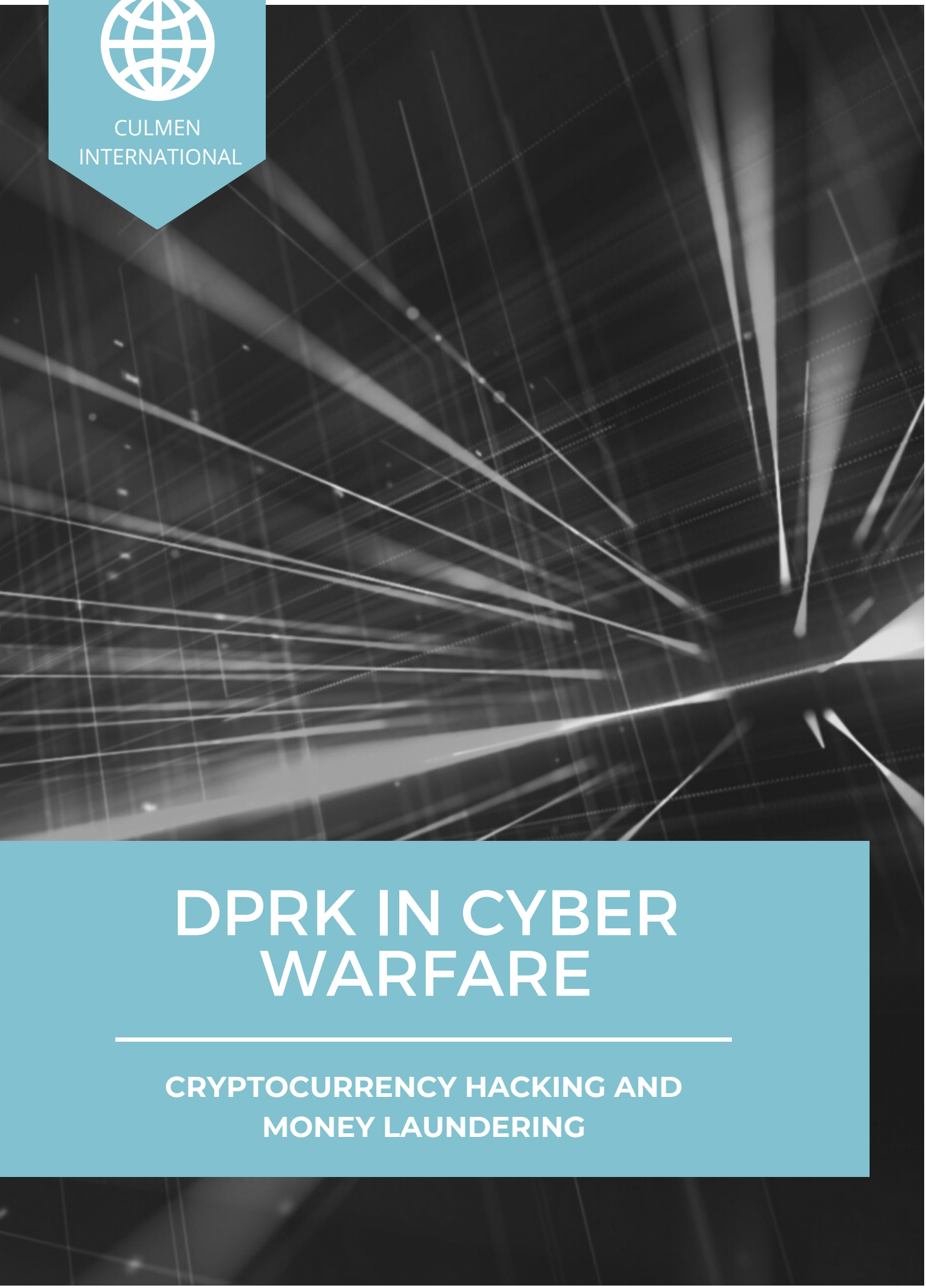


CULMEN INTERNATIONAL

DPRK IN CYBER WARFARE

CRYPTOCURRENCY HACKING AND MONEY LAUNDERING

INCREASING RISKS

The March 2023 report of the U.N. Panel of Experts overseeing sanction on North Korea revealed rising source of fund from increase in illicit maritime activity and theft of cryptocurrency by North Korea.

