

Onorevoli membri della commissione. Grazie per l'opportunità di presentare il mio punto di vista in merito a questa importante riforma e apportare il mio contributo al miglioramento della stessa.

Sono Nicola Buonanno e sono il Vice Presidente per Chainalysis per il Sud-Europa, il Medio Oriente, l' Africa ed il centro-sud dell'Asia.

La mia area di competenza ed esperienza è legata al mondo degli strumenti di analisi delle attività che coinvolgono la **blockchain** con specifico focus sulle tematiche di **investigazione, cyber crime e sicurezza nazionale**. L'azienda che rappresento collabora già attivamente in questi ambiti con le principali agenzie di sicurezza e forze di polizia internazionali che si occupano di monitorare, contrastare e perseguire reati che coinvolgono asset virtuali che insistono sulla blockchain come le criptovalute.

In un'era in cui le tecnologie digitali permeano ogni aspetto della nostra vita, i criminali sfruttano queste stesse tecnologie, assolutamente legittime ed innovative, per condurre attività illecite. I criminali hanno infatti sempre sfruttato per primi le rivoluzioni tecnologiche, succede per il web, l'Intelligenza Artificiale ed ovviamente anche per le criptovalute che sono sempre più utilizzate come metodo di pagamento per crimini che potremmo definire "crypto-native" - come i ransomware - ma in misura sempre maggiore anche per i reati più *tradizionali* come il riciclaggio, il finanziamento del terrorismo ed anche lo spaccio di droga attraverso l'utilizzo di darknet market (i [dati che abbiamo rilasciato](#) con i volumi di transazioni osservabili sulla blockchain legata al fenomeno del Fentanyl lungo tutta la catena di approvvigionamento e distribuzione ne sono un esempio lampante).

Crypto and the Opioid Crisis: What Blockchain Analysis Reveals About Global Fentanyl Sales [UPDATED 3/7/24]

MAY 24, 2023 | BY CHAINALYSIS TEAM



Si coglie pertanto con piacere questo DDL che è un importante passo avanti alla lotta al crimine cibernetico, che inasprisce le pene ed aumenta competenze e risorse necessarie al suo contrasto.

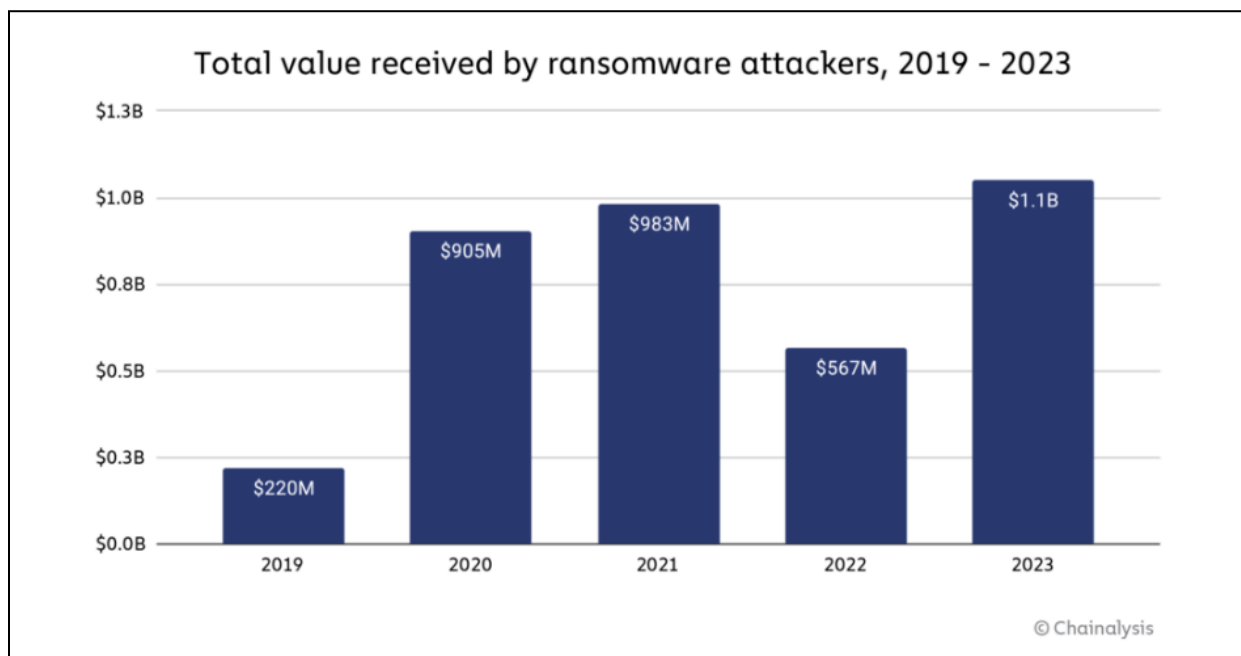
Ritengo che la bozza vada nella direzione giusta ma a titolo propositivo vorrei portare la vostra attenzione sull'importanza cruciale di strumenti di blockchain intelligence nel contesto della prevenzione e del contrasto dei reati informatici e sulla necessità di considerare in questo **DDL Cyber** la creazione di **centri di competenza** nazionali e regionali, con mandato di tipo **operativo** al fine di prevenire e contrastare in maniera coordinata i principali reati informatici che sempre di più vedono un crescente utilizzo di tecnologie abilitate dalla blockchain e che **non sono oggetto di questa bozza.**

