DOI: https://doi.org/10.37075/BJIEP.2023.1.05
Bulgarian Journal of International Economics and Politics, 2023, Vol. 3, Issue 1, pp. 69-90

Application of Innovative Systems for Achieving Compliance in Countering Hybrid Threats

Ivo Goudinov[1]

Received: 04.04.2023
Available online: 16.08.2023

Abstract

The main goal of this article is to draw attention to and contribute to the discussion on the new challenges facing the countering of the financing of hybrid threats. The research problem cuts across three study and policy areas: national security, legal codification and Artificial Intelligence. A serious theoretical conflict regarding the concept of hybrid warfare is identified and an attempt is made to demonstrate the seriousness of the risk of funding hybrid threats by global actors. The focus of the study is the economic aspects of hybrid warfare, related to the threat of covert financing of hybrid operations, and accordingly a possible model with innovative financial technologies for risk management. A short but comprehensive overview of the current legal regulations providing possible guidelines for legislative changes and technological solutions in this area has been made.

On the basis of an interdisciplinary systematic analysis, including a presentation of technical parameters of innovation systems with Artificial Intelligence elements (AIE) and an overview of European and American practices and regulations, gaps in the current regulations in Bulgaria are identified and some conclusions are made about this aspect of the country's security.

Keywords: hybrid warfare/threats, hybrid warfare financing, financial monitoring systems with Artificial Intelligence elements; cybersecurity, cryptocurrency
JEL: F15, F17, C33

[1] Doctoral student at the Institute of Robotics (IR) St Ap. And Ev. Matheus at the Bulgarian Academy of Sciences, e-mail address ivo.gudinov@ir.bas.bg

Introduction

In the context of Russia's ongoing war in Ukraine, one of the most serious challenges in the economic life of EU member states is the accelerated introduction of sanctions aimed at imposing algorithmic power on the access of Russian capital from and to its "fifth column" in the democratic world. This challenge makes it extremely important to adapt the Bulgarian national legislation in the field of money laundering and terrorist financing in order to meet the requirements of the EU and the strategic allies in the field of security. The topic is a continuation of the author's assumptions, developed in the article *Artificial Intelligence – a Weapon in the Hybrid War* published in the *International Relations* Journal (Goudinov, 2022), where an answer is sought to the question: How are assembled and where the separate elements of Russia's hybrid strategy intersect on the multi-layered and multi-dimensional chessboard of hybrid warfare? This determines the second goal of this article – to expose the high complexity of hybrid threats and the seriousness of the risk of their financing with digital and crypto-currencies by global actors (adversaries). The research problem is situated at the intersection of three research areas and policy fields – national security, law and artificial intelligence. The objectives of the study were achieved through the implementation of the following tasks:

1. Carrying out a comprehensive review of current, open sources, current regulations and practical case studies providing guidelines for possible solutions;

- Presentation of a specific concept of hybrid warfare - the so-called Russian Hydra;
- Presentation of the changes in law enforcement in the field of countering hybrid threats;
- Presentation of the existing innovation systems with AIE, having DML algorithms to achieve compliance;

2. The outlining and analysis of a specific model of financial monitoring systems with AIE with DML algorithms for the study and management of the financing risk of hybrid actors;

3. Presentation of the legal challenges in Bulgaria regarding virtual and crypto-currencies in the context of countering hybrid threats.

The article is structured in several parts and begins by presenting and analysing the model of the Hydra crypto-exchange and outlining the role of this exchange in financing the hybrid war. The article goes on to review the process of transformation of the US law enforcement community to respond to hybrid threats, and specifically the Department of Financial Protection and Innovation (DFPI) campaign against Nexo Group (Nexo) and the subsequent operational realization of Hydra.

The following is an overview of the guidelines of the Office of Foreign Assets Control (OFAC), which is jointly subordinated to the U.S. State Department and the Department of the Treasury, on the need for a functional toolkit which, for the purposes of this article, is defined as financial monitoring systems with Artificial Intelligence elements (AIE) featuring Deep Machine Learning (DML) algorithms.

The current application of these innovative systems to achieve compliance in support of national requirements for indebted legal entities is examined. A model of these systems having DML algorithms in managing the risk of financing hybrid actors is presented and some legal challenges in our national regulatory framework are exposed. Finally, in the last section, conclusions are drawn.

What is Hydra? Funding the hybrid war

In a publication headlined *The Russian Hydra*, Mark Voyager, the special adviser to the former commander of the US Army in Europe, Lieutenant General Ben Hodges, published a chart (Chart 1) that schematically presents the so-called Russian hydra (cited in Robinson, 2021). In its comprehensiveness, it provokes discussions about the scale of the concept that encompasses intelligence operations, diplomatic missions, lawsuits, socio-cultural activities, attacks in cyberspace, information warfare, economic influence, corrupt deals in strategic industries, subversion and sabotage of critical infrastructure, use of organized crime and paramilitary and/or conventional military forces. The complexity of the research problem is conditioned by the methods by which the Russian Federation exerts its hybrid influence on the targeted states. Hence the reasonable question is posed: "Can informational or economic relations be considered as war"?

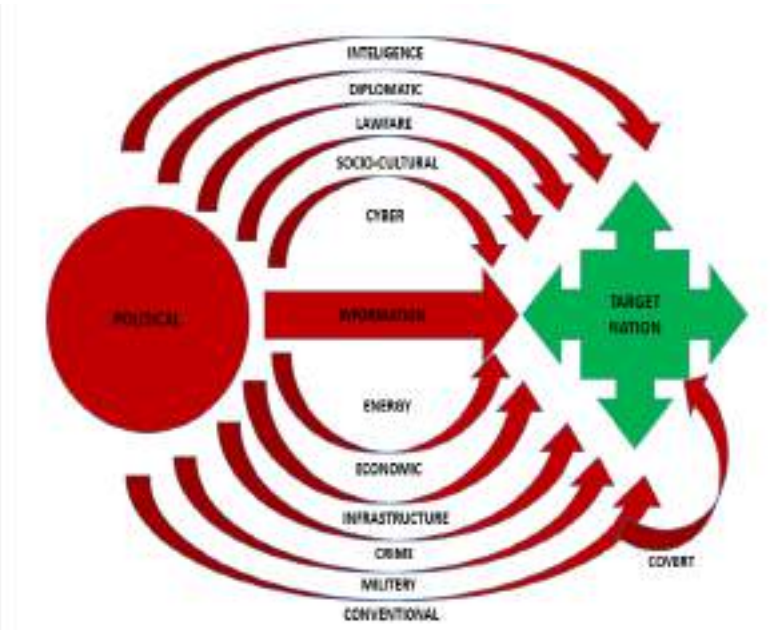

Chart 1. Conceptual model of the Hydra hybrid war
Source: retrieved from Robinson (2021)

At the same time, the name of the most contested concept model of Hybrid War strikingly matches that of the illegal Russian cybercrime market Hydra, which is hugely popular among cybercriminals due to its easy payment options and automatic encryption. Hydra's business is primarily transacting with cryptocurrency exchange addresses - sending and receiving large sums of money from them. On 25 May 2021 the cybersecurity companies Flashpoint and Chainalysis, engaged in an investigation into high-volume cryptocurrency activity, published an open source document headlined *Hydra: Where The Crypto 9Trail Goes Dark* (Flashpoint, Chainalysis, 2021).