This report raised concerns on North Korea engaged in illicit activities and their impact on global security, as well as their ability to circumvent international sanctions to finance it nuclear program.

For years North Korea, confronted embargo, trade sanction and denied access to fiat currency, has sought to alternative means of laundering money to evade U.S. and UN sanctions. In the past, North Korea has focused on attacking financial institutions including the Bank of Bangladesh, Taiwan's Far Eastern International Bank, and ATM networks throughout Africa and Asia region.

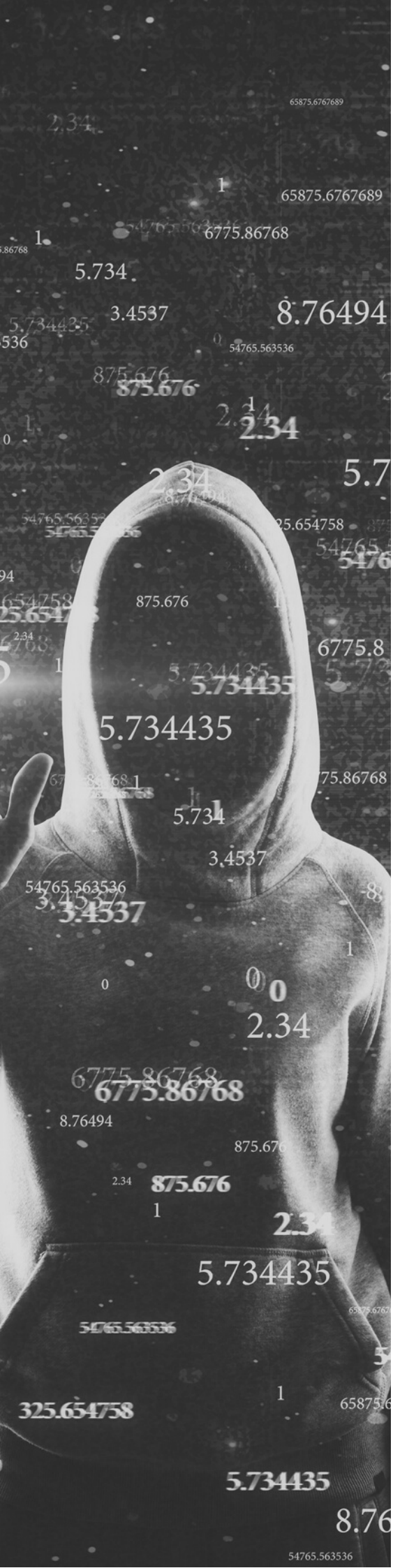
But the emerging crypto economy has opened a window for them to fund their military weapons. The cryptocurrency introduces new global financial risks from hacks to ransomware to money laundering.

IINCREASING RISKS

In the past five years, several cyberattacks—stealing directly from cryptocurrency exchanges, have been identified were orchestrated by DPRK. Particularly the notorious “Lazarus Group”, also known as “APT38” is the threat group sponsored by DPRK specialized in financial cyber operations which has been attributed to the Reconnaissance General Bureau.

Since Lazarus Group first gained its name from its Sony Pictures and WannaCry cyberattacks, it has concentrated on cryptocurrency crime, which proved to be profitable immensely.

Cryptocurrency for the nature of decentralization and anonymity, has become the most robust vehicle employed by the DPRK for money laundering. From 2018 to the present, estimated hackers linked to DPRK have stolen more than $3 billion that is being channeled into funding the country’s nuclear missile program.



