THE FUTURE OF CYBER ENABLED FINANCIAL CRIME:

New Crimes, New Criminals, and Economic Warfare

A Threatcasting Lab Report

ASU

THE FUTURE OF CYBER ENABLED FINANCIAL CRIME:

New Crimes, New Criminals, and Economic Warfare

Analysts:
Brian David Johnson - ASU
LTC Jason C. Brown - ACI/USMA
Josh Massad - Deloitte
Christopher Owens - USSS

The Threatcasting Lab is supported by

This project was supported by US Army Grant No. W911NF-20-1-0330.

ASU THREATCASTING LAB

Brian David Johnson	Director
Cyndi Coon	Chief of Staff
Ana Abasta	Coordinator
MDX Arts	Report Editor
MORR Design	Layout/Design

Arizona State University Threatcasting Lab

The Threatcasting Lab at Arizona State University serves as the premier resource for strategic insight, teaching materials, and exceptional subject matter expertise on Threatcasting. By using its approach, experts from multiple disciplines envision possible threats ten years into the future. The lab provides a wide range of organizations with actionable models to comprehend these possible futures as a means to identify, track, disrupt, mitigate, and recover from the possible futures as well. Its reports, programming, and materials bridge gaps, and prompt information exchange and learning across the military, academia, industrial, and governmental communities.


NEODENARIUS

Research Question:

What will the future of cyber-enabled financial crime, perpetrated by either criminals or nation states, look like 10 years from now?

In the coming decade, those who engage in cyber-enabled financial crimes (CEFC) will take advantage of a collection of technologies and adjacent practices -- creating new classes of crimes, conditions, and adversary vectors. There are numerous technologies at the forefront of societal evolution, including cryptocurrency, artificial intelligence, 5G, physical and digital autonomous systems, the Internet of Things (IoT), Smart Cities, biometric identity, space-based systems, and quantum computing. The combination of changes in these technologies and in society are likely to also include an over-reliance on digital devices, digital payments, monopolized smart systems, and broader technology dependencies. In addition, the nature of financial crimes is expected to change in that they will initially target vulnerable communities, consumers, companies, and cyber computer systems. Furthermore, financial crimes will increasingly be used to enable more advanced and egregious economic warfare opportunities for adversarial nations and nation-state proxies.

THREATS

- **New Financial Crime(s)** - Small target/ scale crimes by individuals and organizations for financial gain.
- **Economic Warfare** - Large scale economic warfare attacks by nation-states and their proxies to destabilize economies and erode trust.
- **A Ladder to Chaos** - A ladder from small to large targets wherein financial crimes mask a broader nation-state attack.
- **CEFC Conditional State** - A conditional state with a vacuum for criminals to expand “new crime” and for nation states to wage geopolitical, economic warfare.

