ANALYST

Co-funded by the European Union

ANALYSIS OF THE RELATIONSHIP BETWEEN VALUE CHAIN, SUPPLY CHAIN, TERRORISM, AND BLOCKCHAIN

The analysis of information sources to anticipate emerging threats is an essential component of supply chain security. The automation of Cyber Threat Intelligence (CTI) has enabled security agencies to track and analyze vast volumes of data in real-time, facilitating the detection of suspicious patterns and criminal trends.

National security is intricately intertwined with the integrity of supply chains, especially in critical sectors such as pharmaceuticals and digital infrastructure. Attacks on these chains represent a growing threat that necessitates the constant adaptation of defense strategies.

Blockchain technology emerges as a promising tool for enhancing security and transparency in supply chains. Its ability to create immutable and decentralized records allows for precise tracking of products along the chain, making it more difficult to introduce counterfeit or compromised products.

Smart contracts facilitate the automation of processes and compliance verification, reducing the risk of manipulation.

HOZINT · fyg consultores · UNIVERSITY OF WESTERN MACEDONIA · AMISTaDeS APS · UNIVERSITÀ CUSANO · European Institute for Local Development · UNIVERSIDAD DE ALMERÍA

ANALYST

Co-funded by the European Union

CRITICAL SUPPLY CHAIN VULNERABILITIES

Pharmaceutical Supply Chain

The vulnerability of the pharmaceutical supply chain to drug counterfeiting and adulteration poses a risk to public health and undermines trust in the healthcare system. Traceability is a crucial element in verifying the authenticity and origin of medicines, enabling a swift response to the detection of fraudulent products.

Digital Supply Chain

In the digital sphere, the distribution of malware and credential theft through attacks on the software value chain constitute significant threats. These attacks can compromise information security and critical infrastructure, facilitating espionage, sabotage, and the financing of illicit activities.

ANALYST

Co-funded by the European Union

Intelligence-Based Strategies for Supply Chain Protection

Cyber Threat Intelligence (CTI)

Plays a crucial role in identifying and mitigating risks within supply chains. The collection and analysis of information regarding threats, vulnerabilities, and malicious actors allow for the anticipation of attacks and the strengthening of defenses.

Collaboration and Information Sharing

Essential among different organizations for building a more robust cybersecurity ecosystem.

Authentication and Traceability

Implementing robust solutions to verify product authenticity throughout the supply chain.

Security Protocols and Audits

Establishing clear protocols and conducting periodic audits to ensure compliance.

Cybersecurity Awareness

Promoting awareness and training among all stakeholders in the supply chain.

International Cooperation

Strengthening cooperation to combat cybercrime and terrorism across borders.

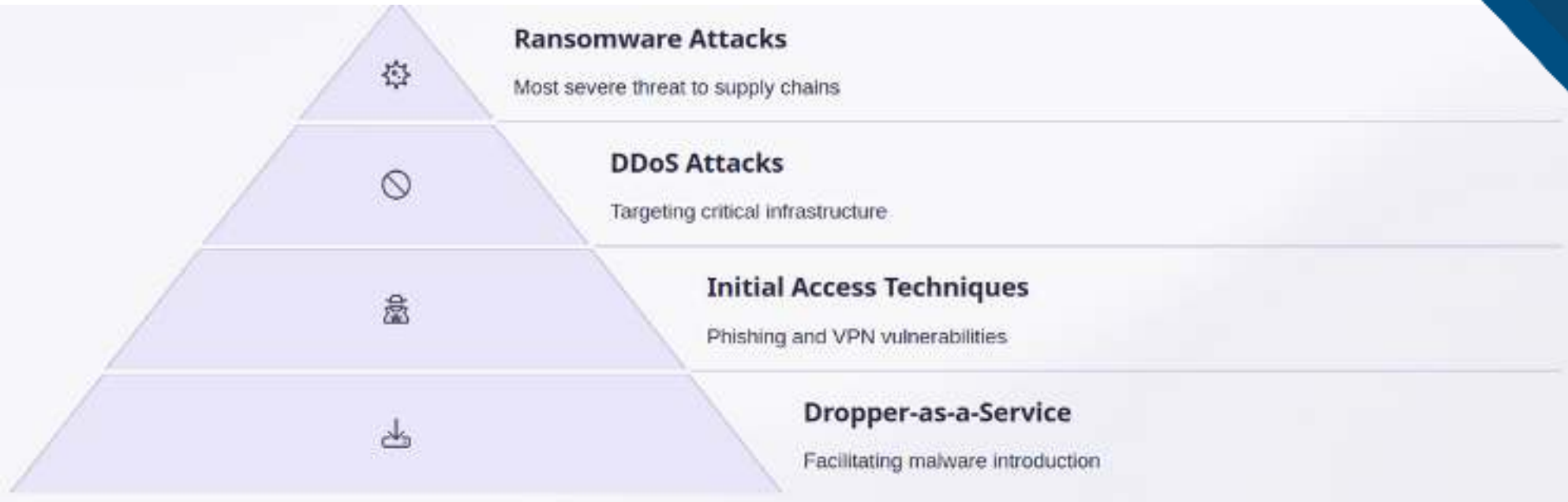
Intelligence plays a fundamental role in protecting the supply chain, not only in identifying threats but also in implementing effective strategies to mitigate risks. The collection and analysis of Cyber Threat Intelligence (CTI) can help anticipate potential attacks and strengthen security in critical sectors such as pharmaceuticals and technology.