Contrasto ai Ransomware

Secondo i dati di Chainalysis, il 2023 è stato l'anno dei record per i ransomware, con i riscatti pagati dalle vittime eccedenti un **miliardo di dollari**.

Secondo [un report](#) apparso anche sulle principali agenzie di stampa 6 giorni fa, l'Italia è il paese più colpito in Europa ed il [terzo al mondo](#). Vittime di questi attacchi sono prettamente la PA, gli ospedali e le PMI.

Nessuno di questi soggetti può contrastare da solo questo fenomeno che ha contorni internazionali molto complessi. Il mondo dei ransomware è infatti un fenomeno internazionale, molto articolato e sorprendentemente strutturato. Siamo di fronte a vere e proprie organizzazioni multinazionali del crimine, che a volte collaborano in maniera più o meno dichiarata con governi stranieri a noi ostili e che puntano a destabilizzare il nostro Paese.



Per mezzo di strumenti di analisi della blockchain si può non solo portare avanti studi predittivi degli attacchi ma anche fare luce sulla killchain e porre in essere azioni di risposta efficaci **mettendo il luce connessioni altrimenti invisibili.**

Un esempio concreto viene dall' **Operazione Cronos**, una complessa azione di polizia annunciata a febbraio 2024 coordinata dalla National Crime Agency (NCA) del Regno Unito in collaborazione con l'Europol, FBI ed altre forze di polizia internazionali. L'operazione ha portato al sequestro di siti web operati dalla gang Lockbit, una delle gang ransomware più prolifiche al mondo, nonché all'arresto di due dei suoi membri.

In questa operazione, l'analisi dei flussi di criptovalute e la collaborazione co Chainalysis, come apertamente dichiarato dalla NCA, è stata fondamentale per mappare i movimenti finanziari dei componenti del gruppo criminale.



L'infografica presentata dalla NCA che menziona la collaborazione con Chainalysis in Operazione Cronos

Paesi “canaglia” e furto di crypto asset

Il furto di criptovalute per mezzo di azioni di hackeraggio di wallet personali o di operatori del settore è un altro tema estremamente rilevante all'interno dei crimini più diffusi. Mi preme però sottolineare che in alcuni casi trattasi non solo di un reato informatico ma anche di un tema di sicurezza. Si basti pensare che che l'organizzazione di hacker **Lazarus Group**, legato al regime della Corea del Nord, nel solo 2022 ha portato avanti azioni di hackeraggio per rubare criptovalute totalizzando un bottino totale di quasi \$1.7 Miliardi!

Per metterlo in contesto, il totale delle esportazioni della Corea del Nord è inferiore a \$250M. Il furto di criptovalute è quindi un pilastro della economia del regime il che potrebbe non sembrare un tema di sicurezza internazionale ma lo diventa dal momento che ci sono [evidenze](#) che questi fondi siano destinati al programma nucleare del regime di Pyongyang.

Finanziamento al Terrorismo

Anche il terrorismo internazionale vede un crescente coinvolgimento di questi strumenti. Il fenomeno è ancora in larga parte finanziato con metodi tradizionali ma sempre di più sta crescendo l'utilizzo delle criptovalute.

