies have the capacity to disrupt conventional financial systems, affecting the overall stability of the economy and undermining the trust of investors. The potential consequences of virtual currencies on financial security and the Common Security and Defence Policy (CSDP) should be carefully analysed in this context.

The current section employs a multidisciplinary approach, incorporating knowledge from financial studies, securitization theory, and policy research, to examine the interconnected relationship between virtual currencies, financial stability, and CSDP operations. Through the perspective of financial stability, we aim to analyse how the risks and opportunities of virtual currencies are connected to the EU's security goals. By conducting a methodical investigation of this connection, our aim is to clarify the intricate interactions involved and enhance our overall comprehension of the possible obstacles and adjustments needed for a secure and robust security framework in the European Union.

The success of CSDP activities relies on a consistent and secure financial setting. Establishing strong financial bases is essential for supporting peacekeeping missions, crisis management, and measures to increase security. A functional financial ecosystem that is safe supports the timely distribution of resources, promotes collaboration among member states, and enables the EU to effectively achieve its security goals.³

The Common Security and Defence Policy (CSDP) relies on a strong foundation of financial stability, which is essential for effective operations.

The complex network of CSDP activities, which include peacekeeping operations, crisis response, and strengthening collective security, relies on the guarantee of stable financial support. The EU's financial framework allows for efficient and accurate mobilization and allocation of necessary resources.

A stable and predictable financial system is not just a facilitator but a necessary condition for the smooth coordination of CSDP missions. It provides the foundation for the logistical structure, facilitates cooperative efforts among member countries, and simplifies the acquisition of defence capabilities. Financial robustness essentially refers to the EU's ability to exert influence, mitigate security threats, and protect its strategic interests on a global level.

The financial framework underpinning CSDP projects must possess resilience to endure the dynamic challenges of the international arena. The emergence of virtual currencies brings advantages as well as obstacles within this setting. Facilitating swift cross-border transactions with decreased dependence on conventional financial institutions has the potential to improve

³ Fiott, Daniel, ed. "The CSDP: National Perspectives in the Face of Brexit." Egmont Institute, 2018.

the EU's ability to respond to crises. On the other hand, the natural instability and lack of clear regulations around digital currencies could potentially endanger the financial stability that is crucial for the success of the CSDP.

This paper aims to analyse the interdependent connection between the financial infrastructure of the Common Security and Defence Policy (CSDP) and the dynamic nature of virtual currencies markets. The objective is to comprehend how the European Union (EU) may effectively utilize this technological breakthrough to strengthen its defence capabilities while minimizing the accompanying financial hazards.

Although virtual currencies provide advantages such as fast cross-border transactions and lower expenses, their intrinsic instability and absence of conventional governmental supervision present obstacles to financial security. These variables can affect the stability of both national and international financial systems, potentially causing resources to be redirected from CSDP priorities in order to address economic volatility and investor fears.⁴

The theory of securitization, formulated by the Copenhagen School of security studies,⁵ offers a conceptual structure for comprehending the process by which specific concerns are elevated to the status of security concerns. Securitization is the process in which a person or group, by using persuasive language, presents a problem as a serious threat to a specific thing or entity, and this presentation is believed by a relevant audience, thereby providing a reason to take extreme actions to deal with the perceived threat.⁶

When analysing the risks of virtual currencies usage and implications for CSDP from a securitization standpoint, we may break down the process in the following manner:⁷

- **Securitizing Actor:** Within the EU, the securitizing players may include EU officials, regulatory organizations, or financial institutions who express concerns regarding the potential hazards associated with bitcoin usage in relation to financial stability and the Common Security and Defence Policy (CSDP).
- **Referent Object:** The reference objects pertain to the financial stability of the European Union (EU) and the operational efficacy of its Common Security and Defence Policy (CSDP). These assets are

⁴ European Central Bank. (2020). Virtual currencies and central bank digital currencies: challenges ahead, available at https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200731_1~2.en.html, accessed on 10.05.2024.