HOZINT · fyg consultores · UNIVERSITY OF WESTERN MACEDONIA · AMISTaDeS APS · UNIVERSITÀ CUSANO · European Institute for Local Development · UNIVERSIDAD DE ALMERÍA

ANALYST

Co-funded by the European Union

Cyberattacks on the Supply Chain



The Spotlight Report - Cyber-attacks: the Apex of Crime-as-a-Service by Europol identifies cyberattacks as one of the most critical threats to the supply chain. Among the main risks are ransomware attacks, which have affected key sectors such as manufacturing and logistics. Distributed Denial-of-Service (DDoS) attacks have also increased, particularly in Europe, where pro-Russian groups have targeted critical infrastructure in response to international sanctions.

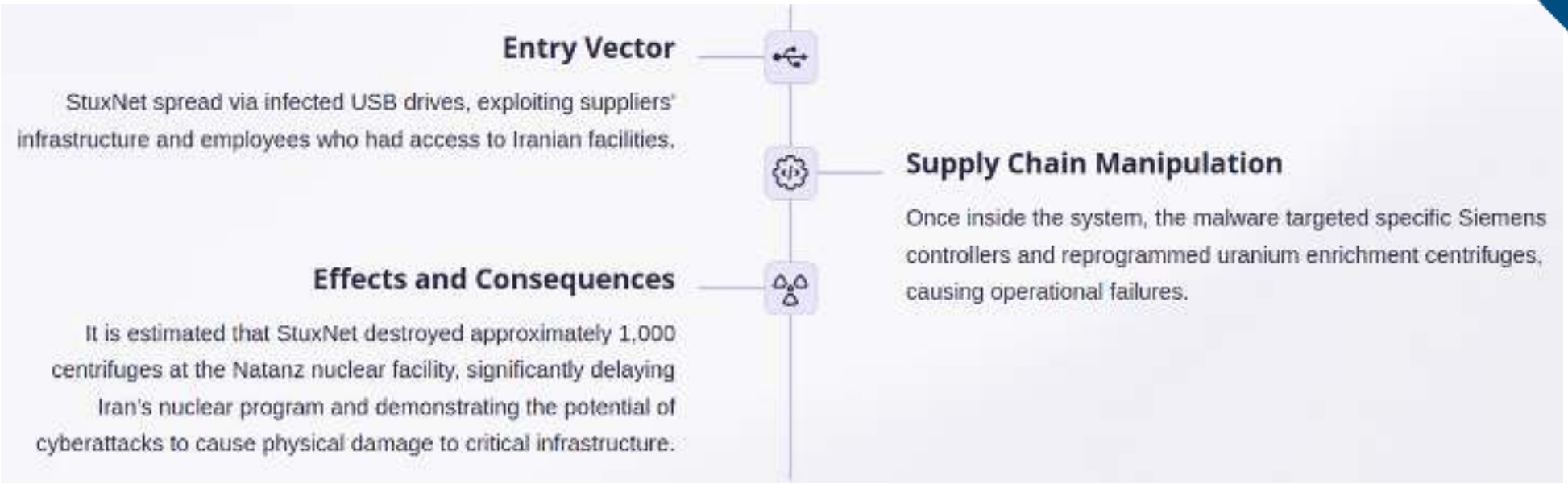
The report highlights how attackers use initial access techniques such as phishing and exploiting vulnerabilities in VPN and RDP software, compromising logistics infrastructure. Additionally, the use of dropper-as-a-service enables malware introduction into enterprise systems, facilitating data extraction or file encryption to demand ransoms.

