



PAYMENT TRANSACTIONS AS CRITICAL INFRASTRUCTURE

Die CISS Munich Working Papers spiegeln die Meinung der jeweiligen Autorinnen und Autoren wider. Sie stellen nicht die Meinung der Bundeswehr oder der Universität der Bundeswehr München dar. Die Reihe wird vom Center for Intelligence and Security Studies (CISS) an der Universität der Bundeswehr München herausgegeben. Die Working Paper Serie am CISS befasst sich mit aktuellen, historischen und strategischen Fragestellungen in den Bereichen Sicherheit und Intelligence, Militär und Technologie, Politik und gesellschaftlichem Wandel. Die Reihe ordnet Entwicklungen in diesen Bereichen ein, liefert Analysen und Denkanstöße und skizziert Handlungsoptionen.

Weitere Ausgaben: <https://www.unibw.de/ciss/working-paper-series>

ISSN 3053-7800

Executive Summary

The need to securitize a state's critical infrastructure has become an unquestionable necessity due to its continued targeting by hostile actors and its vitality to society's functioning. One of the critical infrastructure sectors not normally associated with securitization but whose targeting has increased is the financial sector, particularly payment transactions. Naturally, payment transactions are seen as a mundane part of daily life – but an increase in their targeting by hostile actors and their interconnectedness to other vital areas of society have exposed their importance in states' broader critical infrastructure. This paper examines the securitization of payment transactions as a form of critical infrastructure, assessing existing protection measures and, considering current evidence, exploring potential strategies to further enhance their operational resilience.

By Alessia Noschese and Lucas Obregón

State-sponsored cyberattacks targeting financial institutions, rising geopolitical tensions – particularly Russia's ongoing war of aggression against Ukraine – and assaults on cross-border transactions, combined with the growing digitalization and interconnectedness of the global economy, have made payment transactions a crucial component of states' critical infrastructure (CI). As essential elements of both the financial system and CI, payment transactions have become central to exposing new vulnerabilities and threats that modern CIs confront. Indeed, failures in payment transaction systems can generate societal insecurity while simultaneously eroding citizens' trust in the financial system and in state institutions.

This paper examines the need for payment transactions to be framed as security issue, a process security scholars calls "securitization". We deploy such a securitization perspective to emphasize how it enables a broader understanding of payment transactions: one that reveals their critical importance to the functioning of modern societies and the preservation of the rules-based order.

To develop a securitization perspective on payment transactions, we will first embed the understanding of CI as part of a security

framework and explain how payment transactions have become part of CI. This is followed by a discussion of the effects of payment disruptions and a deep dive into the type of threats payment transactions nowadays face. A case study based in Sweden about the potential fallout of payment disruptions and the lessons learned – with a focus on most recent legal responses in the European Union – follows. Potential solutions and future threats to Europe conclude the paper.

Security and Critical Infrastructure

Security has traditionally been understood from a military perspective, focusing on military threats and prioritizing military solutions. Over the years, however, this traditional emphasis has been both broadened and deepened to include other sectors of society usually associated with civilian life. In fact, contemporary security challenges faced by governments increasingly involve the exploitation of economic, technological, and societal vulnerabilities. CI is one such vulnerable sector, and the financial system, as a central pillar of CI, has been a primary target.

Public administration most affected of all sectors in the EU.