This document describes Hydra as "a Russian-language dark web marketplace that has been active since 2015 as an open competitor to RAMP (Russian Anonymous Marketplace)." The research by Flashpoint and Chainalysis said: "Hydra provides for a higher level of anonymity and security for users and provides 'professional quality' deliveries. From the quoted open source, it becomes evident that the established direct connections with suppliers in China allow the supply and sale of "large quantities of cheap synthetic drugs" (Ibid.: 3).

As the analysis shows, the Russian market is the leader in the dark web for illegal trade in: opiates, cannabinoids, chemicals/precursors for the production of synthetic drugs, trade in BTC (Bitcoin), Secure Shell or Secure Socket Shell (SSH)[2], digital goods, documents, fake ID cards, SIM cards, design and analytical graphics, counterfeit money, devices and components with possible dual use, equipment, anabolics/steroids, employment in organized crime groups (OCGs), recruitment in private military companies (PMC) etc. The joint team of Flashpoint and Chainalysis, which has systematically monitored Hydra activity since its inception and continued into 2015, found a continuous increase in the volume of activity and the frequency of engagement in user activity. The conducted blockchain analysis reveals a drastic increase in Hydra's revenue over a period of 4 years – from less than $10 million in cryptocurrency in 2016 to over $1.3 billion in 2020. This means that from 2016 to 2020 alone, Hydra increased its annual transaction volume by 624% (see Chart 2). Based on this data, it can be argued that this upward trend is due to the escalation of the Hybrid War, respectively of the search for hidden financing and supply of organized crime groups and PMCs for participation in the kinetic conflict (war in Ukraine) and hybrid operations in Europe.

[2] SSH is a network protocol that allows for the encrypted transfer of data and rights for the construction and access to *virtual private network* (VPN).

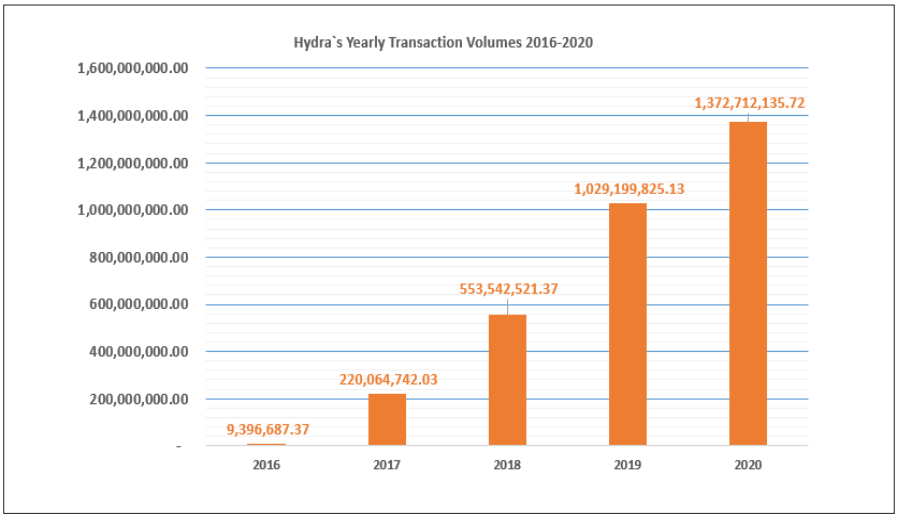

Chart 2. Trends in Hydra's development
Source: Flashpoint, Chainalysis (2021)

Flashpoint and Chainalysis analysis shows that other Russian and regional crypto-exchanges are also dominated by Hydra, as it is unique in that it mainly transacts with cryptocurrency exchange addresses, sending and receiving large amounts to and from them. This means that regional exchanges and payment service firms are the "heads" that carry out transactions to and from sellers and buyers. Many of the various exchanges that Hydra transacts with are classified by Chainalysis as high risk (Chainalysis Team, 2023), which suggests they have weak or non-existent security and compliance programs, particularly with regard to Know Your Customer (KYC) procedures, which is an indication of possible complicity.

Transformations in US law enforcement in response to hybrid threats

In his article for *Decipher*, Denis Fisher reports: "as part of the federal government's broad efforts to crack down on ransomware operators and other cybercriminal groups, the FBI has formed a new unit dedicated to investigating cryptocurrency abuse and launched a new international initiative that will work with law enforcement bodies, prosecutors and cryptocurrency platforms to track ransom payments and develop applicable anti-money laundering legislation" (Fisher, 2022). These initiatives signal a further escalation in the US government's response to Russia's Hydra. It becomes evident from the publication that in the month of October 2022, the Ministry of Justice announced the formation of the National Cryptocurrency Enforcement Team (NCET), which consists of 12 lawyers specializing in law enforcement in the field of cryptocurrencies (U.S. Department of Justice, 2022). What reveals the team's level of ambition is the fact that Un Yong Choi is appointed as NCET's

director, who is a highly experienced cybersecurity prosecutor that will presumably work closely with the FBI's new virtual asset seizure unit. In just one week after its establishment, the NCET seized more than $3.6 billion in bitcoins that were stolen during the Bitfinex hack a few years ago, thus demonstrating the efficiency of work that a team with hybrid expertise[3] can do. Collaboration with agencies around the world is required to multiply the resources available to such cybercrime investigation teams.

Malicious Ransomware, encrypting information about the user who is to be subsequently extorted into paying a ransom, as well as many other cryptocurrency-based crimes, aim for hybrid players to obtain criminal proceeds. This is why the author believes that in international coordination with the law enforcement authorities in the USA and Europe, the business model itself should be broken. In this respect, tactics, techniques and procedures (TTPs) is suitable for even more in-depth research of the experience of the FBI and the US Department of Justice, which strive to pre-emptively disrupt cybercriminal operations even before the investigation is complete, including if the suspects need to be warned. This could mean more confiscations or destruction of servers, releasing ransomware decryption tools, or using other technical means to stop or prevent attacks. The difference in NCET's approach is in the assessment at which stage of the investigation to use proactive measures, such as pre-emptive counter-attacks to prevent attacks, even before charges are raised. In view of advanced hybrid threats, a fundamental change in modus operandi is required because reactive actions are no longer effective, as proactive interventions are needed. It can be argued that to effectively counter and intercept complex, multi-channel and high-tech hybrid threats, operational thinking should be in tune with the shift in US national security concept adopted after the attacks of 11 September 2001, where the right approach is aimed at pre-emptively intercepting the "first strike".