⁵ Wæver, Ole. "Securitization and Desecuritization." In "On Security," edited by Ronnie D. Lipschutz, 46-86. Columbia University Press, 1995.

⁶ Buzan, Barry, Ole Wæver, and Jaap de Wilde. "Security: A New Framework for Analysis." Lynne Rienner Publishers, 1998.

⁷ Balzacq, Thierry, ed. "Securitization Theory: How Security Problems Emerge and Dissolve." Routledge, 2011.

portrayed as being endangered due to the instability and regulatory obstacles created by virtual currencies.

- **Existential Threat:** The term "threat" in this context refers to a complex situation where virtual currencies have the potential to undermine the integrity of the financial system, enable illegal actions, and disrupt the crucial financial infrastructure necessary for CSDP operations.
- **Speech Act:** The speech act refers to the communication made by the actors responsible for security to the intended audience (which may include EU member states, the general public, or other institutions within the EU) stating that the unregulated use of virtual currencies poses a security concern that needs urgent and extraordinary actions.
 - **Audience:** The approval of the audience is essential for the successful implementation of the securitization strategy. If the EU member states and institutions acknowledge the potential dangers linked to virtual currencies as a valid security issue, they are more inclined to endorse exceptional measures.
 - **Extraordinary measures:** These measures might involve the establishment of strict regulatory frameworks, increased collaboration among member states, and the utilization of advanced technologies to oversee and regulate virtual currencies transactions in order to safeguard the financial security of the European Union and the Common Security and Defence Policy (CSDP).
 - **Emergency Mode and its Impact:** Through the successful securitization of the issue, the EU can activate an emergency mode, enabling swift resource mobilization and the adoption of policies that would typically fall beyond the realm of conventional political procedures.

From a securitization standpoint, the risks of virtual currencies' usage and implications for CSDP can be viewed as a component of a wider discussion that frames the difficulties presented by virtual currencies as matters of security.⁸ This construction justifies the use of extraordinary measures to protect the financial security of the EU and the effectiveness of the CSDP. These measures may involve increased cooperation in regulations and the development of flexible policy frameworks. The efficacy of these solutions, however, depends on the acceptance of the issue as a security threat by the appropriate audience.

⁸ Stritzel, Holger. "Towards a Theory of Securitization: Copenhagen and Beyond." *European Journal of International Relations* 13, no. 3 (2007): 357-383.

By defining virtual currencies as posing security risks, the discussion not only emphasizes the seriousness of the problem but also sets the stage for the validation and implementation of exceptional measures.⁹ These measures could include a range of responses, such as implementing strict regulations, promoting high levels of cooperation between states, and creating flexible policy instruments that can adjust to the rapidly changing digital finance industry.

The success of these securitization actions depends on the acknowledgment and support of the threat narrative by a key audience, which includes EU member states, policymakers, security specialists, and financial regulators. Their agreement is crucial to activate an 'emergency mode' reaction, which would enable the prompt execution of policies and actions that may otherwise be limited by regular political or bureaucratic procedures.

Essentially, the success of the suggested actions to control the influence of virtual currencies on the European Union's financial security and the Common Security and Defence Policy (CSDP) depends on the securitizing strategy being persuasive enough to gain agreement among the main parties involved. If this consensus is reached, it would confirm the acceptance of a thorough and proactive approach to tackle the complex difficulties presented by digital currencies. This would strengthen the EU's ability to withstand any future financial and security shocks.

Virtual currencies have significant price volatility, making them vulnerable to sudden and unanticipated changes in value. The presence of such instability has the potential to erode the trust of investors, disrupt established financial markets, and have an effect on the overall stability of EU member states at a macroeconomic level. As a result, this instability might shift focus away from the security priorities that are specified in CSDP initiatives.¹⁰

Virtual currencies' decentralized structure facilitates pseudonymous transactions, which might potentially be exploited for money laundering, tax evasion, and terrorism financing.¹¹ The lack of comprehensive regulatory frameworks can create an environment that is favourable for illegal financial activity, posing a threat to both financial stability and the ability to properly fund CSDP operations.¹²

⁹ Conti, Mauro, et al. "A Survey on Security and Privacy Issues of Bitcoin." *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, Fourthquarter 2018.