METHODS

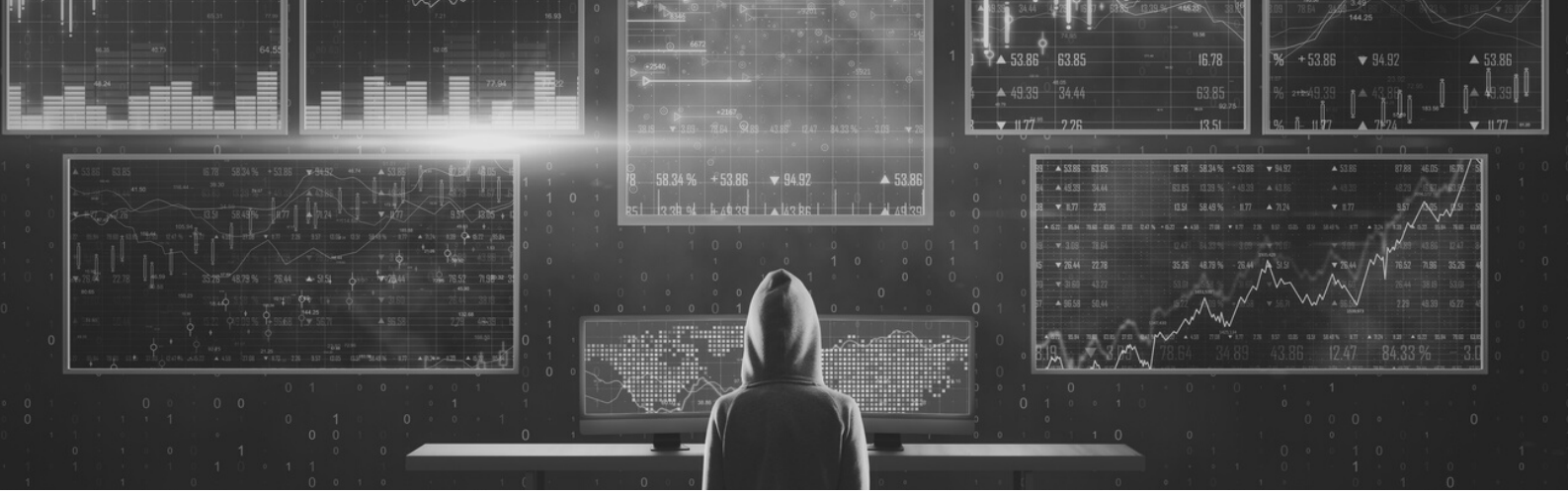
INCLUDE:

North Korea takes the full advantage of the cryptocurrency's anonymity and regulatory disparities between jurisdictions across the world. Attacks targeting cryptocurrency service providers, including:

- **Malicious cryptocurrency apps**
- **Hacking attacks**
- **Ransomware attacks**
- **Spear phishing emails**
- **Fraudulent Initial Coin Offerings (ICO)**

After hacks and stealing cryptocurrency, hackers seek to launder them through cryptocurrency exchange services with weak KYC verification/AML program and recent case shown often use Mixer-known as software tools that pool and scramble cryptocurrencies from thousands of addresses for money laundering. Diversity the use of different Mixers that further obscure the origin of the illicit funds.

At last stage of money laundering, to be able to cash out, Bitcoin is sent to deposit addresses at crypto-to-fiat, most of them based in Asia, but most recently, identified increasing use of Russia-based exchanges to launder illicit crypto assets.