DFPI against Nexo Group (Nexo)

In a press release, the California Department of Financial Protection and Innovation announced that it had "joined seven state securities regulators in bringing claims against Nexo Group (Nexo)" (DFPI, 2022). From the analysis it is clear that these are accounts allowing investors to deposit crypto-assets in Nexo, in return for which they received annual interest rates of up to 36% on investors' deposited crypto-assets, which are significantly higher than the interest rates for short-term fixed income securities, the respective investment grade in legal bank savings accounts. In professional circles, the opinion that Nexo Group (Nexo) is the virtual crypto-exchange and bank of Hydra has been gaining ground.

"Implementation" of Hydra

On 5 April 2022, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) announced that they are conducting a multi-pronged operation with international partners targeting Russian cybercrime. As a result of this operation, sanctions were imposed

[3] The new FBI unit includes agents who have specialized knowledge of cryptocurrencies and blockchain, and will be focused on the task of investigating abuses of cryptocurrencies and exchanges, tracking the proceeds of cybercrime, and working with other law enforcement agencies on cryptocurrency investigations.

on the world's largest and most famous darknet marketplace, the Russian-based site Hydra Market (Hydra), with the aim of curbing the spread of cybercriminal services, dangerous drugs and other illegal products (U.S. Department of the Treasury, 2022/a). The scale of the threat from Hydra is revealed by the composition of the participants in the operation team that they join:

- United States Department of Justice (USDoJ);
- Federal Bureau of Investigation (FBI);
- Drug Enforcement Administration (DEA);
- IRS Criminal Investigation (CI);
- National Security Investigations Division (NSID);

Cryptocurrency transactions are recorded on the main blockchain, making them transparent, but ransomware attacks on digital currencies go some way to helping the Russians make up for the revenue lost due to sanctions. Illicit markets, such as Hydra, positioned on the darknet, almost entirely accept virtual and crypto-currencies as payment for a wide range of illegal services and goods, including Ransomware-as-a-Service (RaaS)[4]. Hybrid actors conduct illicit transactions, often mistakenly believing that these are anonymous and untraceable means of exchange. On this occasion, the position of the US Treasury Department is that they are taking action against all hybrid actors who, "like Hydra and Garantex, knowingly disregard anti-money laundering and counter-terrorist financing (AML/CFT) obligations and allow their systems to be used by criminal (or hybrid) actors" (U.S. Department of the Treasury, 2022/b). It can be argued that the emphasis in these messages to the Virtual and Crypto-Currency Industry is on the implementation of appropriate AML/CFT measures and compliance with sanctions. The U.S. Department of the Treasury published an updated National Strategy for Combating Terrorist and Other Illicit Financing, which provides guidance on planned efforts to further combat the abuse of virtual currencies and crypto-exchanges used to finance the Hybrid War. The mobilization of this colossal international resource is linked to the following data set out in the OFAC publication:

- approximately 86% of illegal bitcoins received directly from Russian virtual currency exchanges in 2019 came from Hydra;
- Hydra's revenue has increased dramatically from under $10 million in 2016 to over $1.3 billion in 2020.

It is logical to assume that this growth in Hydra's profits is related to the financing of Russian hybrid warfare campaigns and operations, in which the main proxy players are Russian sanctioned individuals who use a wide range of measures in their efforts to circumvent US and international sanctions.

[4] Ransomware-as-a-service is a cybercrime business model where ransomware operators write software and affiliates pay to launch attacks using said software. The partners do not need to have their own technical skills, but rely on the technical skills of the operators.

Innovation systems with AI with DML algorithms to achieve compliance

In order to increase security in the sector of virtual and crypto-currencies (see Chart 3) in the month of October 2021, the Office of Foreign Assets Control (OFAC), which is jointly subordinated to the Department of Foreign Affairs and the US Department of the Treasury, published an open source under the headline Virtual currency guidance for sanctions compliance (OFAC, 2021). The document emphasizes risk management, recommending that risk assessments should reflect: "the company's customer base, products, services and supply chain, contractors, transactions and geographic locations, and may also include an assessment of whether contractors and partners have adequate compliance procedures and mechanisms in place."

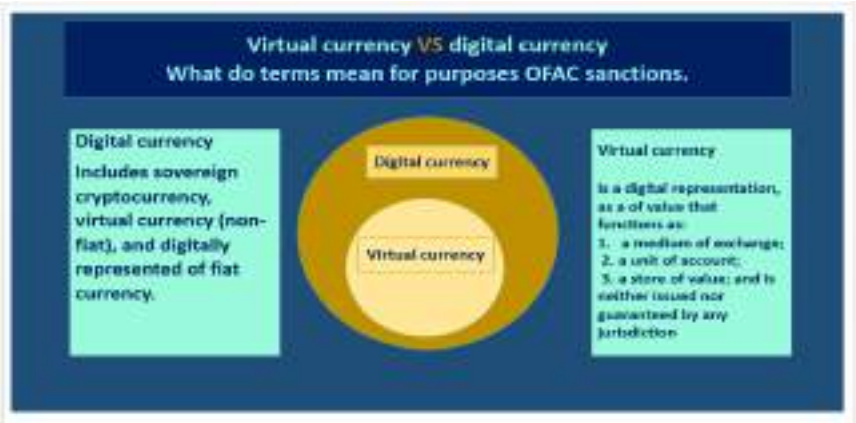

Chart 3. Defining differences between digital and virtual currency
Source: Foodman CPAs & Advisors (2022)

Innovative AIE systems can be used to manage risk by detecting potential violations of OFAC sanctions by analysing data such as customer names, transaction details and financial information. SAIE's algorithms can identify patterns that expose violations of sanctions provisions thus allowing companies to take appropriate action before potential violations materialize. Some of the most suitable such systems with DML algorithms that can be effective in detecting potential violations of OFAC sanctions are naive Bayes[5], Support

[5] In statistics, *naive Bayes classifiers* are a family of simple "probabilistic classifiers" based on applying Bayes' theorem with strong (naive) independence assumptions between the features (see Bayes classifier). They are among the simplest Bayesian network models, but coupled with kernel density estimation, they can achieve high accuracy levels.

Vector Machines (SVM)[6] and Random Forest[7]. These systems have algorithms that can quickly and accurately analyse large amounts of data, making them ideal for identifying potential infringers.