¹⁰ Juskauskas, M., & Kriauciuniene, L. (2020). Bitcoin and Its Effect on Financial Stability. In *Proceedings of the 34th International Business Information Management Association (IBIMA) Conference*. [PDF](<https://ibima.org/wp-content/uploads/2020/07/69-MJ.pdf>)

¹¹ European Union Agency for Cybersecurity (ENISA). (2020). *Threat Landscape for Cryptocurrencies*. [PDF], available at <https://www.enisa.europa.eu/publications/threat-landscape-for-cryptocurrencies>, accessed on 11.05.2024.

¹² Goodhart, C., & O'Hara, M. (2020). *Cryptocurrencies, Fintech, and Financial Regulation*. In *Cryptocurrencies and Blockchain Technology* (pp. 123-143). Palgrave Macmillan, Cham.

3. Cybersecurity concerns: a threat to financial infrastructure

Virtual currencies depend on digital platforms for the purposes of trading, storing, and conducting transactions. These systems are vulnerable to cyberattacks, such as hacking, phishing, and distributed denial-of-service (DDoS) attacks.¹³ Effective breaches can result in monetary losses, compromised user credentials, and market disturbances, affecting the broader financial ecosystem.¹⁴

An intrusion into the infrastructure of bitcoin can lead to far-reaching ramifications, impacting not only the virtual currencies market but also the wider financial system.¹⁵ As virtual currencies grow more intertwined with conventional financial systems, a significant attack resulting in big losses might have a ripple effect, causing broader financial instability. This, in turn, could hinder the European Union's capacity to finance CSDP operations and peacekeeping efforts.¹⁶

The integration of virtual currencies in the financial ecosystem has led to an increase in concerns over cybersecurity, which directly jeopardizes the stability and integrity of the financial infrastructure. Virtual currencies rely on a technological infrastructure consisting of trading platforms, wallets, and blockchain networks, all of which are vulnerable to cybercriminals due to their digital nature.

The infrastructure of virtual currencies is highly vulnerable to a wide range of cyber threats. Trading platforms are susceptible to security breaches, which can result in the theft of digital assets. Cryptographic wallets are susceptible to hacking, leading to unauthorized transactions. Despite its reputation for security, even blockchain technology is susceptible to advanced cyberattacks, such as those targeting smart contract flaws or consensus mechanisms.

The repercussions of these cybersecurity concerns might extend widely. Effective breaches have the potential to result in significant monetary damages and erode trust in virtual currencies. User account breaches and trading activity disruptions can result in market instability, potentially impacting the wider financial system.

¹³ European Union Agency for Cybersecurity (ENISA). (2020). Threat Landscape for Cryptocurrencies. [PDF], available at <https://www.enisa.europa.eu/publications/threat-landscape-for-cryptocurrencies>.

¹⁴ Vasek, M., Thornton, M., & Moore, T. (2016). Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 765-777).

¹⁵ World Economic Forum. (2020). Advancing Cyber Resilience in the Financial System: Addressing Cyber Risk in Supply Chains and Third-Party Providers. [PDF](http://www3.weforum.org/docs/WEF_Advancing_Cyber_Resilience_Financial_System_2020.pdf)

¹⁶ Shafiee, S., & Anuar, N. B. (2020). Cybersecurity Threats in the Blockchain Ecosystem: A Systematic Review. Journal of King Saud University-Computer and Information Sciences.

The presence of cybersecurity threats in the virtual currencies domain poses a substantial systemic risk, which is a matter of great concern. As virtual currencies become increasingly interconnected into conventional financial systems, the potential consequences of hacking expand. A significant attack might rapidly propagate across financial networks, causing huge losses and resulting in wider market disruptions.