IT security incidents in the EU by sector

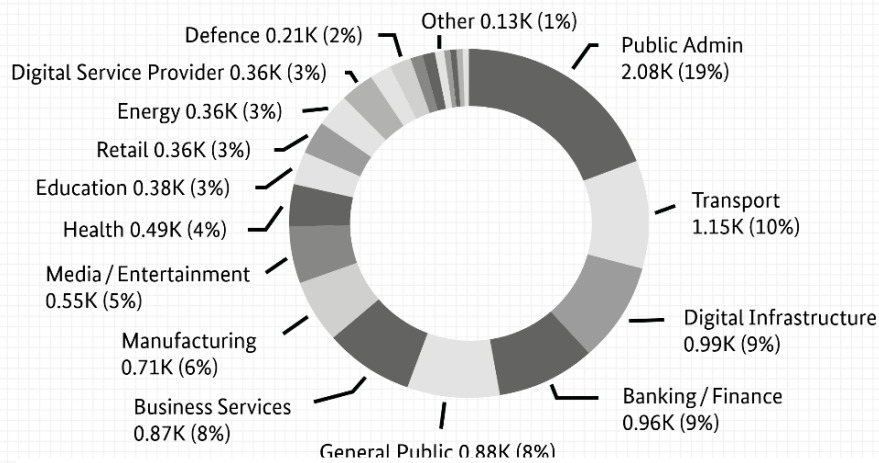


Figure 1: Sectors of CI (adapted from Federal Office for Information Security – BSI 2024)

Traditionally, CI has been understood to include physical assets such as bridges, highways, railways, and air and seaports, mainly in sectors like transportation and energy.¹ In today's world, however, the rapid digitalization of services has greatly expanded the range of vulnerabilities. This shift allows hostile actors to disrupt a nation's core functions at relatively low cost, all while avoiding full-scale military confrontation and evading accountability. The risks that emerge from these vulnerabilities are commonly described as hybrid threats.

NATO, for instance, defines hybridity² as the use of different but coordinated measures that exploit the vulnerabilities of a rival state. When applied simultaneously, these tools allow a hostile actor to pursue strategic objectives that can directly harm the target state. A defining feature of hybridity is its ambiguity, which blurs the thresholds for detection and response. Actors use this obscurity to avoid attribution and complicate the ability of targeted states to respond effectively. While hybrid threats are not a completely new concept or strategy, they

have become increasingly significant in the 21st century due to rising geopolitical tensions and their growing use in international conflicts.

In response to emerging threats and challenges, the definition, understanding, and protection of CI have evolved over time. As non-physical sectors increasingly became targets and hybrid warfare grew into a common tool of hostile actors, the concept of security expanded to encompass CI as well. This shift did not happen overnight; rather, it developed as a direct response to the rising frequency of hybrid attacks and the growing vulnerabilities of digitized CI. EU legislation in 2008³, for example, first emphasized the protection of CI, but only in two sectors: energy and transport. By 2022, however, acts of sabotage – most notably the Nord Stream pipeline attacks – highlighted the need to broaden this scope. The EU consequently expanded CI to include nine additional sectors, among them banking and financial infrastructure. In practice, this expansion, along with new legislation to safeguard CI,

¹ Moteff, J./Parfomak, P. (2004): Critical Infrastructure and Key Assets: Definition and Identification. Available at: <https://sgp.fas.org/crs/RL32631.pdf> (18.9.25).

² https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en (27.10.25).

³ [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662604/EPRS_BRI\(2021\)662604_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662604/EPRS_BRI(2021)662604_EN.pdf) (27.10.25).

represents a countermeasure to the growing use of hybrid warfare.

Payment Transactions as Critical Infrastructure in the European Union

The European Union currently classifies as CI those entities essential for maintaining vital societal functions, including the financial sector. The latter, however, was not always recognized as CI within the EU. It gained this status in 2016 under the Network and Information Security (NIS) Directive, a decision driven by the growing importance and pervasiveness of the services the sector provides. Payment transactions are a core component of this sector, forming the foundation of a well-functioning society. As these transactions increasingly move to digital platforms, become more interconnected, and depend on one another, they require a correspondingly higher degree of operational resilience.

Member State have at times been followed by hacktivist activity targeting financial institutions and other critical sectors within that country. Strikingly, most of the observed DDoS attacks were directed at European credit institutions, especially banks.