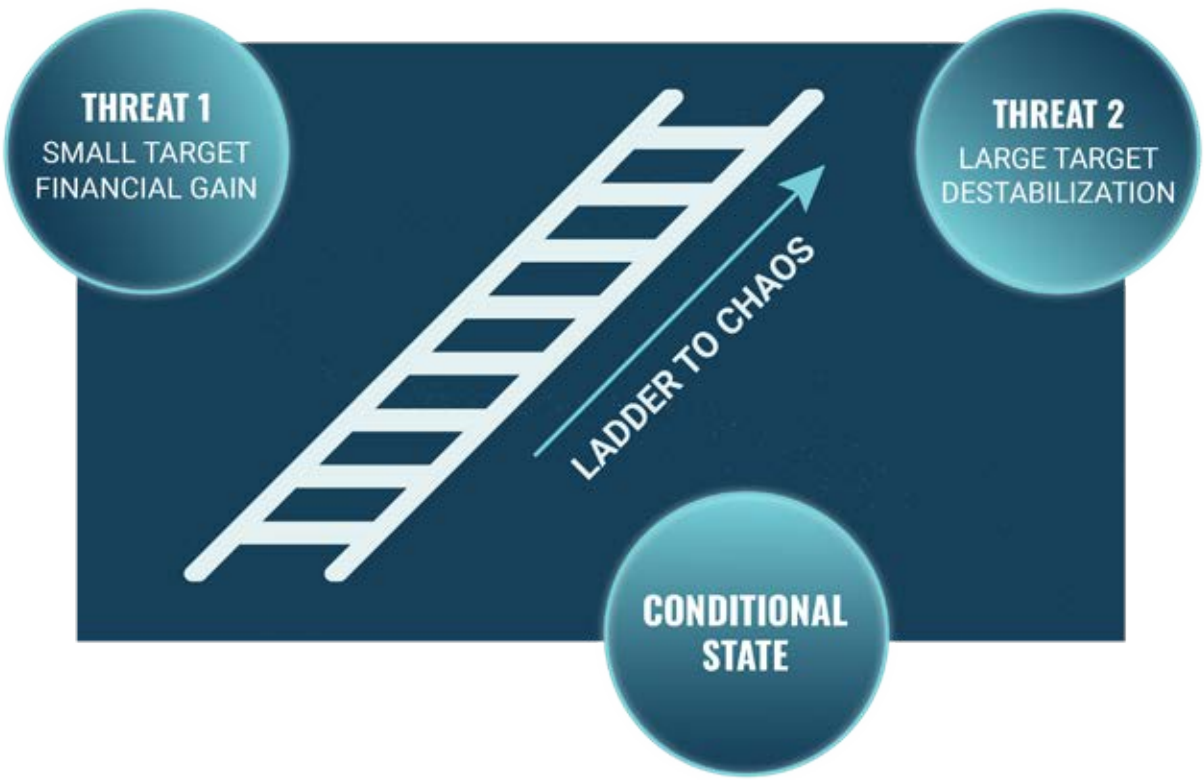
ACTIONS TO BE TAKEN

To disrupt and mitigate these threats, Federal Law Enforcement organizations should consider:

- Aligning their functional definition of CEFC technology and adjacent practices. The definition should address the differences between traditional financial crime and “new crime” that includes the increased impact of speed, scope, and scale of CEFC to federal law enforcement.
- Building a plan to empower, protect, and engage vulnerable communities (including consumers, companies, and computer systems) through lawful

monitoring systems that take into account the importance of identity, confidentiality, integrity, and availability.

- Developing a plan for tracking and monitoring emergent CEFC through sharing best practices across federal and local law enforcement, and the U.S. Department of Defense (DoD).
- Determining how to identify what is behind instances of CEFC, in order to unmask a potentially linked broader nation-state attack.
- Developing processes to pass the identification and intelligence of a CEFC from law enforcement to the DoD when jurisdictionally appropriate.
- Further exploring CEFC's pre-crime conditional state with indicators to watch out for and actions to take. Precedents exist for this shift, from a single criminal focus to conditional indicators, such as natural disasters and mass migration.
- Treating cryptocurrencies like real property.



I am pleased to introduce this report jointly sponsored by the U.S. Secret Service and the U.S. Army Cyber Institute. It takes a rigorous, academic look at the insights of economists, bankers, strategists, futurists, and law enforcement professionals' consideration of potential future cyber-enabled financial crime scenarios.

Produced by Arizona State University's Threatcasting Lab, The Future of Cyber-Enabled Crime: New Crimes, New Criminals, and Economic Warfare will help policymakers and law enforcement personnel examine and prepare for the possible future consequences of complex, algorithm-driven financial systems, and their impact on U.S. and global economies.

As a federal agency responsible for investigating individuals and organizations engaged in crimes against the U.S. financial infrastructure, the Secret Service must continue to stay on the cutting edge of emerging financial and economic trends, including quantum computing and related encryption issues. Vulnerabilities in developing artificial intelligence and machine learning algorithms present new opportunities for cyber criminals determined to exploit financial systems for financial gain and economic disruption. As such, examining future threats is essential to readying policymakers, federal agencies, banking institutions, and the public to identify potential risk and respond accordingly.

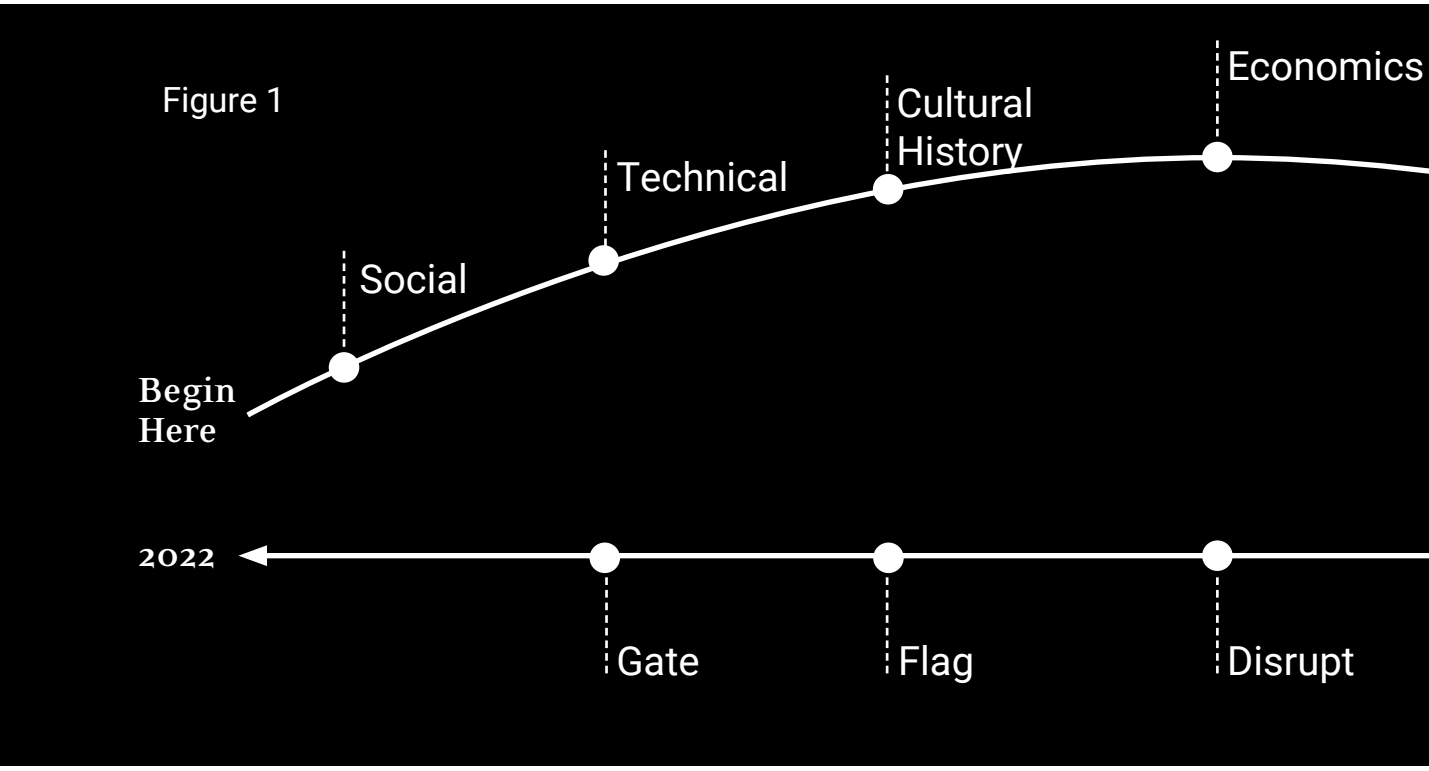
I encourage all readers of this report to consider the vast scope of changes we have seen in recent years and imagine the broad range of innovation yet to come. As we advance technologically and socially, our adversaries will continue to evolve as well, using innovative methods to attack our systems and way of life. Adopting strategic foresight is essential to stay ahead of these threats and protect our financial infrastructure.