The EU is particularly concerned about the systemic repercussions of cyberattacks, as they have the ability to disrupt the finance and operational readiness of CSDP missions. If a cybersecurity incident were to occur, it may potentially jeopardize the capacity to promptly address international crises or provide assistance to peacekeeping and security operations due to the abrupt depletion or immobilization of financial resources.

Given these potential dangers, it is imperative for the European Union to give utmost importance to the creation and execution of strong cybersecurity protocols that can effectively safeguard against the distinct hazards presented by the virtual currencies system. This will contribute to guaranteeing the persistent stability of the financial system and the sustained effectiveness of the CSDP in a fast-changing digital environment.

4. Case studies: intersections of virtual currencies risks and CSDP objectives

Virtual currencies encompass more than simply financial and technological aspects; they also involve the intersection of real-world events with policy and security concerns.¹⁷ In this section, two case studies are presented to shed light on the intricate connection between the emergence of virtual currencies and the goals of the European Union's Common Security and Defence Policy (CSDP). These case studies offer concrete proof of the difficulties and potential advantages that digital currencies present to the European Union's financial security and defence system.

Each case study is carefully chosen to highlight a specific element of the relationship between virtual currencies and the CSDP. The scenarios they investigate encompass a wide range of possibilities, including the potential financial instability caused by swings in the bitcoin market, as well as the utilization of digital currencies to finance illicit operations that harm regional security. Moreover, the case studies analyse specific situations in which cyber threats aimed at virtual currencies infrastructure have had broader consequences for the European Union's financial system and its capacity to maintain Common Security and Defence Policy (CSDP) activities.

This section seeks to provide practical insights into the consequences of virtual currencies in the context of the EU's security and defence policy,

¹⁷ Casey, Michael J., and Paul Vigna. "The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order." St. Martin's Press, 2015.

using real-world examples. Through the examination of these cases, we can gain valuable knowledge on the actions required to strengthen the European Union's readiness and ability to address the complex issues posed by the digital currency revolution.

4.1 Case study 1: financial instability and regional security

Consider a theoretical situation where a prominent virtual currencies exchange, which plays a crucial role in facilitating a substantial amount of virtual currencies trade in the European Union, becomes the victim of a big cyberattack. The cyberattack leads to the breach of user accounts, the theft of significant amounts of virtual currencies, and the disclosure of sensitive personal information.

The cyberattack instigates fear and anxiety among bitcoin traders and investors, resulting in a swift depreciation of virtual currencies values. The compromised exchange halts its operations, resulting in a cessation of trading activities and impeding users' access to their funds. This incident not only undermines confidence in the specific exchange being attacked, but also initiates a broader decline in the value of different virtual currencies, impacting their market prices on a global scale.

Broader Financial System Impact: The extensive instability in the virtual currencies market raises concerns regarding the potential spread of negative impacts to the wider financial system. Given that institutional investors and financial organizations include virtual currencies in their portfolios, any significant decrease in their value may result in financial losses for these companies. Moreover, the interdependence of financial markets implies that pessimistic feelings originating from the virtual currencies market could impact conventional financial assets, resulting in market instability and investor unease.

CSDP Implications: The possible consequences of the cyberattack extend beyond the impact on financial markets. The EU's ability to finance and carry out CSDP programs may be hampered as its financial resources are challenged by economic volatility. EU member states may be required to reallocate resources from security measures to tackle economic issues, so constraining their ability to participate fully in conflict prevention, crisis management, and peacekeeping operations.

The European Union is confronted with the task of preserving financial stability while dealing with the repercussions of the cyberattack. It is imperative that member states, regulatory organizations, and financial institutions work together in a collaborative manner to minimize the negative implications. Simultaneously, the European Union must evaluate the possible consequences on its security obligations and adapt its Common Security and Defence Policy (CSDP) policies accordingly.

Proposed policy suggestions:

- Implement enhanced cybersecurity measures: Reinforce the security standards for bitcoin exchanges and platforms to effectively prevent and address intrusions.
- Develop resilience plans to mitigate any cyber-induced disruptions in the financial market and their impact on security activities.
- Enhance coordination among financial regulators, cybersecurity agencies, and CSDP stakeholders to effectively manage the linked risks.