Diagnosing high-risk relationships

OFAC's Guidance makes it clear that companies that do business with the US and its strategic partners in which there are large US investments should monitor sanctions compliance by vetting their direct customers for potential ties to sanctioned companies. This means checking the available information about customers and contractors - natural and legal entities that use payment platforms to process payments for the purchase and sale of products and services. In particular, before carrying out transactions, the company must have investigated all available information about its customers and contractors, such as names, addresses, telephone numbers, e-mails and Internet (IP) addresses, etc.

Internal control

Another important focus, according to OFAC experts, is "an effective sanctions compliance program that will enable the company to conduct sufficient due diligence on customers, business partners and transactions and identify red flag risks."[8] The internal control that companies in the virtual currency business must apply depends on the product range and services they offer, the locations of the activity carried out, the positioning of its users and the scope of the specific sanctions they fall under. These components are of utmost importance during the risk analysis and assessment process to identify threats to the company. According to OFAC, it is good practice to use industry-specific tools such as transaction screening, investigation and monitoring.

Instruments for geolocation

OFAC strongly recommends the inclusion of geolocation, monitoring and reporting tools to block IP addresses. According to the author, this can be achieved by implementing an Intelligent System for Security Incidents and Event Management - SIEM (Security Incidents and Event Management) in a Security Operations Center – SOC (Security Operations Center)

[6] In machine learning, support vector machines (SVMs, also support vector networks) are supervised learning models with associated learning algorithms that analyse data for classification and regression analysis. Given a set of training examples, each marked as belonging to one of two categories, an SVM training algorithm builds a model that assigns new examples to one category or the other, making it a non-probabilistic binary linear classifier (although methods such as Platt scaling exist to use SVM in a probabilistic classification setting). SVM maps training examples to points in space so as to maximise the width of the gap between the two categories.

[7] Random forest is a commonly-used machine learning algorithm trademarked by Leo Breiman and Adele Cutler, which combines the output of multiple decision trees to reach a single result. Its ease of use and flexibility have fuelled its adoption, as it handles both classification and regression problems.

[8] Red flags are indications of illegal activity or non-compliance that prompt the company to investigate and take appropriate action.

(Recorded Future…)[9] on a corporate, holding or cluster basis. Companies operating virtual currencies under a strict sanctions regime should implement such tools with respect to IP addresses originating from jurisdictions subject to sanctions or for activities that are prohibited by OFAC regulations. Without this internal control toolkit, virtual currency companies cannot prevent transactions to their platforms or services by legal entities and natural entities subject to comprehensive access sanctions and may possibly engage in prohibited activity, whether intentionally or unintentionally. Analytical algorithms can check against known virtual private network (VPN) IP addresses and identify behavioural anomalies, such as the same user logging in with an IP address from the United States and shortly thereafter with the same IP address from Japan.

Know Your Customer (KYC) Procedures

It is extremely important for a company that wants to avoid secondary sanctions[10] to have information about customers throughout the life cycle of the relationship with them, using this information to perform analysis and assessment to reduce the potential risk associated with sanctions. For example, the collected information may include the following elements, which during the processing of customer transactions will be periodically monitored:

Data about natural persons: name of the subject, date of birth, physical and electronic address, nationality, IP addresses, data related to transactions and logins, banking information, as well as ID cards and other documents of identity and residence;

Legal entities: name of the legal entity, subject of activity, ownership information, physical and electronic address, headquarters information, email and IP addresses, data related to transactions and logins, information about the location from which the entity operates, library for all applicable regulatory documents.

It is logical to assume that this increase in Hydra's profit is related to the financing of Russian hybrid warfare campaigns and operations, in which the main proxy players are Russian sanctioned persons using a wide range of measures in their efforts to circumvent US and international sanctions.

For customers at higher risk, additional screening may be required. This may include, for example, DML of the customer's transaction history for links to sanctioned jurisdictions or transactions with virtual currency addresses linked to sanctioned entities. Additional information may be collected in accordance with existing AML obligations.

[9] Recorded Future's intelligence reduces security risk by automatically positioning threat data in your IBM Security QRadar environment. This empowers analysts to identify and triage alerts faster, proactively block threats, and reduce time spent on false positives to improve analyst efficiency.

[10] On 20 April 2022, on the Stanford University website, an international expert group called "Yermak-McFaul" published an "Action Plan for Strengthening Sanctions against the Russian Federation." The Plan explicitly emphasizes the need to constantly analyse the efficacy of primary and cumulative effects of secondary sanctions as components of a larger international strategy to deter Russia's conventional military aggression. This means introducing secondary sanctions against all foreign natural and legal persons who carry out significant transactions or investments for the sanctioned persons that is to prevent any potential facilitation of transactions related to Russia through front persons and offshore companies (Goudinov, 2022).

Supervision and investigation of transactions

SAIE to identify and block transactions with virtual and crypto currencies should be directed to addresses of sanctioned and associated with sanctioned persons included in the Specially Designated Nationals and Blocked Persons List (SDN) Human Readable Lists. The inclusion of the DML to identify virtual and crypto-currency mining and exchange addresses to OFAC's SDN list will help identify other addressees that may be associated with blocked individuals or otherwise pose a risk of sanctions evasion.

Systems with AIE, with algorithms for DML, in support of the national requirements for indebted legal entities

Performing financial monitoring with systems equipped with DML algorithms is of utmost importance for the prevention of suspicious operations, transactions and clients that can serve as a cover for hybrid actors. They can automatically extract and compare data from integrated databases on the affiliation of customers and members of the Community of interest (CI) – on a cluster or industry basis to the OFAC Lists. Systems with AIE-DML would allow the implementation of automated procedures for research and verification of each new customer or member of the KYC according to approved criteria and indicators [red flags] from the KYC questionnaire (see Chart 4). The data from this questionnaire can be combined with data from declarations on the origin of the client's funds, the annual financial statements for the last three years from the Commercial Register, data for identifying the shares of the actual owners from the Central Depository and credit data from the Central Credit Register. In this way, the information about the transactions and operations of the customers can be compared and based on the results of the risk management, an Assessment can be made for unusual and suspicious business relationships.