Threats: Actors and Means

The ENISA report also classifies three main categories of threat actors: state-nexus actors, hacktivists, and cybercrime actors. State-nexus actors target mostly governments and organizations and focus on espionage and intelligence gathering, often conducting long-term, highly targeted operations. Hacktivists instead engage in cyberattacks as a means of political or social activism. Their skill levels and capabilities vary widely, and in some cases, they may be used by state-linked actors to support influence campaigns or other cyber operations. On the other hand, cybercriminals operate with

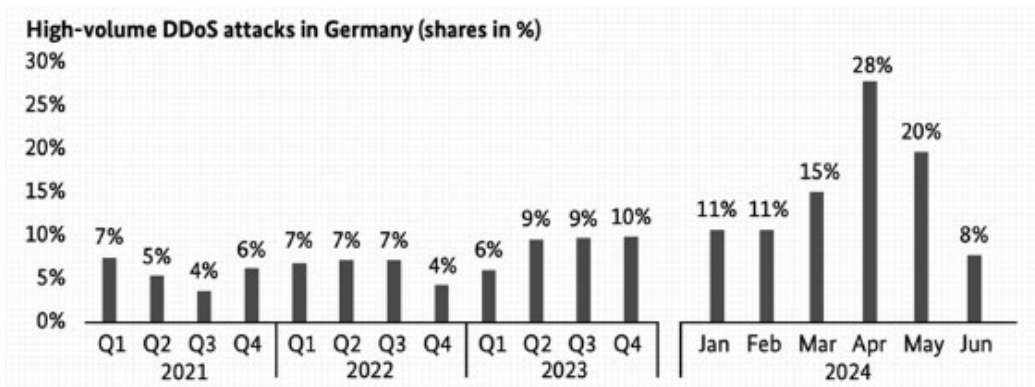


Figure 2: DDoS attacks in Germany 2021-mid 2024 (adapted from ENISA 2025)

A recent report by the European Network and Information Security Agency (ENISA)⁴, conducted between January 2023 and June 2024, underscores this point. The report identifies Distributed Denial-of-Service (DDoS) attacks as among the most prevalent cyber threats and shows how spikes in such attacks often correlate with geopolitical developments—particularly those linked to the Middle East and Russia’s invasion of Ukraine. For example, public declarations of support for Ukraine by an EU

the goal of financial gain, carrying out attacks that are often indiscriminate and opportunistic.

Threat actors have a diverse arsenal of attacks at their disposal. Distributed Denial-of-Service (DDoS) attacks are among the most prevalent cyber threats, primarily aimed at overwhelming a service or network infrastructure by exhausting its resources. The January 2023 Killnet attack serves as an example. Killnet, a pro-

⁴ https://www.enisa.europa.eu/sites/default/files/2025-02/Finance_TL_2024_Final.pdf (27.10.25).

Moscow hacker group, used DDoS attacks against German airports, the financial sector, and federal and state government websites, citing Germany's decision to send Leopard 2 tanks to Ukraine as the rationale.

Beyond DDoS attacks, another significant threat is posed by data breaches—attacks aimed at stealing confidential data. According to the ENISA report, the finance sector is a frequent target for data-related incidents due to the valuable personal and corporate information it handles, making it attractive to threat actors who exploit it for extortion or financial gain. These threats often involve supply chain attacks and social engineering. Widely known is the June 2021 attack by APT 28, a hacking group tied to Russian military intelligence, which targeted German CIs including the banking system. As was the case in the Killnet attack, APT 28's attacks have so far focused on targets supporting Ukraine. APT stands for Advanced Persistent Threats and refers to sustained attacks, often carried out by groups, that infiltrate networks or systems in an undetected manner over a prolonged period. They are carefully planned, fly under the radar, and require a higher level of sophistication compared to other attacks. This was not the first attack by APT 28 either: the group was behind the 2015 cyber-attack on the German Bundestag that targeted the German parliament's information database, stealing data and affecting the systems' ability to operate. APT 28 was also behind the 2023 targeted hackings aimed at the SPD party, again aimed at stealing data, but expanding their targets to include defense, IT, and aerospace companies. Notably, APT attacks tend to not have a monetary goal—APT 28 in particular has a long history of carrying out operations against defense ministries, installations, and NATO nation defense sectors, signaling strategic and geopolitical interests rather

than monetary goals as the main objectives of the group.