HOZINT · fyg consultores · UNIVERSITY OF WESTERN MACEDONIA · AMIStaDeS APS · UNIVERSITÀ CUSANO · European Institute for Local Development · UNIVERSIDAD DE ALMERÍA

ANALYST

Co-funded by
the European Union

Case Study: StuxNet and Supply Chain Vulnerability



StuxNet is one of the most prominent examples of how a cyberattack can impact the supply chain and compromise critical infrastructure. Discovered in 2010, this malware was designed to target SCADA industrial control systems used in Iran's nuclear facilities. Its sophistication made it the first known cyberweapon capable of causing physical damage.

This case underscores the necessity of safeguarding the supply chain not only against physical threats but also against advanced cyberattacks that can compromise strategic infrastructure on a global scale.

ANALYST

Co-funded by the European Union

Supply Chain Breaches by Intelligence Agencies

Tracking and Product Alteration

Intelligence agencies have developed advanced tactics to infiltrate the supply chain for espionage and sabotage purposes, including the use of tracking and product alteration devices in transit.

Shipment Interception

Agencies have intercepted shipments and electronic devices, embedding spy hardware into consumer products before their final delivery, enabling long-term data collection and remote manipulation.

Impact on Security

This type of intervention highlights the need for advanced cybersecurity measures in the supply chain to prevent unauthorized access and ensure the integrity of products before their final distribution.

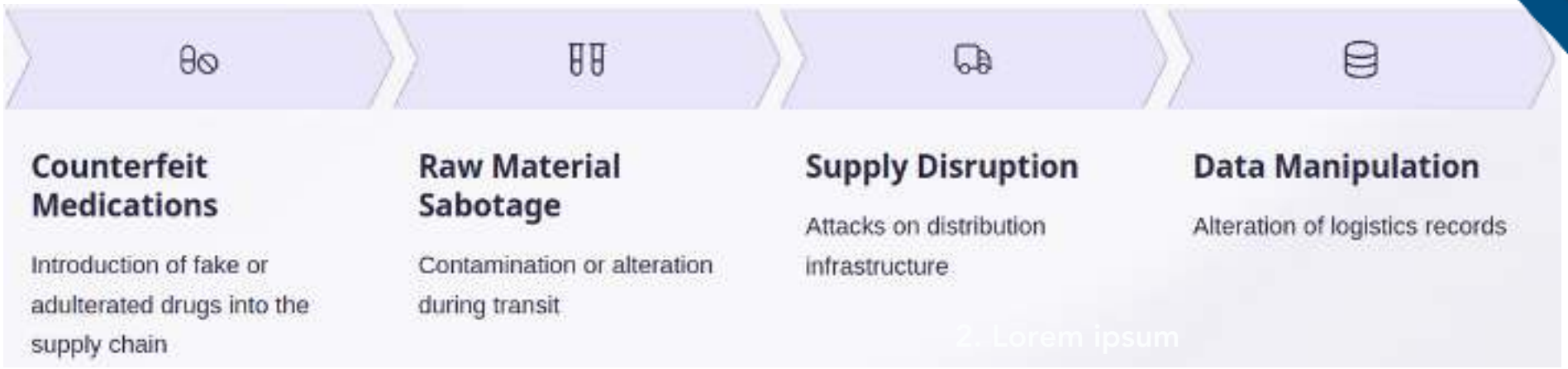
A recent example, revealed through open sources, shows how agencies have intercepted shipments and electronic devices, embedding spy hardware into consumer products before their final delivery. This technique enables long-term data collection and remote manipulation of critical infrastructure.

A tweet published by Edward Snowden illustrates how these methods have been applied in practice, affecting not only individuals but also large corporations and governments.

ANALYST

Co-funded by the European Union

Pharmaceutical Supply Chain Security



The article Hardware-Enabled Pharmaceutical Supply Chain Security by Yang et al. (2017) examines how the pharmaceutical supply chain can be targeted, endangering the population. The counterfeiting of medications is a global threat, as illicit actors can infiltrate the distribution chain and introduce adulterated or ineffective products into the market.