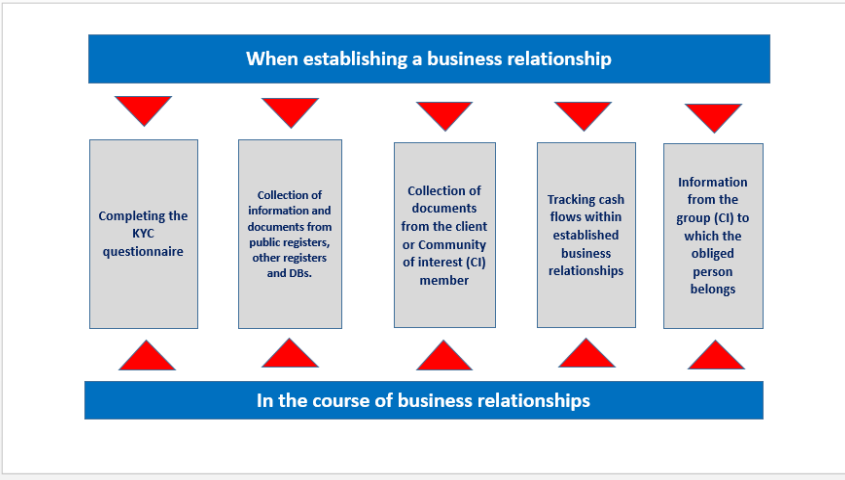

Chart 4. Algorithm for the research of suspicious operations, clients or members of KYC
Source: Developed by the author

Through financial monitoring systems with AIE, with DML algorithms, monitoring and periodic screening can be carried out when performing an extended complex check of business relationships with old customers or Community of interest (CI) members, to identify suspicious transactions (see Table 1), transactions and relationships with new customers and CI members, with regard to belonging to OFAC lists. This method will allow the implementation of automated screening procedures in client registers and integrated databases for research and verification of connections with politically exposed persons (PEP) and their proxies/substitutes who may play the role of intermediaries and representatives falling within the scope of prohibitions on financing and obtaining certain products and services.

Table 1. Factors generating high risk when determining the risk profile of a legal entity

Risk profile points				**Total number of**
N/T Grade	**Risk factors**	**At answer YES**	**At answer NO**	**Mandatory risky category**
Customer and Beneficial Owner Risk Factors				
Risk factors related to the activity of the customer and the beneficial owner				
N/T	The actual owner of the client belongs to one of the categories under Article 36 of the Law on Measures AML - prominent political figures or persons related to them.	25	0	High risk
N/T	The actual owner of the client occupies another, important position, which, although it does not fall under the scope of Article 63 of the Law on Measures AML, could enable the abuse of this position for personal benefit or the benefit of a third party.	15	0	High risk
Risk factors related to the reputation of the customer or beneficial owner				
N/T	Prior notices have been sent to the client or its actual owner or persons related to them under Art. 72 of the Law on Measures AML or under Article 9 of Paragraph 3 of the Law on Measures Against the Financing of Terrorism.	25	0	High risk
Risk factors related to the countries and geographical areas of the customer or the beneficial owner				
N/T	The customer and/or the actual owner of the customer is from a country belonging to the list under Art. 46 para. 3 of the Law on Measures AML	25	0	High risk
N/T	For the country of the client and/or the actual owner, there are instructions from the director of the "Financial Intelligence" Directorate of the State Agency "National Security" under Art. 46, Para. 5 of the ZMIP	25	0	High risk

Source: Regulations for the implementation of the Anti-Money Laundering Measures Act (BG).

These automated DML processing according to pre-set criteria, consistent with the risk factors, allows for demonstrable risk management [analysis and assessment] and ongoing monitoring for periodic updating and implementation of measures in accordance with the requirements of Bulgarian and European legislation. Once the financial monitoring SAIE-DMLs determine the risk profile of clients and CI members, based on their algorithms, scenarios can be generated and specialized reports prepared for unusual and suspicious entities and operations. This would serve the obliged entities to develop and implement procedures[11] for automatic reporting of suspicious transactions (see Chart 5), operations and customers through secure electronic channels based on established internal rules, specific criteria, forms and samples. Thus, in essence, an automated own assessment of the risk of money laundering and concealment of the financing of terrorism or hybrid operations (see for instance Corporater, 2023) in accordance with the National Risk Assessment (NRA) as a requirement of the State Agency for National Security [SANS], as laid down in the EC AML and TF risk assessment methodology (European Commission, 2022) and according to the instructions of the BNB (EBA/GL, 2021) for determining the risk factors and criteria for own risk assessment/in the case of an extended complex check and the preparation of the individual assessment and profile of each client and CI member.

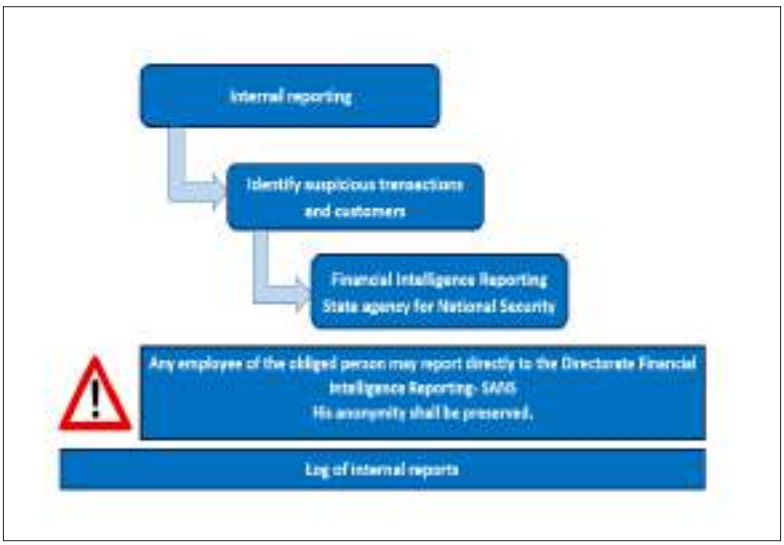

Chart 5. Algorithm for reporting suspicious operations, transactions, customers and KYC members
Source: Developed by the author

[11] Mandatory prescribed and documented processes, procedures, registers and records [documented information] for the management [analysis and assessment] of the risk of the infiltration of agents described as intermediaries and representatives for the purpose of strategic corruption, money laundering and hybrid threat financing.

Model of the systems for financial monitoring with AIE with DML algorithms for the study and management of the risk of funding hybrid actors

Due to the fact that information from open sources on innovative FinTech[12] systems is extremely scarce, given the writing of this article, a different methodological approach was applied. As a specific positive example, a platform of a high-tech Ukrainian startup developing and providing access to a FinTech platform with AIE for DML called "You Control"[13] was the object of research.