Gregory W. Try
Chief Strategy Officer
United States Secret Service

INTRODUCTION TO THREATCASTING

Threatcasting provides a systematic and transparent method to model a range of possible futures and threats in a complex and uncertain environment. Working with organizations via subject matter expert interviews, participatory workshops, and operationalization exercises, it provides decision-makers specific indicators that one or more of the futures or threats are manifesting, with suggestions or possible actions that can be taken to disrupt the threat or pursue more desirable visions of the future.

Threatcasting is not designed to "predict" the future. Rather, the output of the methodology provides organizations and decision-makers a framework by which to

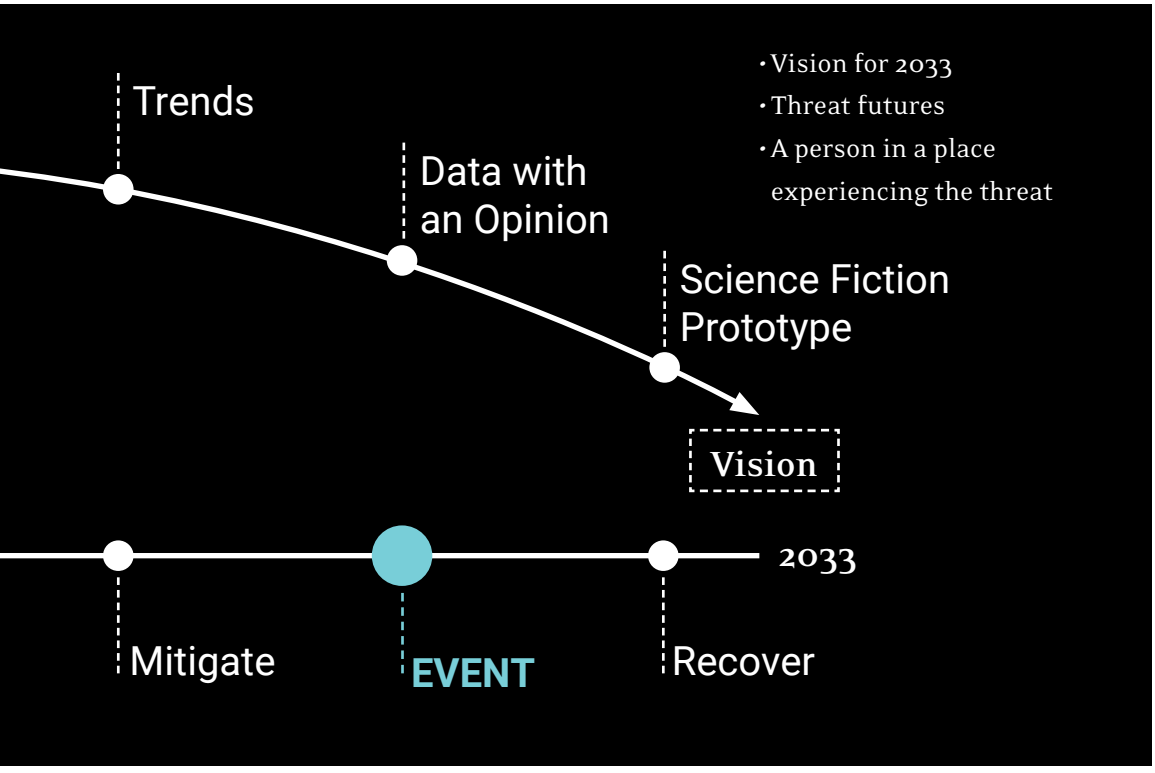


plan, prepare, and make decisions using their own perspectives on how the threats affect them.