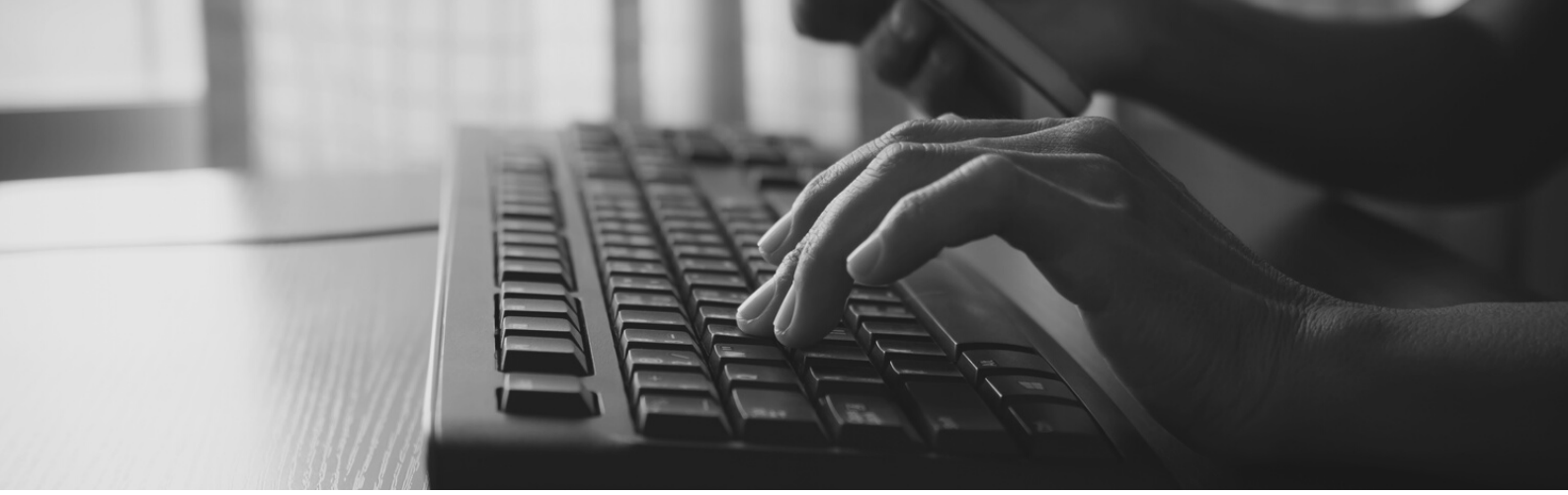
HIGH PROFILE HEISTS

Between 2020 and 2022, the Mixers such as Tornado Cash, Blender, and Sinbad were used to launder cryptocurrency stolen in hacks. The Harmony case also reflect the recent development of close partnership and historical arms meeting between two leaders of DPRK and Russia, most recent hacks shown that DPRK-linked hacking groups are increasing their use of Russia-based exchanges known to launder illicit crypto assets.

The following are some example of cryptocurrency hacking and money laundering linked to DPRK:

- ·The theft of $31.6 million form South Korean crypto exchange Bithumb in 2017. North Korean hackers moved the stolen cryptocurrency to their own wallets and then transfer to a Yobit, a Russian cryptocurrency exchange.

- ·Kucoin case: In 2020, North Korea's Lazarus Group has been linked to the hack of a crypto exchange in Singapore, KuCoin, from which it stole crypto assets worth $280 million. Some of the funds were laundered through DEXs – an indication that North Korea is capable of exploiting DeFi technology.



HIGH PROFILE HEISTS

CONTINUED

- ·Tornado Cash, an entity that provides virtual currency mixing services, obfuscated the movement of over $455 million stolen in March 2022 by the OFAC-designated, DPRK-controlled Lazarus Group in the largest known virtual currency heist to date. Tornado Cash was sanctioned in August and in November 2022 delisted and redesignated Tornado Cash under E.O. 13722 and E.O. 13694.

- ·Harmony case: On 08/22/2023, the FBI confirmed that the North Korean malicious cyber actor group Lazarus was responsible for the theft of $100 million of virtual currency from Harmony's Horizon Bridge reported on June 24, 2022.[2] $21.9 million in cryptocurrency stolen from Harmony Protocol was transferred to a Russia-based exchange known for processing illicit transactions.

Despite UN Security Council Resolutions and U.S. OFAC sanctions which have imposed global and extreme sanctions on North Korea. International governments and authorities often struggle to punish individuals responsible and instead rely on sanctions to deter further attacks.

The abovementioned illicit cryptocurrency attacks indicated that decentralized protocols and Defi services should be subject to the compliance obligations to which centralized financial service providers adhere.