There tends to be a focus around APT 28 specifically because of the group's ties to the GRU and their history targeting the NATO defense sector, but the list of APT groups present in Germany is extensive. The BSI refers to 30 currently active APT groups operating in Germany, with a majority of them targeting CI.⁵ However, an APT attack's secretive nature makes detection and attribution difficult, meaning the number of APT groups currently active in Germany is likely higher.

Nevertheless, the nature of threats expands beyond DDoS and data breach attacks to social engineering tactics, fraud, ransomware, malware, and attacks on supply chains.

Social engineering attacks exploit human error by manipulating individuals into revealing sensitive information or granting access to services. The most prevalent form of social engineering is phishing, which is primarily used to commit fraud. The latter represents a smaller proportion of incidents compared to other attack types, likely because financial institutions may refrain from disclosing fraud cases due to concerns about their reputation or regulatory obligations. Furthermore, fraud is often a by-product of other cyber incidents, which are generally reported under their main attack methods rather than categorized as fraud. To better understand the other types of attacks:

- Ransomware is a type of attack that locks a victim's sensitive data or device, threatening to withhold access or exposing the data unless a ransom is paid to the attacker.
- Malware refers to any software or firmware designed to carry out unauthorized actions that compromise a system's confidentiality, integrity, or availability.

⁵ [https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-](https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen_node.html)

[Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen_node.html](https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen_node.html) (27.10.25).

- Attacks to the supply chain aim at service providers to infiltrate financial institutions bypassing security measures and spreading malware or gathering intelligence.

enables a level of differentiation that traditional security approaches often lack – potentially overlooking distinct cyberattack characteristics or failing to account for the diversity among hostile actors. Indeed, this framework allows state and security actors to move beyond viewing threats as a monolithic bloc, recognizing instead that hostile actors are complex and varied. Depending on their loyalties,

Table 1 presents the means used by threat actors and the aims they seek to achieve.

Threat actors	Target	Threats	Goal
State-nexus actors	<ul style="list-style-type: none"> • Governments • Organisations • Crypto-asset service providers • Financial Institutions 	<ul style="list-style-type: none"> • Cyber espionage • Intelligence gathering • Sabotage • Financial theft 	<ul style="list-style-type: none"> • Collect sensitive information – crucial for both economic and political strategies
Hacktivists	<ul style="list-style-type: none"> • Financial institutions • Public administration • Energy sector • Transport sector 	<ul style="list-style-type: none"> • Distributed denial-of-service (DDoS) attacks • Ransomware payloads 	<ul style="list-style-type: none"> • Cause operational disruption for ideological reasons
Cybercrime actors	<ul style="list-style-type: none"> • Indiscriminate 	<ul style="list-style-type: none"> • Social engineering • Fraud • Scam • Ransomware 	<ul style="list-style-type: none"> • Financial gain

Table 1: The means used by threat actors and their objectives

These threats can compromise payment transactions by exploiting vulnerabilities in payment systems, users, or underlying infrastructure. They can potentially create a domino effect that spreads to other sectors of CI, destabilizing the market, eroding trust in national institutions, disrupting military and defense operations, and creating logistical bottlenecks in service providers and the transportation system. Indeed, attacking a state’s payment transaction system can destabilize an entire society and has proven to be a common tool in geopolitical competition.⁶

motivations, and capabilities, these actors behave differently and therefore require tailored countermeasures. However, cyber threats are not the sole form of risk that could impact or target the financial sector and payment transactions. Electronic payments are completely dependent on electricity, therefore natural disasters such as hurricanes or earthquakes can result in damages to physical infrastructures, leading to power outages and disrupted network connectivity, which in turn hampers the functionality of electronic payment systems.