Their modus operandi is to *crowdsource*[14] the empowerment of "collaborators" and open access to integrated registries/DBs to multiply the intelligence-analytical power to counter "dirty Russian money and their proxies" as the most powerful weapon to cut off the financing of hybrid threats. The key capability "You Control" is expert analysis according to "Financial Monitoring" criteria, which includes the financial analysis of the contractor according to activated risk factors. The capacity of the module is to check a total of 415 factors, of which 11 are used only for financial monitoring. In Ukraine, as the most affected by the Russian full-scale/kinetic and hybrid war, an automated verification of companies is carried out based on risk factors specified in the Decree of the National Bank of Ukraine dated 19 May 2020 (NBU, 2020). In the "You Control" DMI platform, the results of the express Fin Tech analysis are automatically generated in the "Dossier" sections of the same name or in the "Dossier Review" sub-section, after which the "Financial Monitoring" sub-program is activated. The subroutine allows adjusting parameters such as "Short period of existence," "Insufficient amount of authorized capital," "Main type of activity of a "general" nature," "Declaration of bankruptcy" and other important factors for a better NORD – a cycle for countering hybrid threats covertly financed by natural and legal entities operating with virtual and crypto-currencies.

"Professional ties"

The FinTech platform with AIE for DML "You Control" has a specific module with an instrumental algorithm for researching current and historical connections of an object/contractor and related legal and natural entities called "PRO Connections". Through it, when creating a file, it can carry out a study and analysis of the relationships of the persons or companies that are the object of interest. A field with a visualizing network graph of the contactor's business relationship with additional analysis tools automatically appears on the screen. The main nodes in the connection model represent legal entities (firms and ETs) and natural persons (see Chart 6). Connections are built using auxiliary information

[12] FinTech's portmanteau of "financial technology" refers to firms using new technology to compete with traditional financial methods in the delivery of financial services. Artificial intelligence, Blockchain, Cloud computing, and big data are regarded as the "ABCD" (four key areas) of FinTech.

[13] The "You Control" Platform is accessible at: https://youcontrol.com.ua/en/.

[14] "Crowdsourcing," translated by some as open engagement, literally means using the resource of the crowd. It emerges by analogy with outsourcing.

nodes, which contain various types of information about the number of connections and containers with specifying information: with whom, when, exactly how the connection was established and of what nature it is. Information nodes are always close to the main node of a company or natural entity and cannot exist separately from it. Grouping nodes help to group information by a certain attribute/trait (eg. by phone number, house, objects, etc.).

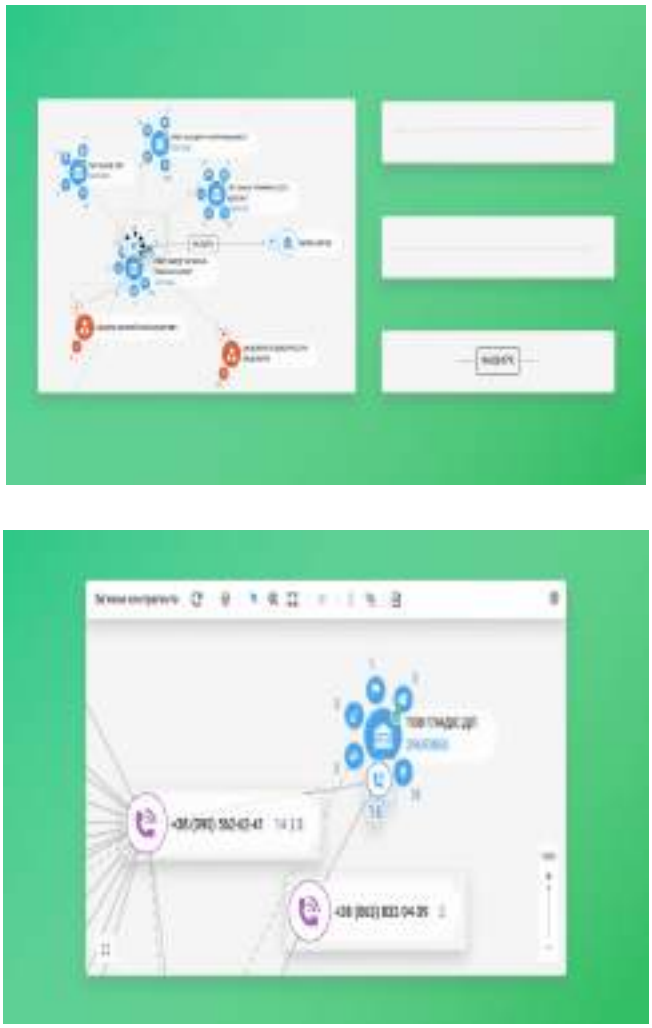

Chart 6. Graphic presentation of informational and grouping nodes for the relationships between natural entities and properties
Source: "You Control" (Module 2)

Analysis of affiliated natural and legal persons

The "You Control" platform has a module "Verification of natural persons" for company employees, management change history, reporting units, national public figures and related companies, etc., depending on the degree of integration of the database in the e-government in the respective country. In Ukraine, for example, when searching for data on a natural person in the "Verification of natural persons" module, the object can be researched using open data[15] from 27 official registers [DB]. Based on the received information, conclusions can be drawn and decisions are made whether to cooperate with a contactor or not, respectively to be submitted to the Security Service of Ukraine (SBU) to be classified as an "object of operational interest."

Search query algorithm

When executing a request to search for an individual, there is a section "Verification of a natural entity in the registers." This block consists of 4 fields in which the following data search criteria are entered:

- The three names (*mandatory verification criterion);
- Registration number (identification number) of the batch card of the taxpayer[16];
- Date of birth (displayed automatically if the identification code is entered incorrectly);
- Diploma of the person;

This provides an access and configuration field providing different criteria for accessing and searching the following registries:

National Security and Defence Council Sanctions Register

In Ukraine, the data in this block come from the lists published after the decisions of the National Security Service of Ukraine (SBU) "On the implementation, cancellation and amendments of personal, special economic and other restrictive measures (sanctions)";

Terrorist Register

It displays data that are on the terrorist lists of the State Financial Monitoring Service/ Financial Intelligence of Ukraine;

Corrupted Register

The data are from the Unified State Register of persons who have committed corruption or corruption-related crimes;

Register "Declarants and members of the public/public figures", as well as "Their relatives" ("The unified state register for the declarations of persons authorized to perform functions of the central or local government").

This register receives data about:

- whether a person submits declarations to the Agency for the Prevention of Corruption;

[15] Open data is a concept according to which certain data should be available to everyone for free use and publication in a free manner without restrictions of copyright, patent or other means of control.

[16] Registration number of the tax payer's card [RNTC] - Ukraine;

- who and how is related to the subject of the declaration (family members, business partners, persons who own joint property);
- whether the subject of the declaration is a nationally significant/public figure.

Register of Implementation of the Law of Ukraine "On Purification of Power"

Data from the Unified State Register of Persons to whom the provisions of the Law of Ukraine "On Purification of Power" have been applied.