The article describes how hardware-based technologies have been developed to ensure the authenticity of medications and prevent their alteration during transportation and storage. Authentication systems based on chips and sensors can monitor the integrity of shipments in real time, detecting any attempt at tampering. Additionally, digital traceability through blockchain enhances the ability to track the origin and movement of products, minimizing the risk of counterfeit medications entering the supply chain.

ANALYST

Co-funded by the European Union

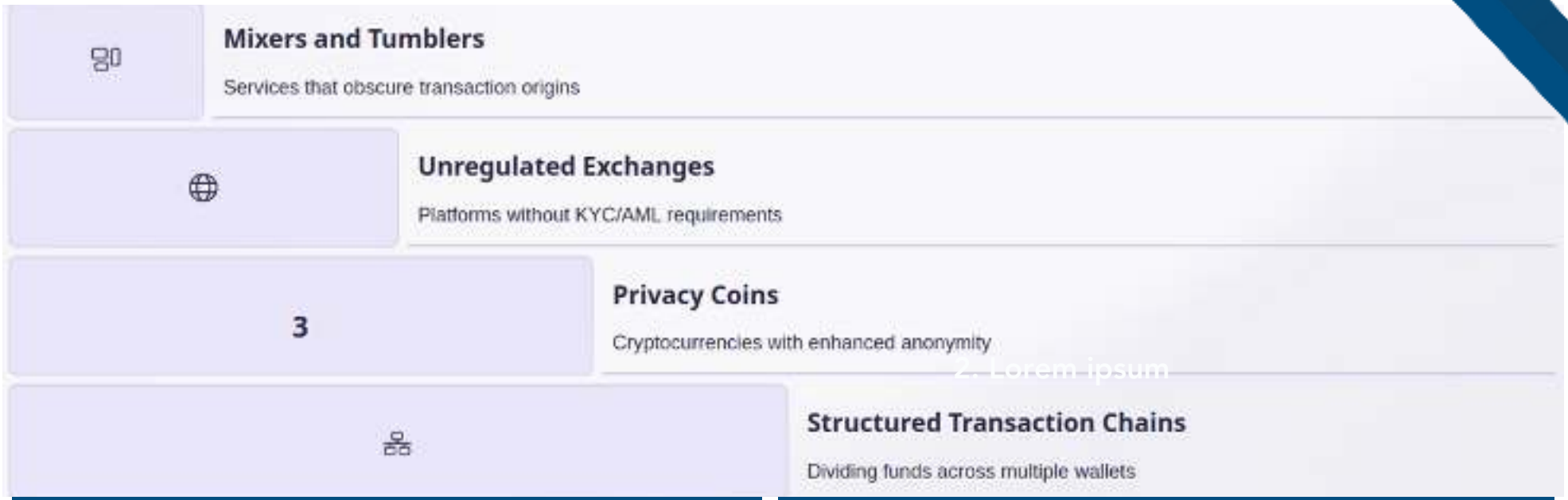
Illicit Financing Through Corporate Infrastructure

The Gold Apollo case has revealed how an apparently legitimate corporate infrastructure, including companies such as BAC Consulting, has been used to move large sums of money in an almost transparent manner without resorting to cryptocurrencies. These companies have enabled international transactions through conventional banking networks and concealed transfers within the gold trade, avoiding immediate suspicion in traditional financial monitoring systems. This case is a notable example of how terrorist organizations, such as Hezbollah, have used illicit gold trade to finance their activities and evade international sanctions. In this scheme, shell companies and smuggling networks were employed to move large quantities of gold from Venezuela to international markets, particularly in the Middle East.