The different types of actors, along with their methods and targets, highlight the need to securitize payment transactions. When effectively applied, the securitization framework

⁶ https://fastpayments.worldbank.org/sites/default/files/2025-02/Cybersecurity_Focus_Note_Feb_19_Final.pdf (27.10.25)

Sweden: A Model for Understanding Payment System Risks

As countries move toward reducing cash usage in favor of electronic payment systems, sectors become increasingly dependent on this infrastructure, amplifying the potential cascading effects of payment disruptions. Sweden serves as a relevant example, having implemented policies to reduce cash usage to curb tax evasion and limit counterfeit currency. A study conducted by Linköping University⁷ tries to predict the broader impact of payment disruptions, particularly in Sweden, where approximately 90% of transactions were processed via card at the time of the research. This study points to the lack of a comprehensive framework for understanding the interconnections between CIs and seeks to explore the challenges posed by disruptions to payment systems, with a focus on their broader impact on infrastructure resilience.

The study theorizes that when customers are unable to make card payments at food stores, restaurants, public transportation, taxis, and gas stations, most sales could come to a sudden halt. ATMs would quickly run out of cash, causing food stores to face a range of problems, from complete cessation of sales for non-essential items to hoarding and shortages of critical products. Unmanned gas stations may experience a significant drop in sales, while manned stations could face hoarding. Small businesses, such as local food stores, gas stations, or freight companies, could be driven to the brink of bankruptcy with just one or two weeks of disrupted sales

Alternatives like SWISH, a mobile payment system developed by six major Swedish banks, offer peer-to-peer payments and facilitate online and in-store transactions. Another alternative involves trust-based payment options, such as receiving goods immediately and paying later.

⁷ van Laere, J./Berggren, P. Gustavsson, P./Ibrahim, O./Johansson, B./Larsson, A./Lindqvister, T./Olson, L./Wiberg, C. (2017): Challenges for Critical Infrastructure Resilience: Cascading Effects of Payment

However, this is more feasible in rural areas, where small business owners, such as gas station operators, are familiar with most of their customers. The location of the disruption also impacts food supply, as rural areas tend to have larger reserves than urban areas. Additionally, the timing of disruptions plays a crucial role, as disruptions during high-traffic days could lead to more severe consequences.

Economically vulnerable groups are disproportionately affected by payment disruptions, as they often lack financial reserves and struggle to access alternative payment methods, relying heavily on social care for essential goods. Furthermore, trust and security concerns arise during these disruptions, with resource scarcity fueling hoarding, conflicts, and a heightened risk of crime, particularly as cash transactions become more prevalent. Social media also plays a significant role, as digital platforms can exacerbate financial instability, making careful communication essential to prevent hoarding and security risks. Lastly, the involvement of numerous diverse actors in payment and goods distribution chains complicates the process of establishing trustworthy relationships, identifying problems, and managing dependencies, especially with dominant players like VISA and MASTERCARD. This complexity makes it harder to coordinate mitigation efforts and communicate effectively during disruptions.

When it comes to Germany, cash remains the most widely used payment method whereas mobile payments via smartphones or smartwatches have seen a significant rise, tripling between 2021 and 2023. “Cash of the Future,” a study by the Bundesbank, forecasts three potential trajectories for cash usage in Germany by 2037: a highly digital payment system where cash accounts for only 15% of transactions, a resurgence in cash use driven by its perceived autonomy and security, and a gradual decline

System Disruptions, in: Proceedings of the International Conference on Information Systems for Crisis Response and Management 14: 282-291.

in cash reliance, with certain demographic groups continuing to use it.⁸ In two of these scenarios, cash usage, access, and acceptance would decrease substantially. Yet, the need to ensure continued access to and acceptance of cash, the main reason being the ability of cash to foster trust during difficult times and help stabilize society is highlighted in the Sixth Deutsche Bundesbank Cash Symposium and reinforced by the study conducted by Linköping University.