Threatcasting often guards against strategic surprise. When a crisis occurs or an opportunity presents itself, a decision-maker or a leader is not caught off guard. Rather, their reply is: "We have talked about this before. We know where to start."

For this project, a cross-functional group of practitioners gathered for two days in November 2021, to create models of cyber-enabled threat futures. The outcomes of the session provided the initial framework for a set of possible threats, external indicators, and actions to be taken. Drawing upon research inputs from diverse data and from subject matter expert interviews, participants synthesized the data into workbooks and then conducted three rounds of effects-based modeling.

In the Threatcasting sessions, participants generated numerous scenarios, each with a person, in a place, experiencing their own version of the threat. After the workshop concluded, analysts examined these scenarios to categorize and aggregate novel indicators of how the most plausible threats could materialize during the next decade and what the implications were for gatekeepers' standing in the way of the threats. While not predictive in nature, this process gives organizations a starting place to consider how CEFCs might affect them.



FINANCIAL CRIME FRAMEWORKS

This section covers how two existing crime frameworks were used to help make sense of the threat models developed in the Threatcasting workshop.

The first framework follows Peter Gottschalk's approach: This framework classifies financial crimes into families with similar characteristics.[1] Although Gottschalk's approach does not account for the emergence of digital currencies, his categories are useful for identifying the problem space. The Threatcasting lab adjusted some of Gottschalk's original classifications to better account for the future of CEFC.

- **FRAUD FAMILY**—These crimes include misrepresentation or deception with the intent of financial gain. This category encompasses traditional fraud crimes, including the ones closely aligned to digital currencies and crypto (e.g., identity theft, counterfeiting, Ponzi schemes, yield farming, liquidity farming, and rug pulls).
- **THEFT FAMILY**—These crimes involve taking money or things of value, but without the misrepresentation that normally accompanies the fraud family of crimes. Examples include hacking and stealing private crypto keys, emptying an exchange, street-level mugging, and embezzlement.
- **MANIPULATION FAMILY**—This group of crimes adopts some of the more esoteric types of CEFC, such as influencing markets or prices, and developing cyber access for follow-on fraud or theft. Although developing cyber access may not first appear as a type of financial crime, the purpose behind most cyber intrusions is to steal data for resale, or for manipulating data for some future monetary gain. Causing an organization to react to an expensive cybersecurity threat is a form of manipulation, making these intrusions arguably a form of financial crime.
- **CORRUPTION FAMILY**—This category of crimes uses force, fear, and/or required payments for favorable treatment. Ransomware falls into this category, even though it might at first appear to better fit in the "theft" bucket. Ransomware is a type of corruption

offense because attackers often put a deadline into their demands, with the threat of some type of data spillage or permanent system lock-out if the demands are not met.

- **OTHER**—These crimes are adjacent to CEFC but are not necessarily "financial" crimes. The development of digital economies will bring with it crimes against society that create a social divide or a category of being "left behind". While to many, this may seem like figurative social Darwinism ("keep up or die"), for the most socially vulnerable, "dying" could be quite literal. Consider electronic bank transfers for welfare recipients. Having all benefits tied up in cumbersome, difficult to audit, and opaque systems puts people at real-life risk of starvation, disease, and death if they are unable to access their benefits and buy food.[2] This can be seen as an indicator of laddering up from small- to large-target crimes if these systems ever succumb to cyberattacks or other categories of financial crimes.

1 Gottschalk, *Categories of Financial Crime*, 441–58.

2 Team Obol 1 imagines Lisa, a low-income and food insecure single mother, whose access to government assistance is threatened as unattended algorithms continue to flag her account for trustworthiness problems caused by other algorithms. "The convergence of digital payments dominating the life of the average person and the over-reliance on AI to mete out services and civil punishments has left her destitute and hard-pressed to improve her situation." See sidebar The Perils of Cyber Enabled Social Support on page 44

THE CRIME TRIANGLE

The second framework considered was the “The Crime Triangle”.[3] Also known as a problem analysis triangle, this framework posits that three things need to occur simultaneously for a crime to happen. As shown in the image, the inner triangle consists of a target/victim, a place, and an offender. All three of these need to be present at the same time for a crime to occur. The outer layer of the triangle shows what is needed to mitigate the crime. A guardian protects the target, a handler monitors the offender, and a manager watches over the place. If just one section of the outer layer is present, the crime can be blocked.