ANALYST

Co-funded by
the European Union

Cryptocurrency Use in Illicit Activities



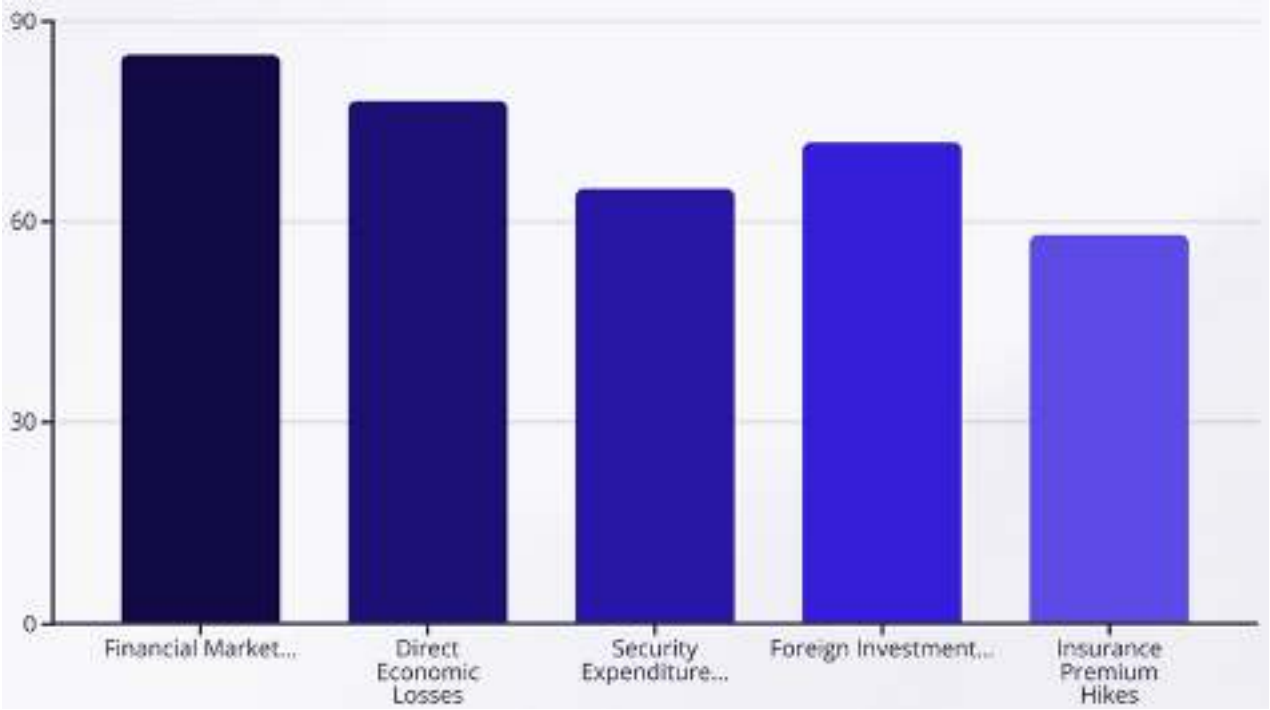
The use of cryptocurrencies in illicit activities has evolved significantly in recent years. Criminals and terrorist groups have found digital assets to be an effective means of mobilizing funds without detection by traditional financial systems. To achieve this, they employ a range of techniques and tools designed to obscure transaction traceability and evade regulatory controls.

One of the most widely used methods is the use of mixers or tumblers, services that combine multiple cryptocurrency transactions to obfuscate their origin and destination. These services fragment funds into small amounts and redistribute them to different addresses, making it difficult for intelligence agencies and financial analysts to track illicit money flows.

ANALYST

Co-funded by the European Union

Economic Impact and Mitigation Measures



Financial terrorism has a profound impact on the global economy, as it distorts markets, erodes confidence in the financial system, and generates significant risks for investors and businesses. Through strategies such as money laundering, evasion of economic sanctions, and the use of cryptocurrencies to conceal the origin of funds, terrorist groups can sustain their operations while avoiding the scrutiny of international financial authorities.

ANALYST

Co-funded by
the European Union

The economic consequences include exchange rate volatility and inflation in regions where terrorism is financed through the illicit trade of goods or the exploitation of natural resources. In addition, the infiltration of illicit financial networks into the formal banking system undermines global regulatory efforts and compliance with anti-money laundering and countering the financing of terrorism (AML/CFT) regulations.

To mitigate these effects, organizations such as the Financial Action Task Force (FATF) have developed stricter regulatory frameworks, requiring banks and fintech companies to implement enhanced due diligence procedures. The fight against financial terrorism requires international cooperation, advanced technological measures, and the strengthening of supervisory mechanisms that balance security and privacy in the global digital environment.

ANALYST

Co-funded by the European Union

CYBERATTACKS AGAINST CORPORATIONS AS STRATEGIC GEOPOLITICAL WEAPONS

In July 2021, one of the largest supermarket chains in Sweden, Coop, was forced to close approximately 800 stores due to a ransomware attack. The attack targeted Kaseya, a U.S.-based IT management firm, and exploited its software to deploy ransomware across a large number of companies worldwide. Coop, although not a direct client of Kaseya, became a collateral victim because one of its software providers was affected. This cyberattack had a severe impact on Sweden's economy and food distribution network, highlighting the cascading effects of supply chain vulnerabilities.