As the number of risks and hostile actors increases – emboldened by the current geopolitical scenario – appropriate solutions must be swiftly implemented to mitigate the consequences of payment disruptions. Sweden’s experience highlights the vulnerabilities that arise when a society becomes heavily reliant on digital payment systems. The Linköping University study demonstrates how even short-term disruptions can have cascading effects across critical sectors, from food supply and transportation to small business viability. One key lesson is the enduring value of cash as a resilient fallback option – particularly in emergencies – underscoring the importance of maintaining access to physical currency. Additionally, Sweden’s case reveals the broader security implications of payment systems and the need for integrated frameworks that account for both technological and social dimensions, especially in safeguarding economically vulnerable groups and maintaining public trust during crises. Moreover, the study illustrates that, in some instances, reverting to cash may be the most effective countermeasure, despite the well-known limitations and vulnerabilities that accompany its use.

Beyond current examples, historical lessons also underscore the essential role of the financial sector in maintaining societal stability. The 1930’s financial crisis, for example, demonstrated how the erosion of public trust in

financial institutions can trigger widespread collapse. History does not always repeat itself – but this is still a valuable example that provides us a glimpse of what might happen when people do not have trust in public institutions. Trust is not just a financial asset – it is a foundational element of national security. Sweden’s case, combined with past financial shocks, highlights the critical need to integrate payment systems into broader security frameworks, where trust, accessibility, and preparedness are central pillars of resilience.

Lessons learned: Legislative Efforts

One of the main results from these events and the vulnerabilities, is the increasing number and depth of regulations introduced in recent years – at both European and national levels. Currently, the Digital Operational Resilience Act (DORA) directly applies across all EU member states starting January 17, 2025, without requiring national transposition. Under DORA, financial entities are supervised by national authorities, such as BaFin (Federal Financial Supervisory Authority) and Bundesbank in Germany, along with EU authorities like the ECB, ESA, and ENISA. The act mandates risk management frameworks, resilience testing, and incident management procedures, and major incidents must be reported to authorities for impact assessment. In Germany, payment service providers already comply with similar obligations under the German Payment Services Supervision Act (Zahlungsdiensteaufsichtsgesetz – ZAG). DORA broadens and standardizes ICT (Information and Communication Technology) incident reporting across all financial entities.

Another key directive is the Critical Entities Resilience (CER), which mandates member states to adopt national resilience strategies and conduct risk assessments to identify critical entities providing essential services, including those in banking and financial infrastructure.

⁸ <https://www.bundesbank.de/en/publications/reports/studies/cash-of-the-future-941484> (27.10.25).

Member states must identify critical entities by July 17, 2026, and develop risk assessment frameworks and national resilience strategies. In Germany, the KRITIS Umbrella Act transposes the CER Directive into national law, establishing a comprehensive framework for identifying CI, monitoring disruptions, conducting state-led risk analyses, and enforcing minimum resilience requirements for operators. These regulations, adopted as responses to recent events discussed above, only highlight the growing need to securitize CI.

Conclusion: Possible Future Scenarios

Looking ahead, beyond Russia other looming threats expand on the necessity of adopting measures to prevent payment transaction disruptions. Terrorist groups such as Al-Qaeda and ISIS have already threatened and attempted to develop cyber capabilities to attack European financial sectors,⁹ and their previous concentration on attacking Europe indicates there is still a risk of Jihadist terrorist attacks across Europe, despite these threats not yet coming to fruition or terrorist groups' cyber capabilities yet materializing. Actors such as Hezbollah have also carried out cyber-espionage, cyber-sabotage, and influence activities in Europe, and their history of terror against European targets implies an attack on the financial sector is not off the table.¹⁰ Hezbollah's status as an Iranian proxy also heightens the risks of an attack to European financial sectors, with experts warning of potential DDoS attacks against financial institutions in countries allied to the United States and Saudi Arabia.¹¹ This is compounded by the EU's decision in 2022 to adopt restrictive measures towards Iran due to their continued military support to Russia. Indeed, the alliance between Iran and Russia does not go to the extent as Russia's alliance

with North Korea; Iran is yet to send troops to fight Ukraine. However, Iran's continued support to Moscow and the existing evidence of cyberattacks perpetrated by Iran and its proxies against Europe means there is a possibility of cyberattacks being perpetrated by Iran or its proxies against European targets, including CI.