3 The crime triangle (also known as problem analysis triangle) comes from one of the main theories of environmental criminology – the Routine Activity Theory, cited from Cohen and Felson, *Social Change and Crime Rate Trends : A Routine Activity Approach*, 588–608.

HISTORICAL CONTEXT:
The Dutch East India Company

To explore the transition from traditional financial crime to CEFC, cultural historian Jamie Carrott researched other examples of the privatization of currency and levers of power.[4] The Dutch East India Company (known scholarly as VOC[5]) and the English East India Company (EIC), give early examples of these types of transitions.

The following are some historical implications for the future of CEFC:

Piracy isn't just piracy.

Piracy is not just about theft. Piracy (officially "privateering") drove the global power shift in the early modern world. It allowed the relatively poor and scrappy English and Dutch to take down the Spanish and Portuguese empires, and was central to the success of both the Dutch and English East India Companies. It would not be an exaggeration to say that both companies were founded on silver and gold stolen from Spanish treasure fleets. Theft funded the whole enterprise, and it built upon itself. The VOC massacred indigenous populations in their quest to control the spice trade. The EIC[6] turned mercenary, and acted as a drug kingpin to build an empire that lasted into the middle of the 20th century, which ultimately drained significant wealth out of India.

When watching for change, look to the fringes.

Chipping away at the edges of a situation eventually undermines the dominant paradigm. Each individual act of rebellion or piracy may be survivable, but an empire can collapse under the cumulative weight of a thousand “cuts”. What shifts the paradigm is not the piracy itself, but rather the undermining of the system – and blind faith in the system – that erodes “the dam” bit by bit, until the dam breaks and the river changes course.

When raw power is at risk, it is generally those on the edge of the power who are willing to break the rules and facilitate power shifts.

The medium is the message.

Money is not just about the raw power of exchange. An individual or group who issues, controls, and manipulates currency has substantial cultural power. The Portuguese established a monetary lingua franca or common language in the Asia trade. From the late 15th through 16th centuries, trade became normalized around a base value of the coin. Additionally, minting coins was highly symbolic. Specie, or money in the form of coins, was a literal representation of power--embodying their value in gold or silver. Rulers used coins to communicate power. Throughout the Mughal and European wars of the 18th century, one of the first things any new conqueror did was mint coins in their image. Digital currency, of course, lacks the physical symbolism or literal worth of a coin. What it does not lack, however, is the ability to communicate power. All forms of monetary exchange inherently contain a level of power.

Think flexibly.

Criminals are willing to break rules for personal influence, power, and profit. Often, they have little regard for countries, corporations, or other organizations. This requires organizations to think flexibly.

In the early modern world, power was less balanced, and the public vs. private dichotomy did not exist. Kings, Queens, and councils could delegate power in ways that today, most would find uncomfortable. An example of this is allowing a shareholder-owned company to develop and maintain an army, declare war, and/or print money.

The great successes of entities like the VOC and EIC were even more flexible. For instance, captains and governors often simply disobeyed orders and followed their own plans, which generally worked in the company's favor. This illustrates how the line between criminals and nation-states has been fluid.

One of the major findings described in this report is that seemingly small-scale crimes for personal gain can easily be scaled into a type of economic warfare, akin to the conflict that kings and presidents waged against other kingdoms or nation-states. The historical context of pirates and privateering reminds us that history may not repeat exactly as it did in the past, but it certainly informs how the future may look.

4 Carrott, *The Dutch East India Company and the Future of Currency.*
5 The English translation of *Vereenigde Oost-Indische Compagnie (VOC)* is the Dutch East India Company.
6 To expand, English East India Company entities like the VOC and EIC were more flexible. For instance, captains and governors often disobeyed orders and followed their own plans, which generally worked in the company's favor. The line between criminals and nation-states has historically been fluid.

TECHNOLOGICAL DEFINITIONS WITH EXAMPLES

The following definitions were derived from analyst data and multiple subject matter expert (SME) interviews, including an economics professor at West Point and a blockchain analyst with U.S. Cyber Command. The definitions are not all-inclusive of the digital finance economy and cryptocurrency market, but are useful for understanding the findings of this report.

Blockchain Bridge - Allows for one party to exchange tokens of one crypto asset into tokens on another blockchain. As an example, imagine Alice has three Bitcoin (BTC) and wants to send five Ethereum (ETH) to Bob. BTC and ETH are on separate blockchains. A third person, Charlie agrees to take Alice's three BTC and sends the five ETH to Bob. Charlie acts as the bridge between Alice and Bob. Many crypto exchanges are centralized versions of a blockchain bridge. Bridges improve the ability for new traders to enter markets on other blockchains, but their centralized control is somewhat at odds with the benefit of decentralized networks.

Central Bank Digital Currency (CBDC) - Digital tokens issued by a country's central bank, attached to the country's fiat currency.[7] Generally a fiat currency is any money made legal tender by a government. Often the national government writes their own consensus protocol and ties it to taxes, so that users are forced to be compliant.