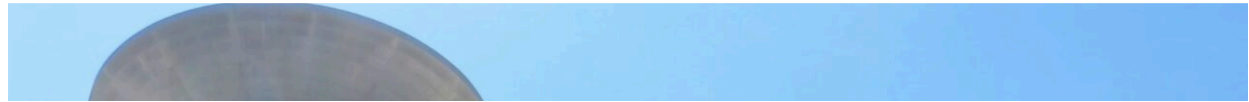


Esempio di una campagna di finanziamento tramite criptovalute promossa dai mujahidin in Syria

Utilizzando strumenti di blockchain intelligence, il 27 giugno scorso, l'Ufficio nazionale israeliano per il contrasto al finanziamento del terrorismo (**NBCTF**) ha sequestrato per la prima volta criptovalute provenienti da **Hezbollah** e dalla **Forza Quds dell'Iran**, che finanzia e collabora ampiamente con Hezbollah. In totale, l'agenzia ha sequestrato circa 1,7 milioni di dollari di criptovalute ma soprattutto interrotto la catena di finanziamento basata su questi strumenti. Siamo orgogliosi di poter affermare che gli strumenti di Chainalysis hanno avuto un ruolo in questo importante risultato per la sicurezza internazionale

Chainalysis In Action: Israeli Authorities Disrupt Hezbollah and Iran Quds Force Terrorism Financing Crypto Infrastructure, Seize \$1.7 Million in First

JUNE 27, 2023 | BY CHAINALYSIS TEAM



Conclusioni

Onorevoli membri, la lotta al cyber crime in un mondo digitale richiede strumenti all'avanguardia e un approccio innovativo. La blockchain intelligence rappresenta una risorsa preziosa per identificare, tracciare e contrastare le minacce alla nostra sicurezza.

Le transazioni che avvengono sulla blockchain ed in cripto valute **non sono anonime** ma pseudonime e sfruttando la trasparenza e immutabilità delle stesse possiamo concatenare eventi anche in apparenza non correlati e generare fonti di intelligence estremamente rilevanti.

Il fenomeno discusso è un fenomeno globale, che coinvolge organizzazioni molto strutturate e potenti come Mafie, organizzazioni terroristiche e sempre più governi ostili all'occidente che utilizzano questi strumenti all'interno delle loro strategie di attacco e destabilizzazione.

Si suggerisce di stanziare **risorse** per la creazione di **centri di eccellenza**, sia presso l'**ACN** che a livello **regionale** al fine di aumentare la resilienza del Paese. In quest'ottica, ritengo che possa essere molto utile prevedere l'adozione di soluzioni specifiche di monitoraggio delle blockchain a scopi di analisi preventiva e risposta rapida e credo che la tematica sia complementare con le soluzioni di intelligenza artificiale di cui all'**articolo 7** per cui si suggerisce l'adozione.