The hypothetical cyberattack demonstrates the complex interaction of technical vulnerabilities, financial instability, and security concerns. As the European Union deals with the consequences of such an attack, the task of effectively managing both financial security and security objectives becomes a crucial concern. Flexible regulations and cooperative methods are necessary to prevent virtual currencies-related occurrences from undermining the EU's ability to handle security crises within the CSDP framework.

This case study illustrates the potential consequences of a cybersecurity attack in virtual currencies infrastructure on financial stability, which in turn can impact the EU's capacity to effectively address security crises within the CSDP framework. This emphasizes the necessity for taking proactive steps to handle the financial and security concerns that arise from the ever-changing realm of cryptocurrencies.

4.2 Case study 2: financial instability, economic crisis, and CSD engagement

Consider a fictional country called NationX, where there is a significant reliance on virtual currencies trading for generating income. The trading of virtual currencies has emerged as a large contributor to the gross domestic product (GDP) of NationX. Additionally, the government of NationX is able to generate significant tax revenue from activities related to virtual currencies. The country also actively engages in international security cooperation, including making contributions to Common Security and Defence Policy (CSDP) projects.

The impact of virtual currencies volatility on the economy: the virtual currencies market experiences an abrupt and significant decline, resulting in enormous financial losses for both individual investors and institutional stakeholders in NationX. The high volatility of virtual currencies trading leads to a sharp decline in revenue, resulting in a substantial budget deficit for the government. Consequently, the national currency experiences devaluation, inflation escalates, and unemployment rates surge as a consequence of reduced economic activity.

The impact of economic instability on engagement in the Common Security and Defence Policy (CSDP): NationX's ability to deploy resources for its security commitments, including contributions to CSDP efforts, is weakened by economic volatility. The government's limited fiscal resources

restrict its capacity to allocate funds towards defence, peacekeeping operations, and security cooperation. Furthermore, the public's attention transitions from security concerns to economic anxieties, resulting in diminished support and attention for CSDP initiatives.

NationX's diminished financial capacity results in a decrease in its involvement in CSDP operations and peacekeeping endeavours, which has implications for lower engagement and compromised security. The diminished involvement of the nation has a negative influence on the overall efficacy of CSDP projects, as there are fewer resources allocated for collaborative security measures. This might potentially impact NationX's position inside the EU security framework and its ability to shape decision-making procedures.

Geopolitical Consequences: The repercussions of NationX's economic instability transcend its national boundaries. Reduced commerce, capital flight, and greater security concerns may lead to economic spillover consequences in neighbouring nations. If NationX is unable to properly contribute owing to its economic issues, it could jeopardize the coordinated regional response to security threats, which is facilitated through the EU and CSDP.

Mitigation Strategies:

- **Revenue Diversification:** Advocate for NationX to expand its revenue sources beyond virtual currencies, thereby enhancing economic stability and reducing vulnerability to market fluctuations.
- **Create contingency funding** to minimize the effects of unforeseen economic disruptions on security-related operations, ensuring uninterrupted involvement in CSDP.
- **EU Solidarity:** Utilize EU resources to provide assistance to NationX during periods of economic turmoil, enhancing the nation's capacity to engage in security collaboration endeavours.

This case study demonstrates the susceptibility of nations that could largely depend on virtual currencies trading to economic volatility, which might subsequently impede their ability to successfully contribute to CSDP operations. The interaction between economic stability and security obligations emphasizes the necessity for well-balanced policy measures that take into consideration both financial and security factors within the EU's comprehensive security framework.

This example demonstrates how the unpredictable fluctuations in virtual currencies prices can result in economic instability in a country, which can in turn hinder its capacity to successfully participate in Common Security and Defence Policy (CSDP) operations. This statement highlights the interdependence of economic and security issues and emphasizes the significance of governmental actions that tackle both aspects.