ANALYST

Co-funded by the European Union

Cyberattacks as Hybrid Warfare

Economic Sabotage

From a geopolitical standpoint, this type of attack serves not only as an act of economic sabotage but also as a potential vector of hybrid warfare. By paralyzing a key player in the Swedish retail sector, attackers disrupted the daily lives of thousands of citizens.

Erosion of Public Trust

This led to an erosion of public trust in the state's capacity to provide basic services and protect its critical infrastructure. Similar events occurred in Denmark with 7-Eleven, where a ransomware attack in August 2022 halted all operations nationwide, preventing transactions and disrupting the economy.

Strategic Maneuvers

In a broader geopolitical context, these attacks can be seen as strategic maneuvers linked to competition for regional influence. For example, the disruption of Swedish and Danish economic infrastructures weakens the resilience of the Nordic bloc, an area of strategic interest in Arctic geopolitics.

ANALYST

Co-funded by the European Union

Digital Identity Wallets and National Security

Streamlined Public Services

The widespread adoption of digital identity wallets promises to streamline public services, facilitate secure online authentication, and enhance citizen control over personal data.

Blockchain Technology

These wallets, which store digital credentials such as IDs, driver's licenses, and health records, are often based on blockchain-like technologies to ensure data integrity and immutability.

Complex Security Risks

However, their integration into national identity systems introduces complex risks, particularly from a national security perspective.

Intelligence Benefits

From an intelligence standpoint, digital identity wallets offer significant benefits. Centralized or federated control of identity systems allows national security agencies to monitor identity authentication events in real time.

HOZINT · fyg consultores · UNIVERSITY OF WESTERN MACEDONIA · AMIStaDeS APS · UNIVERSITÀ CUSANO · European Institute for Local Development · UNIVERSIDAD DE ALMERÍA

ANALYST

Co-funded by
the European Union

The Manipulation of Digital Supply Chains

New Frontier of Cyber Conflict

A new frontier of cyber conflict lies in the manipulation of digital supply chains to generate systemic instability within democratic regimes.

Silent Yet Impactful

Such interventions are designed to be silent yet impactful, allowing attackers to extract sensitive data, observe internal decision-making processes, and preposition for future sabotage.

SolarWinds Attack

One illustrative example is the SolarWinds cyberattack in 2020, in which a U.S.-based IT firm unwittingly distributed malware through a routine software update.

Digital False-Flag Operations

These forms of intervention also pave the way for digital false-flag operations, wherein data manipulation or staged leaks are used to sow confusion, implicate political figures, or manipulate election cycles.

HOZINT · fyg consultores · UNIVERSITY OF WESTERN MACEDONIA · AMIStaDeS APS · UNIVERSITÀ CUSANO · European Institute for Local Development · UNIVERSIDAD DE ALMERÍA

ANALYST

Co-funded by the European Union

Cryptocurrency Infrastructure as a Geopolitical Trojan Horse

HOZINT · fyg consultores · UNIVERSITY OF WESTERN MACEDONIA · AMIStaDeS APS · UNIVERSITÀ CUSANO · European Institute for Local Development · UNIVERSIDAD DE ALMERÍA

ANALYST

Co-funded by the European Union

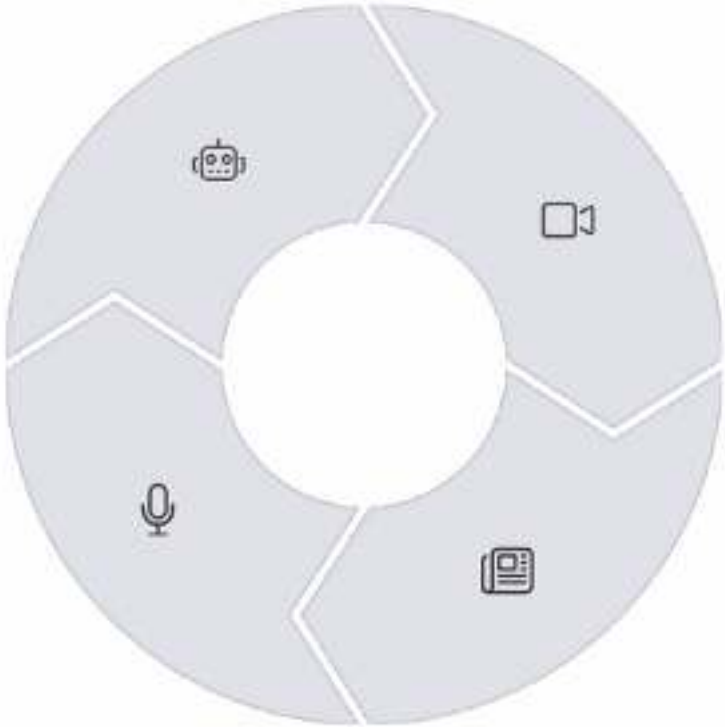
Generative Artificial Intelligence in Hybrid Conflict