Consensus Protocol - The rules about how a blockchain verifies transactions on the network. Depending on the protocol, all (or some) of the computers on a network participate in verifying whether a transaction is valid.[8] Some protocols reward the computers that finish the verification first, while others reward computers that do the most work.

Distributed Ledger - A decentralized database of transactions and records that are shared and updated by all members of the network. All participants are governed by the network's consensus protocol rather than by a central authority. Because all participants on a network have a copy of the ledger, once a transaction is written and shared, the record becomes immutable and auditable.[9]

Oracles - Computer programs that act as bridges between the real world and a blockchain. An oracle watches for certain conditions that a smart contract needs to execute. For instance, an oracle could monitor stock prices and when a specific stock reaches a set price that is written into the contract, the oracle signals the blockchain that the contract condition has been met and to execute a buy or sell order.[10]

Private Key - A series of numbers and letters that make up the key to unlock your assets on a blockchain or in a crypto wallet. The private key authenticates a user on a network. It is the single most critical piece of information a person needs to conduct transactions on a blockchain. For instance, if a user loses their private key, there is no way to access their assets on the blockchain. Similarly, if someone gains access to this key, they can make transactions with the original user's assets. The companion piece of information is one's public key, which is like an email address, so others know how to contact the person for transactions.

Seed Phrase - A string of 12 to 24 words that act as the master password for an individual's crypto wallet. The seed phrase generates private keys necessary to authenticate a user and their transactions on the blockchain network.[11] Safeguarding the seed phrase is essential to the security of the private key.

Smart Contract - Tiny pieces of computer code that carry out certain instructions and may be tied to the execution of another linked contract. They are usually a form of "if…then" statements written in code and stored as a record on the blockchain.[12] When the "if" condition is met, the computers on the network run the "then" statement of the contract. Once the contract is executed and accepted by the blockchain, it becomes immutable. Malicious, malformed, or improper smart contracts can attack the network, usually for significant monetary loss to one party.[13] Contract attacks are a growing area of concern for security specialists and financial crime investigators.

SOCIETAL CHANGES

The development and deployment of emerging technologies will not be the sole enabling factor for CEFC. As technologies mature, populations, markets, and industrial applications will utilize them to create new businesses and societal activities. The following are key societal changes enabled by technology that will create the environment for CEFCs.

7 Seth, *Central Bank Digital Currency (CBDC) Definition.*
8 Kramer, *What Are Consensus Protocols?*
9 Brakeville and Perepa, *Blockchain Basics: Introduction to Distributed Ledgers*.
10 Injective Labs, *What Is a Crypto Oracle?*
11 Coinbase, *What Is a Seed Phrase?*
12 Hussey, Matt, and Phillips, *What Are Smart Contracts and How Do They Work?*
13 Innocent, *Smart Contract Security: The Attacks and Solutions.*

Wealth and Investment - There are three things to consider as cryptocurrencies shift to become a larger portion of an individual's wealth.

First, the threat models produced in the workshop suggested that more people will use cryptocurrencies of various sources – in addition to Bitcoin, Ethereum, and other front-runner currencies. A larger percentage of individuals' net worth is expected to be tied to crypto, and much of it could be uninsured. Examples include retirement plans and college funds stored as crypto assets.

Second, corporations are likely to begin "dabbling" or investing small amounts of money in a variety of e-currencies and digital commodities as part of their long-term financial strategies. Corporations with sufficient reserve funds should be able to weather crypto market instabilities better than individual investors, thereby giving corporations stronger control of crypto-involved wealth.

Third, there are a number of variables that have tremendous potential to expand the "digitally disadvantaged" class, including the unbanked. These include a lack of fiscal education and awareness at the individual consumer level, as well as rapid financial model shifts that are tied to increased investments in digital commodities. Although decentralized finance (DeFi) tools, such as cryptocurrencies and digital commodities should increase the availability of these markets to currently unbanked individuals, research doesn't yet address the extent to which this population will have access to DeFi tools. What is needed is an accompanying educational push by the federal government or the DeFi community.

Confidentiality, Integrity, Availability (CIA) - In the world of information security, the CIA triad represents 1) Confidentiality – an individual's data is available only to him/her and other authorized viewers; 2) Integrity - an individual's data is true and has not been changed; and 3) Availability - an individual can access his/her data whenever s/he needs to. This triad is the foundation of trust in data and computing. The workshop's threat models indicated several ways in which this trust might be thwarted with the advancement of future CEFCs.

Early successful attacks on institutions that develop and support digital currencies and digital commodities could create a delay and reduce trust in the digital banking system. Cryptocurrency exchanges have recently lost billions of dollars in thefts and hacks,[14] slowing the growth of crypto investment. Banks and financial institutions that are hacked are likely to similarly lower the confidence in both the digital economy and federal government that are backing any plans for centrally supported, digital finance tools and markets.