NEW REGULATIONS

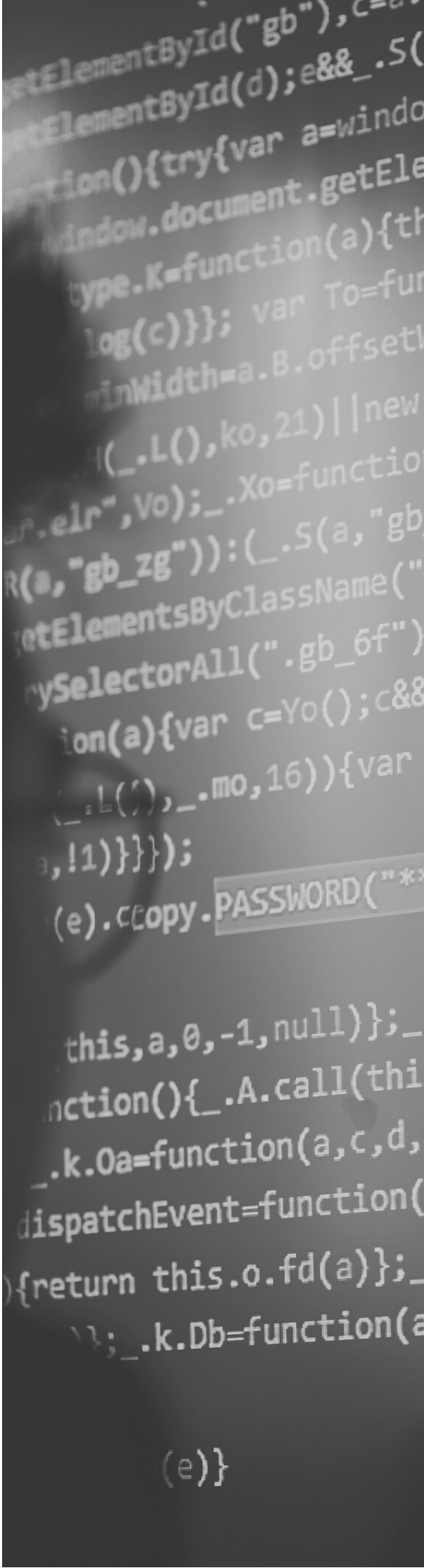
President Joe Biden's executive order on crypto from last year, and other jurisdictions including the European Union have also started tackling money laundering risks associated with DeFi services and money laundering with cryptocurrency.

Evidently, the updating of the new regulations for compliance in crypto can efficiently track and prevent illicit activities. It should be noted that there are no specific regulations applied to cryptocurrency. Many regulatory authorities have introduced their own frameworks for cryptocurrency regulation. Here is regulations framework fall under different domain of compliance for crypto:

- ·Financial Crimes Enforcement Network (FinCEN): Cryptocurrency service providers should implement an AML compliance program and obtain a license from FinCEN. FinCEN also stipulates the need for maintaining records and submitting timely reports to relevant authorities.

- ·Securities of Exchange Commission: SEC recently announced the separation of asset custody from registration and regulation of cryptocurrency. SEC also collaborates with the Commodity Futures Trading Commission or CFTC to monitor the compliance on crypto trading platforms.

- ·Commodity Futures Trading Commission: CFTC defines cryptocurrencies as commodities. However, it also pointed out the limited regulatory oversight and authority over commodity cash markets.