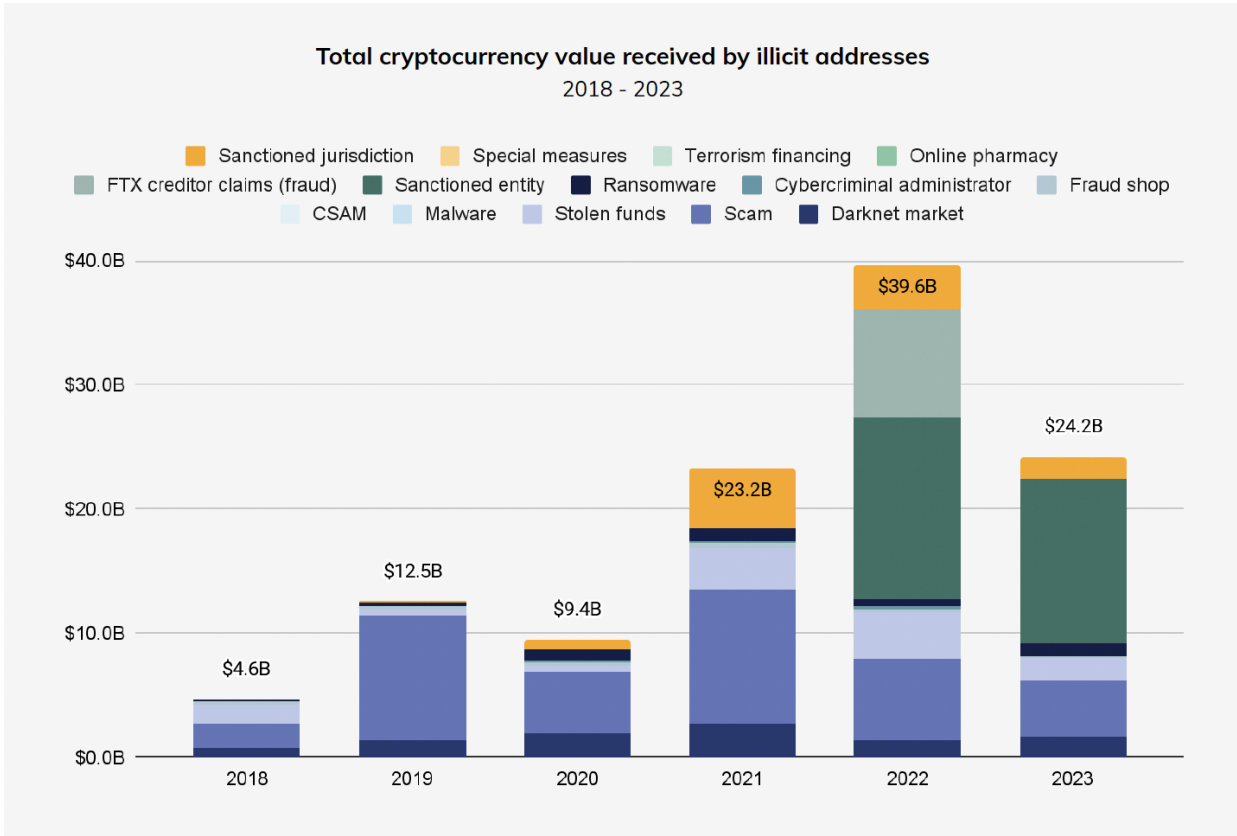
Considero inoltre fondamentale investire in **formazione** e si coglie con favore il riferimento a specifici percorsi di specializzazione di cui all'**articolo 9**. Dalla mia esperienza, considero però

essere più efficace la strada dell'**incentivazione**, superando limiti che potrebbero allontanare professionalità invece che attrarle in questa agguerrita caccia internazionale dei talenti. Ritengo quindi auspicabile l'introduzione di ulteriori incentivi come la possibilità al personale distaccato presso l'ACN di mantenere il proprio ruolo all'interno dell'amministrazione o corpo di origine, al fine di facilitare il reperimento da parte dell'Agenzia dei migliori talenti.

Si vede inoltre con favore la possibilità di estendere le competenze della ACN dandole un **mandato di carattere operativo** all'interno delle tematiche di sicurezza cyber. Tale tema, come esposto sopra, tocca spesso aspetti di sicurezza nazionale e quindi sembra opportuno trattarla come tale estendendo al personale di ruolo dell'ACN i benefici delle leggi di cui godono le Agenzie per la **sicurezza nazionale** nell'ambito del contrasto ai crimini informatici di cui all'**articolo 5**. Questo abiliterebbe una possibilità di una efficace azione di monitoraggio e contrasto al fine di aumentare aspetti di sicurezza e resilienza cibernetica

La rivoluzione delle blockchain va molto al di là del fenomeno delle cryptovalute che ne sono solo un aspetto collegato. Affrontare un tema complesso come quello del cyber crime senza dotarsi di strumenti di blockchain intelligence sarebbe estremamente limitante. Risulta pertanto essenziale disporre degli strumenti e delle competenze necessarie per interpretare e utilizzare queste informazioni in modo efficace, creando una rete di coordinamento capace di collaborare sia a livello nazionale che internazionale al fine di contrastare un fenomeno sempre più globale ed articolato.

In allegato alla mia relazione aggiungo il nostro **Crypto Crime Report 2024** appena rilasciato ed in cui si analizzano i principali crimini che coinvolgono l'uso di cripto asset per un totale di oltre 23 miliardi di dollari nel solo 2023.



Grazie per la vostra attenzione e buon lavoro,

Nicola Buonanno