Disruptive Paradigm

The emergence of generative artificial intelligence has introduced a disruptive paradigm in the arsenal of hybrid warfare

Voice Impersonation

Through voice cloning and natural language generation, malicious actors can simulate calls or messages from officials



Synthetic Media

A key risk lies in the deployment of synthetic media to discredit public institutions

Disinformation Campaigns

GenAI models can be trained to generate persuasive disinformation campaigns at scale

HOZINT · fyg consultores · UNIVERSITY OF WESTERN MACEDONIA · AMIStaDeS APS · UNIVERSITÀ CUSANO · European Institute for Local Development · UNIVERSIDAD DE ALMERÍA

ANALYST

Co-funded by
the European Union

Strategic Cyberattacks on Critical Infrastructure

Power Grid Attacks

One of the most concerning scenarios involves cyberattacks on power generation and distribution facilities. These attacks can lead to large-scale blackouts, halting industrial production, disabling communication systems, and endangering public safety.

Water Infrastructure Compromise

The compromise of water infrastructure, such as dams and treatment plants, poses a direct threat to civilian populations. An attacker gaining access to control systems could manipulate valves and sensors, potentially causing floods or contaminating water supplies.

Satellite Disruption

Satellites—used for communication, navigation, meteorology, and intelligence—represent another critical vulnerability. A successful cyberattack against satellite control systems could disrupt GPS services, military communications, or environmental monitoring.

4 Strategic Objectives

From a strategic perspective, attacks on critical infrastructure aim to erode the state's legitimacy, provoke public disorder, and exert coercive leverage without crossing conventional thresholds of war.