It's also expected that a new market will be developed for third party actors who manage digital identity authentication tools and data integrity checks. With these authentication technologies, criminals could take advantage of advances in biometrics, digital passports, microchips and implants, tattoos, and/or DNA-based secure tokens. They, and the businesses that develop around them, will be under intense scrutiny from consumers who need the technologies to work as advertised and from regulators who will insist that privacy leaks are minimized. It's also projected that there will be a concurrent black market that will manipulate, counterfeit, or otherwise defeat digital identity authentication technologies.

14 Browne, *Criminals Have Made off with over $10 Billion in 'DeFi' Scams and Thefts This Year.*

Digital Life - Another underlying condition in the future of CEFC is the inevitable reliance on digital devices. Society is expected to run wholly supported by the Internet of Things (IoT). The dilemma arises when something happens to disrupt electrical grids, cell phone towers, and/or portions of the internet that move IoT data. As the transition to digital-only services continues, artifacts such as land-line phones, brick-and-mortar banks, and even in-person medical appointments will be significantly reduced. This threatens the capability to recover from disruptive events.

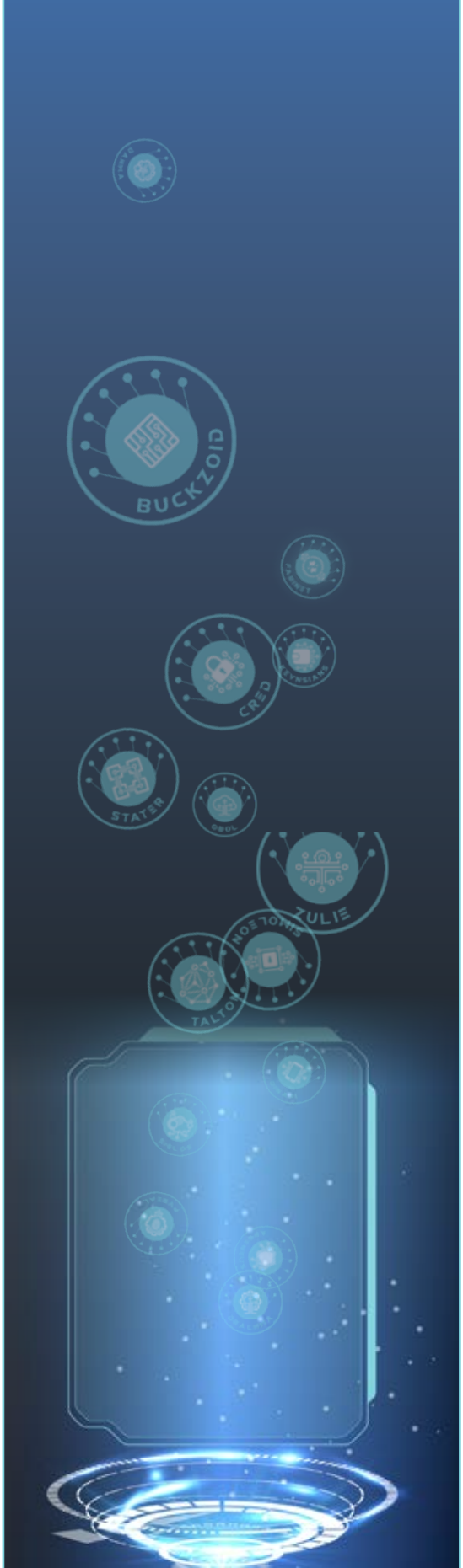
Artificial Intelligence (AI) - It's difficult to discuss a digitally-supported life without understanding how AI technologies underpin it. Likely the only way to keep up with the speed, scope, and scale of CEFC is with a clear understanding of automation, or more precisely, the use of algorithms, AI, machine learning, and other technologies where humans are not making all the decisions. Future criminals will attempt to exploit victims at the individual level, using insights from their publicly available information (e.g., from social media platforms) or private information (e.g., their crypto wallet private key). Criminals are also likely to use AI and automated tools to climb the ladder into wide-spread economic crime and even into state-sponsored economic warfare. However, AI is also expected to be used as a defense against digital criminals, even to the point of algorithms battling each other. This means that while AI can improve public trust in digital payments by ensuring their confidentiality, integrity, and availability, it can also create vulnerable communities. The complexity and proprietary nature of many AI systems often prevents human interaction until it is too late to mitigate unintended harm.

Regulation - Over the next decade, a continued struggle is expected between regulation and decentralization. The technologies that make up cryptocurrencies and the crypto market were originally intended to be decentralized and subject to control of the community consensus. At the same time, law enforcement agencies are rightly focused on stopping the rampant money laundering, fraud, theft, and other illicit activities that occur due to the decentralized nature of crypto-based financial crimes. While the law often lags behind criminal innovation, over time, diverse CEFC cases will provide regulators with a better understanding on how CEFC works and what legal authorities will best equip law enforcement to fight it.

Regulation to counteract CEFCs might take advantage of three different types of efforts. The first type of regulation would be to hold platforms responsible for the activities of their users. A second helpful regulation would be for government entities to provide guidance and boundaries for the private insurance industry to make sure individuals have recourse for recovering lost money. A third regulation would be to combine forces with cross-border agencies, whether through international criminal investigations (INTERPOL, EUROPOL) or

through industry-wide standard setting at the United Nations, International Monetary Fund, and/or the World Bank.