Register Lawyers

This block shows the results of checking the availability of personal data (PD) in the "Unified Register of Lawyers of Ukraine". It may contain the following information:

- contact details of the lawyers (business address, telephone numbers, links to social networks, photo and video files);
- data on diplomas and certificates;
- persons who completed an internship with the lawyer;
- legal assistants;
- power of attorneys of lawyers with whom foreign lawyers work.

Legal challenges in Bulgaria

In preparing this article, the author made some inquiries to partner services involved in the investigation of the Nexo case. Almost identical and formal responses were received: "In the public eye, it will appear that you are investigating a case that is currently under investigation. That is your question, but we do not see any government or public body willing to correspond with you based on an email request. We cannot really help you in this regard and suggest that you establish a line of inquiry through your academic network." To this effect, we will limit ourselves to a brief legal analysis of some gaps in our legal framework regarding virtual and crypto-currencies. The lack of a clear legal framework in Bulgaria raises the issue of effective regulation, and specifically regarding persons who acquire, trade, make payments and finance with virtual and cryptocurrencies must be licensed. So far there is a described case law that accepts that "trade and mining of virtual currencies, financing through virtual currencies" or "mining and purchase and sale of virtual currency, purchase and sale of machines and devices for mining virtual currency" do not fall within the scope of Art. 12, para. 3 and Art. 4 of the Law on Payment Services and Payment Systems (LPSPS, 2023), which places payment services under a license regime. According to the opinion of the deputy governor of the Bulgarian National Bank expressed in a letter No. BNB – 108809/19.09.2014, the virtual currency "Bitcoin" is not legal tender. In the same direction is a letter No. 07-00-114 / 23.10.2014, in which the Financial Supervision Commission (FSC) expresses its opinion that the acquisition, trading and payment of "bitcoins" does not fall within the scope of the until recently effective European and national legislation and are not subject to a license and registration regime.

This means that "Bitcoins" or other virtual currencies were not recognized and treated as financial instruments within the meaning of the Law on Markets and Financial Instruments (LMFI) and should not be subject to the requirements of the LMFI. The legal vacuum in the Bulgarian legislation in the field of cryptocurrencies is explicitly stated in the publication *Regulation of Cryptocurrency Around the World: November 2021 Update* of The Law Library of Congress of the USA (Law Library of Congress, 2021). In it, the Global Legal Research Directorate directly states: "as of November 2021, compared to 2018, the number of countries that have adopted advanced tax laws, anti-money laundering and anti-terrorist financing laws, or both types of laws has increased – these jurisdictions include the EU member states, with the exception of Bulgaria." From the point of view of the criminal aspects, our legal framework should be updated and specify whether lending in cryptocurrencies as an activity covered by the Law on Credit Institutions (LCI) and specifically the performance of which without a corresponding permit (for a bank) or registration (for a financial institution) is a crime within the meaning of Art. 252, para. 1 of the Criminal Code[17].

With the adoption of the new European regulations on information accompanying transfers of funds and transfers of certain cryptoassets (EU Regulation, 2023/a) and on cryptoasset markets (EU Regulation, 2023/b) the picture has changed significantly. EU Regulation 2023/1113 provides for the transmission of information along the payment chain for transfers of cryptoassets. The regulation envisages the creation of a system to oblige crypto-asset service providers to accompany fund transfers with payer and payee information. This effectively aligns with the risk-based approach developed by the FATF[18] for enhanced due diligence. EU Regulation 2023/1114 on crypto-asset markets aims to introduce a regulatory framework for all member states regarding financial, legal and technological processes in blockchain chains, ensuring legal clarity and certainty. In order to aid regulation, the Regulation requires crypto service providers to clearly identify their customers through the "Know your customer" (KYC) protocol in order to combat money-laundering ("anti money-laundering" or AML) and the financing of terrorism.

The regulation addresses one of the main criticisms of the Transfer of Funds Regulation (TFR) protocol that applies to cryptocurrency transactions, namely the concern that because so much personal data is collected about cryptocurrency users, it would create an additional vulnerability for hackers to take advantage of. Therefore, TFR's approach to data protection must follow the EU's General Data Protection Regulation (GDPR), which is considered one of the most robust regulations worldwide. The author believes that the

[17] Art. 252, para. 1 of the Criminal Code postulates: "who, without a corresponding permit, conducts banking, insurance or other financial transactions, provides payment services or issues electronic money, for which such a permit is required, shall be punished with imprisonment of three to five years and with confiscation of up to 1/2 of the perpetrator's property."

[18] Financial Action Task Force or FATF (in French *Groupe d'action financière* or GAFI) is an intergovernmental organization. The reason for its organization is the G-7 initiative of 1989 to develop strategies aimed at combating money laundering.

quick and high-quality implementation of the two new EU Regulations for the prevention of legal conflicts with our National legislation would shorten the *vacatio legis*[19] respectively the time frame that hybrid players would take advantage of.

Conclusion

The assumptions and examples based on allied experience provide another positive example of a proactive and defensive hybrid strategy to deter and intercept hybrid threats, as recommended in the report of the European Centre for Excellence in Countering Hybrid Threats *DETERRENCE: Proposing a more strategic approach to countering hybrid threats*. An important axiom in the concept of countering hybrid threats is that "A hostile actor that employs this method tries to avoid eliciting a traditional response, disrupts one's ability to respond effectively and seeks to achieve its goals while remaining unattributed and unpunished" (Keršanskas, 2020: 7). Hostile actors must know that the Hybrid Defence will expose and incriminate them, for which they will be widely supported by their allies. From the official documents of the Bulgarian government, it is not clear whether work is being done on the creation of a conceptual framework and relevant doctrines of the responsible institutions, which, in view of the new challenges facing the country, should in practice coordinate their work in the conditions of a Hybrid War. The lack of a deterrence strategy in a country that is clearly subject to systematic hybrid attacks raises reasonable doubts that this is to the benefit of Russia, which is clearly using single-launch hybrid operations in accordance with the Hydra combat concept, through which it is trying to prepare the security environment in Bulgaria, the countries of Southeast Europe and the Black Sea region for its likely current and future hybrid and conventional plans.

References

Chainalysis team (2023). *How Darknet Markets and Fraud Shops Fought for Users In the Wake of Hydra's Collapse*. 9 February 2023. [Online]. Available at: https://blog.chainalysis.com/reports/how-darknet-markets-fought-for-users-in-wake-of-hydra-collapse-2022/ (last visited 10 April 2023).

Corporater (2023). *Anti-Money Laundering Software* [Online]. Available at : https://corporater.com/solution/anti-money-laundering-software/ (last visited 13 April 2023).