ANALYST

Co-funded by the European Union

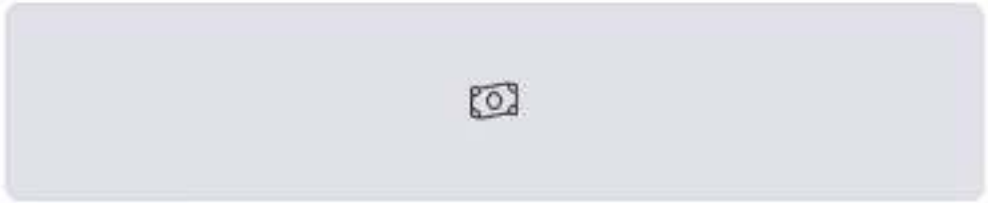
Digital Economic Warfare

Stock Exchange Sabotage

Coordinated cyberattacks capable of manipulating market data

SWIFT System Attacks

Intrusions into global financial communication protocols



Digital Currency Vulnerabilities

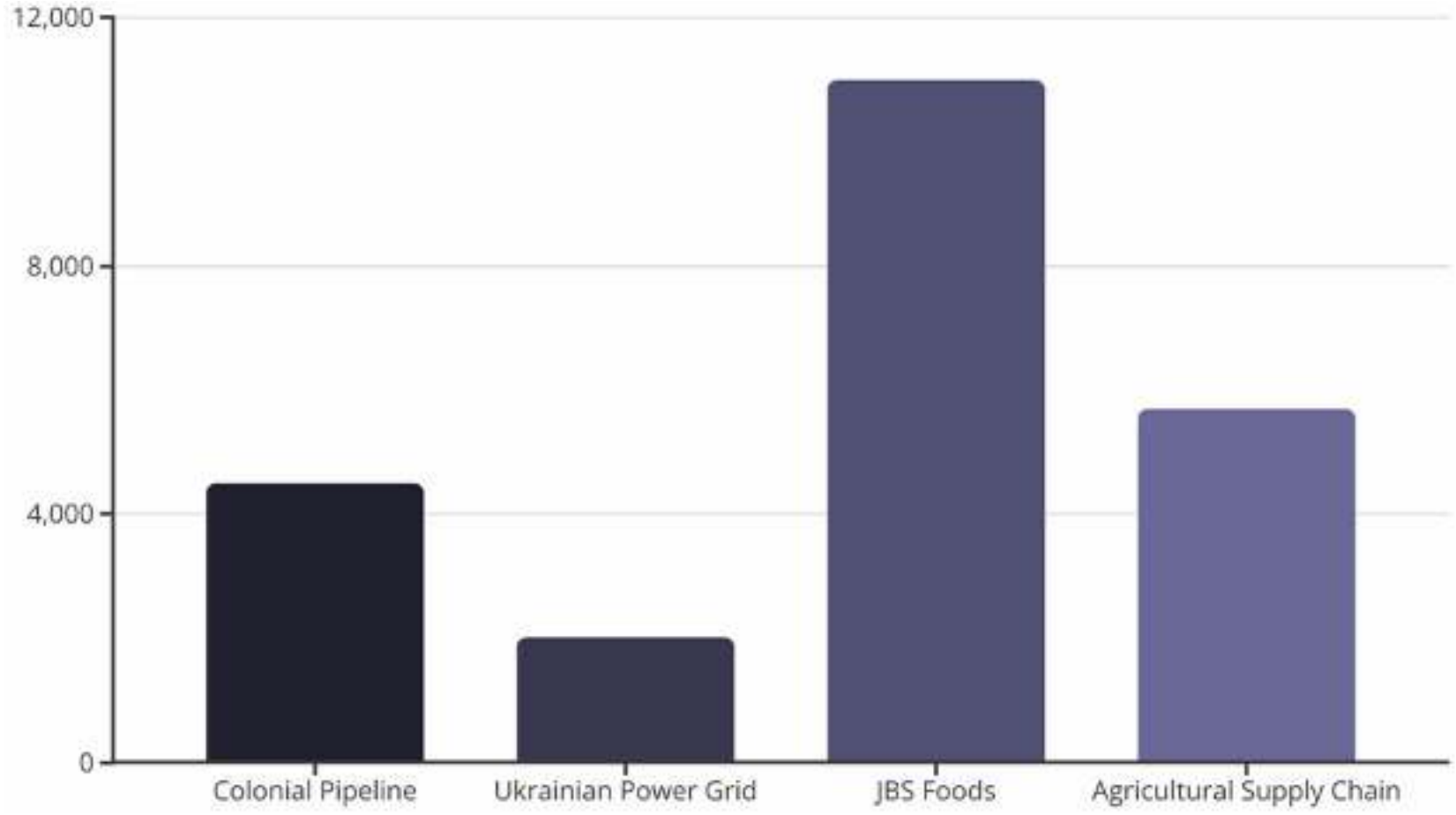
Breaches in national digital currency infrastructure

In the emerging landscape of cyber conflict, the economy itself becomes a battlefield. Digital economic warfare consists of targeted cyber operations against financial infrastructure with the aim of disrupting capital flows, eroding trust in institutions, and destabilizing rival economies. This new form of asymmetric warfare leverages digital sabotage as a means to achieve strategic geopolitical goals without triggering conventional military responses.

ANALYST

Co-funded by
the European Union

Food and Energy Security as Strategic Targets



HOZINT

fyp consultores

UNIVERSITY OF WESTERN MACEDONIA

AMIStaDeS APS

UNIVERSITÀ CUSANO

UNIVERSIDAD DE ALMERÍA

ANALYST

Co-funded by the European Union

Food and Energy Security as Strategic Targets

In the context of geopolitical instability and asymmetric threats, food and energy systems have become strategic targets for cyberterrorism. These infrastructures sustain the vital needs of populations and are deeply intertwined with national security. Disrupting them generates not only logistical and economic crises but also societal unrest and loss of trust in state institutions.

Attacks on energy infrastructure have already demonstrated their devastating potential. The Colonial Pipeline attack in 2021, attributed to the DarkSide ransomware group, disrupted fuel distribution across the U.S. East Coast, leading to panic buying, fuel shortages, and economic losses. Similarly, coordinated cyber operations against Ukrainian power grids in 2015 and 2016 (linked to Russian state actors) caused widespread blackouts and illustrated how digital sabotage can yield physical consequences.

HOZINT · fyg consultores · UNIVERSITY OF WESTERN MACEDONIA · AMIStaDeS APS · UNIVERSITÀ CUSANO · European Institute for Local Development · UNIVERSIDAD DE ALMERÍA