Conclusions

In conclusion, the intersection of virtual currencies and the Common Security and Defence Policy (CSDP) of the European Union poses a multifaceted set of concerns and opportunities. The rapid development of virtual currencies has substantial consequences for the financial stability of the European Union, requiring a meticulous examination of the dangers and advantages linked to their acceptance.

The instability and absence of comprehensive regulation in the virtual currencies markets jeopardize the financial stability that is crucial for the operational effectiveness of CSDP efforts. The possibility of virtual currencies being utilized for illegal activities adds complexity to the security situation, necessitating stronger legislative frameworks and international collaboration to reduce these threats. Moreover, the cybersecurity risks linked to the infrastructure of digital currency could have far-reaching consequences, possibly impacting the wider financial system and jeopardizing the European Union's capacity to finance and carry out Common Security and Defence Policy (CSDP) missions.

In addition to the difficulties they provide, virtual currencies also have potential benefits, such as enabling fast and transparent cross-border financial transactions. The European Union must thus find a middle ground between embracing the advantages of technology advancement and tackling the security vulnerabilities inherent in the digital financial sphere.

In order to preserve the integrity and effectiveness of the CSDP, it is crucial for the EU to formulate a unified approach that combines financial security issues with defence policy. The policy should incorporate strong cybersecurity protocols, a unified regulatory approach to digital currencies, and a framework for global cooperation to tackle the worldwide nature of virtual currencies marketplaces.

The EU's capacity to adjust its policies and regulations to the changing environment of virtual currencies will be essential in protecting its financial infrastructure and ensuring the stability necessary for the effective achievement of its security and defence goals.



BIBLIOGRAPHY

- BALZACQ, T., ed. "Securitization Theory: How Security Problems Emerge and Dissolve." Routledge, 2011.
- BISCOP, S., and Richard G. Whitman, eds. "The Routledge Handbook of European Security." Routledge, 2013.

- BUZAN, B., Ole Wæver, and Jaap de Wilde. "Security: A New Framework for Analysis." Lynne Rienner Publishers, 1998.
- CASEY, M. J., and Paul Vigna. "The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order." St. Martin's Press, 2015.
- CONTI, M., et al. "A Survey on Security and Privacy Issues of Bitcoin." IEEE Communications Surveys & Tutorials, vol. 20, no. 4, Fourthquarter 2018.
- FIOTT, D., ed. "The CSDP: National Perspectives in the Face of Brexit." Egmont Institute, 2018.
- GOODHART, C., & O'Hara, M. (2020). Cryptocurrencies, Fintech, and Financial Regulation. In Cryptocurrencies and Blockchain Technology (pp. 123-143). Palgrave Macmillan, Cham.
- JUSKAUSKAS, M., & Kriauciuniene, L. (2020). Bitcoin and Its Effect on Financial Stability. In Proceedings of the 34th International Business Information Management Association (IBIMA) Conference. [PDF], available at (<https://ibima.org/wp-content/uploads/2020/07/69-MJ.pdf>)
- MÖLLING, C., and Sophie-Charlotte Brune. "Funding EU Military Operations: The Athena Mechanism." EU Institute for Security Studies, 2011.
- SHAFIEE, S., & Anuar, N. B. (2020). Cybersecurity Threats in the Blockchain Ecosystem: A Systematic Review. Journal of King Saud University-Computer and Information Sciences.
- STRITZEL, H., "Towards a Theory of Securitization: Copenhagen and Beyond." European Journal of International Relations 13, no. 3 (2007): 357-383.
- VASEK, M., Thornton, M., & Moore, T. (2016). Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 765-777).
- WÆVER, O.. "Securitization and Desecuritization." In "On Security," edited by Ronnie D. Lipschutz, 46-86. Columbia University Press, 1995.
- European Central Bank. (2020). Virtual currencies and central bank digital currencies: challenges ahead, available at https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200731_1~2.en.html.
- European Union Agency for Cybersecurity (ENISA). (2020). Threat Landscape for Cryptocurrencies. [PDF], available at <https://www.enisa.europa.eu/publications/threat-landscape-for-cryptocurrencies>.