DFPI (2022). "DFPI Joins Other State Securities Regulators To Bring Actions Against Another Crypto Interest Account Provider." In: Department of Financial Protection and Innovation, State of California. Press Release, 26 September 2022. [Online]. Available at: https://dfpi.ca.gov/2022/09/26/dfpi-joins-other-state-securities-regulators-to-

[19] *Vacatio legis* – time period for the qualitative functionality of the consequences of legal prescriptions. It is necessary that *vacatio legis* be adequately specified in order to become a prerequisite for assimilation and adoption of the spirit of the law by its addressees. This is possible precisely through the regulatory assessment of the law (Mihailov, 2014).

bring-actions-against-another-crypto-interest-account-provider/ (last visited 10 March 2023).

EBA/GL (2021). "Okonchatelen doklad otnosno nasokite za kompleksna proverka na klienta i faktorite, koito kreditnite i finansovite institutsii sledva da vzemat predvid pri otsenkata na riska ot IP/FT, svŭrzan s individualni delovi vzaimootnosheniya i sluchaĭni sdelki" [Final report on the guidelines for comprehensive client due and factors that credit and financial institutions should consider in assessing IP/FT risk related to individual business relationships and random deals]. European Banking Authority EBA/GL/2023/02 1 March 2021. [Online]. Available at: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/Guidelines%20on%20ML-TF%20risk%20factors%20%28revised%29%202021-02/Translations/1016920/Guidelines%20ML%20TF%20Risk%20Factors_BG.pdf (last visited 25 February 2023).

EU Regulation (2023/a). Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1113 (last visited 15 March 2023).

EU Regulation (2023/b). Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1114 (last visited 15 March 2023).

European Commission (2022). REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities. Brussels, 27.10.2022. COM(2022) 554 final. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0554 (last visited 20 February 2023).

Fisher, D. (2022). "New FBI Unit Will Focus on Cryptocurrency Exploitation." In: DECIPHER. Security news that informs and inspires. 17 February 2022. [Online]. Available at: https://duo.com/decipher/new-fbi-unit-will-focus-on-cryptocurrency-exploitation (last visited 25 March 2023).

Flashpoint, Chainanalysis (2021). Hydra: Where The Crypto Money Laundering Trail Goes Dark. Sequencing Cryptocurrency Flows on the Russian Cybercrime Market "Hydra". [Online]. Available at: https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com/external/flashpoint-chainalysishydra.pdf (last visited 25 March 2023).

Foodman CPAs & Advisors (2022). "OFAC Asvierte A La Industria De Moneda Virtual". In: Foodman CPAs & Advisors. March 2022. [Online]. Available at: https://foodmanpa.com/ofac-advierte-a-la-industria-de-moneda-virtual/ *(last visited 15 March 2023).*

Goudinov, I. (2022). "Artificial Intelligence - a Weapon in Hybrid Warfare". In: *Mezhdunarodni otnosheniya*, issue 3-4 (1 August 2022). [Online]. Available at: https://spisaniemo.bg/author/ivo-gudinov/ (last visited 20 March 2023).

Keršanskas, V. (2020). *DETERRENCE: Proposing a more strategic approach to countering hybrid threats*. Hybrid CoE Paper 2, March 2020. Hybrid CoE. The European Centre of Excellence for Countering Hybrid Threats. [Online]. Available at: https://www.hybridcoe.fi/wp-content/uploads/2020/07/Deterrence_public.pdf (last visited 20 February 2023).

Law Library of Congress (2021). *Regulation of Cryptocurrency Around the World: November 2021 Update*. November 2021. LL File No. 2021-020594, LRA-D-PUB-002568. The Law Library of Congress, Global Research Division. [Online]. Available at: https://tile.loc.gov/storage-services/service/ll/llglrd/2021687419/2021687419.pdf (last visited 20 March 2023).

LPSPS (2023). Zakon za platezhnite uslugi i platezhnite sistemi [Law on Payment Services and Payment Systems]. Adopted by the 49th National Assembly on 28 July 28 2023. {Online]. Available at: https://www.bnb.bg/bnbweb/groups/public/documents/bnb_law/laws_payment_services_bg.pdf (last visited 15 April 2023).

Mihailov, G. (2014). "Opredelyane vacatio legis spored regulatornata otsenka." [Determining vacatio legis according to the regulatory assessment]. In: *Nauchni trudove na Rusenskiya Universitet* [Scientific Papers of the Ruse University], vol. 53, series 7, pp. 71-74. [Online]. Available at: https://conf.uni-ruse.bg/bg/docs/cp14/7/7-11.pdf (last visited 10 April 2023).

NBU (2020). POSTANOVA № 65. Pro zatverdzhennya Polozhennya pro zdiysnennya bankamy finansovoho monitorynhu [DECISION No. 65 On the approval of the Regulation on Financial Monitoring by Banks]. National bank of Ukraine, 21 May 2020. [Online]. Available at: https://bank.gov.ua/admin_uploads/law/19052020_65.pdf?v=4 (last visited 20 February 2023).

OFAC (2021). Sanctions Compliance Guidance for the Virtual Currency Industry. In: U.S. Department of the Treasury, Office of Foreign Assets Control, October 2021. [Online]. Available at: https://ofac.treasury.gov/media/913571/download?inline (last visited 25 February 2023).

Recorded Future for IBM Security QRadar. Joint Solution Brief. Joint Solution Brief. Recorded Future. [Online]. Available at: https://go.recordedfuture.com/hubfs/data-sheets/qradar-1.pdf (last visited 20 January 2023).

Robinson, P. (2021). "The Russian Hydra". In: *Irrussianality*, A Blog by Paul Robinson, professor at the University of Ottawa, 16 March, 2021. [Online]. Available at: https://irrussianality.wordpress.com/2021/03/16/the-russian-hydra/ (last visited 20 March 2023).

U.S. Department of Justice. (2022). Justice Department Announces First Director of National Cryptocurrency Enforcement Team. Press Release, 17 February 2022. Office of Public Affaires, U.S. Department of Justice. [Online]. Available at: https://www.justice.gov/opa/pr/justice-department-announces-first-director-national-cryptocurrency-enforcement-team (last visited 15 March 2023).

U.S. Department of the Treasury (2022/a). "Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex." Press Release 5 April 2022. U.S. Department of the Treasury. [Online]. Available at: https://home.treasury.gov/news/press-releases/jy0701 (last visited 15 March 2023).

U.S. Department of the Treasury (2022/b). *National Strategy for Combating Terrorist and Other Illicit Financing*. May 2022. [Online]. Available at: https://home.treasury.gov/system/files/136/2022-National-Strategy-for-Combating-Terrorist-and-Other-Illicit-Financing.pdf (last visited 20 February 2023).