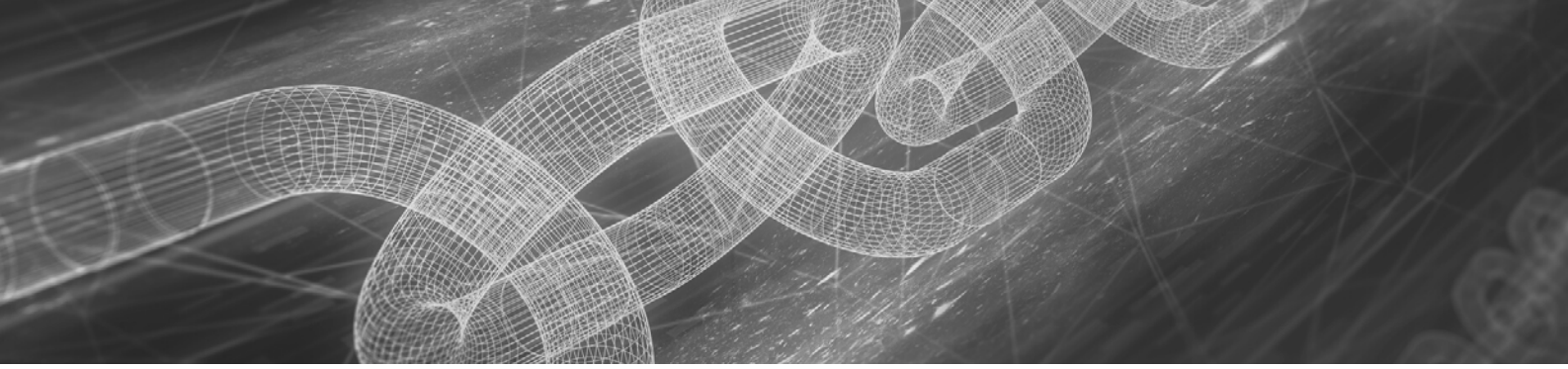
NEW REGULATIONS

.

- ·Options Clearing Corporation: The OCC mandated that national banks and federal savings associations could connect with blockchain networks and use cryptocurrencies for payment transactions.

- ·Office of Foreign Assets Control (OFAC): OFAC improves crypto compliance by including virtual currency addresses associated with authorized persons on the SDN list. The SDN list is basically the Specially Designated Nationals and Blocked Persons list.

The abovementioned cryptocurrency hacking cases indicated their weakness on KYC/CDD requirement and AML/CFT compliance. We can identify when Defi protocols and cryptocurrency exchanges fail to comply with the appropriate regulator, fail to establish efficient AML/CFT controls or do not comply, criminals are more likely to exploit their services successfully, including to circumvent U.S. and United Nations sanctions.



WHAT TO DO

Therefore, a robust compliance program can help to detect, mitigate, and prevent the risk raised from the use of cryptocurrency for illicit activity and money laundering by bad actor like North Korea. The following measures commonly suggested for compliance in cryptocurrency:

- Effectively implement the Financial Action Task Force (FATF) standards on AML/CFT/CPF.
- ·Identifying red flags and criminal typologies to ensure the internal control.
- ·Establish risk assessment in implementation of compliance measures.
- ·Build a compliance team equipped with the capability and skills to identify potential threats.
- ·Integrate compliance technology into crypto compliance.

Cutting off North Korea's cryptocurrency pipeline has become a national security imperative for the government. To use the stolen digital money or remittances from North Korean IT workers abroad to fund its weapons programs is part of the regular set of intelligence products.

2017 UN Security Council resolution required all Member States to repatriate DPRK nationals earning income abroad, including IT workers, by December 22, 2019. The United States also seeks to enhance the capacity of foreign governments and the private sector to understand, identify, defend against, investigate, prosecute, and respond to DPRK cyber threats and participate in international efforts to help ensure the stability of cyberspace.

The governments, industry, civil society, and individuals should take all relevant actions and measures to protect themselves from and counter the DPRK cyber threat. If an organization detects that it has been the victim of malicious cyber crime associated with North Korea, to notify law enforcement is required. This not only can open the investigation in a timely manner, but also can help to recover the stolen assets. (Win a reward: please visit www.rewardsforjustice.net to win the rewards up to $5 million for providing the information to US Department of State about illicit DPRK activities in cyberspace).

CULMEN CAN HELP

If you have questions regarding DPRK sanctions evasion, Culmen International can help. Contact us if you have questions ragarding improving due dillgence and compliance procedures.

Prepared by Culmen International