Another potential threat is North Korea. Although intelligence of payment disruption by North Korean actors has so far been unreported, the recent alliance between North Korea and Russia following Russia's invasion of Ukraine might signal an increase in cyberwarfare operations by North Korean actors against states supporting Ukraine. This is supported by the recent increase in cryptocurrency theft and extortion operations by North Korean state actors against large organizations in the EU.¹² The alliance between Russia and North Korea also increases the potential of Russian state-affiliated hacking groups to provide North Korean actors with the know-how required to disrupt payment transactions, increasing the threat to states supporting Ukraine. Beyond these cases, threats from China are also prevalent, albeit in a lesser manner: while they have the capabilities to carry out attacks, there is a lack of intent. Future developments, especially in the case of a Chinese invasion of Taiwan, will show if this lack of intent changes. These threats might not have the same prevalence and urgency as threats coming from Russia directly for the present moment, but cyber defense capabilities must still be built to counter them. Quantum computing must also be considered: if achieved, it could potentially give actors hostile to the EU a technological edge that would throw the current cybersecurity measures off balance.

Progress is being made to regulate and fortify the financial sector, as proven by the

⁹ <https://icct.nl/sites/default/files/2023-01/Chapter-29-Handbook-.pdf> (27.10.25).

¹⁰ <https://www.washingtoninstitute.org/media/6900> (27.10.25).

¹¹ <https://georgetownsecuritystudiesreview.org/2018/03/11/the-cyber-party-of-god-how->

[hezbollah-could-transform-cyberterrorism/](https://icct.nl/sites/default/files/2023-01/Chapter-29-Handbook-.pdf) 27.10.25).

¹² <https://cloud.google.com/transform/ultimate-insider-threat-north-korean-it-workers> (27.10.25).

legislations and acts discussed above. Evidently, the criticality of the financial sector to society has been recognized, but much remains to be done to address the complex threats that Europe will face in the increasingly volatile geopolitical landscape. The rise of hybrid warfare incidents, the current international scenario, and the digitalization of the financial sector have raised the vulnerabilities of CI in the financial sphere, and adequate measures must be implemented to tackle current and emerging threats.

Payment transactions securitized as CI have consequences – one country’s alliance with another has ramifications and can lead to attacks from hostile entities. Payment transactions might not be their most desired target, but that is merely due to their distance from the battlefield. Indeed, sectors that can more directly cripple a nation, such as energy or food, are

more attractive to attack. However—payment transactions are still part of a state’s CI, and they will continue to be targeted as they have been so before.

Analyzed through a critical lens, payment transactions are not only economic or technical processes, but they are also CI. This inclusion carries significant security implications and reimagines payment transactions as objects to whom threats can be constructed for use in geopolitical competition. The vitality of payment transactions to societal functions means that securitizing and reframing them as CI not only protects financial stability, but also highlights the political stakes involved in managing such systems in the rapidly evolving geopolitical landscape of the 21st century.

Alessia Noschese is pursuing a Master’s degree in International Affairs at the Hertie School in Berlin, specializing in International Security. She was an intern in the Security and Intelligence Research Unit at the CISS. Her research interests include military technology, EU-NATO cooperation, NATO defense policy, and the role of women in shaping the global security discourse.

Lucas Obregón was an intern in the Security and Intelligence Research Unit at CISS, where he supported project research and implementation. He is also currently pursuing a Master’s degree in Global Security at King’s College London, where he is researching irregular warfare as a threat to NATO states in the age of great power competition.