New Iterations of Old Schemes - The future of CEFCs is projected to see criminals trying to adapt old schemes with new technologies. They will likely take advantage of the fact that there is a gap between when a new technology appears and when law enforcement and regulators can act to understand, investigate, regulate, and minimize the opportunities for criminal gain. It's expected that known grift, con, fraud, and theft techniques will be applied to digital banking and crypto currencies. Most of the criminals' successes are likely to come from exploiting the unaware, especially by using those schemes that promise a mirage of success, as individuals will not know where to look to verify or confirm whether a scheme is valid or not. Some methods will immediately evolve as regulation and law enforcement catch up to the criminal activity more quickly than anticipated. Other possibilities include adaptations of crypto fraud as a service, like the evolution of denial-of-service attacks and ransomware attacks as services-for-hire on the dark web.



NEW FINANCIAL CRIME(S)

CEFCs are expected to first appear as acts against vulnerable consumers, companies, communities, and/or computer systems and networks (VCs).

Additionally, the CEFC environment will give rise to new forms of financial crime that do not fit in existing crime frameworks. These "New Crime(s)" will challenge federal and local law enforcement's existing understanding of crime prevention, detection, and prosecution.

Over the next decade, the emergence of New Crime(s) will first be seen in the VCs. VCs will not be as ready or equipped to respond effectively, thus making the population even more vulnerable.

SMALL TARGET/SCALE CRIMES

by criminals and organizations for financial gain

CONSUMERS:

A broad range of the U.S. public can fall into the "vulnerable" category. Essentially, a population is considered vulnerable because they lack resources to address criminal behavior (e.g., information, capital, social safety net, experience).

- Example Vulnerable Consumers:
  - Retired veterans,[15]
  - Elderly,[16]
  - Retirees, and
  - Youth and young adopters.[17]
- Vulnerable consumers have specific areas where they are affected or susceptible to CEFCs, including:
  - Personal data, often referred to as personally identifiable information (PII),
  - Personal devices that act as a 'gateway' for cyber exploitation and additional theft,
  - Individual financial information,
  - Financial portfolios,
  - An individual's entire digital, financial, and societal presence, and
  - Digital currencies.

15 Retired veteran scenario: Team Buckzoid 1 imagines Josh, a retired and disabled military veteran experiencing AI-enabled fraud through an online veteran support group. The AI digitally "resurrects" dead people's online profiles and procedurally generates life updates. Josh's support group is filled with these AI ghosts, and it pulls him into a multi-level marketing scheme converting his money into Bitcoin, of which he understands very little.

16 Elder scenario: Team Dhama 2 imagines Auntie Irma, a pensioner living in Florida who is trying to catch up on her retirement accounts after the 2029 European Union Financial Collapse took nearly everything. Her desperation to reestablish a safety net makes her look past the warning signs of yet another online crypto investment site that is not fully vetted. She loses her safety net – again.

16 Youth and young adopter scenario: Team Drachma 2 imagines Jane, a professional in her early 20's who lives in Washington, DC. Jane invests in an NFT (non-fungible token) artwork consortium (like a timeshare) and then "rents" her portion of the NFT access to other people on her social media platforms. The NFT consortium is owned by a foreign social media site and since Jane didn't carefully read her contract, her "rent" income legally belongs to the consortium, and therefore to the foreign media site.

COMPANIES:

Vulnerable Companies provide a different attack surface for CEFC.

- Small Businesses: Typically, vulnerable companies are small businesses without the resources to address criminal behavior (e.g., IT staff, security knowledge, up to date systems). Small businesses might be overwhelmed by legislation, insurance agencies, or previous lawsuits and attempt to take shortcuts to meet their profit goals.
- Large Enterprises: Some vulnerable companies can be large national or international organizations. Their vulnerability stems not from a lack of resources but by their size and scale, leaving blind spots and holes in their security posture. Additionally, these large organizations may have legacy technical systems that have not been updated or replaced because they have escaped the notice of their IT security department.

COMMUNITIES:

"Communities which include, but are not limited to, women, racial or ethnic groups, low-income individuals and families, individuals who are incarcerated and those who have been incarcerated, individuals with disabilities, individuals with mental health conditions, children, youth and young adults, seniors, immigrants and refugees, individuals who are Limited English Proficient (LEP), and lesbian, gay, bisexual, transgender, queer and questioning (LGBTQQ) communities, or combinations of these populations." [18]

- Example Vulnerable Communities:
  - Underserved populations,
  - Unbanked populations,
  - People at different age groups with varying understanding of digital economy threats and opportunities, and
  - People subject to authoritarian regimes enacting CBDC controls.[19]

COMPUTER SYSTEMS AND NETWORKS:

Vulnerable computer systems and networks can also be categorized as “vulnerable companies”. Simply by using computers and attached networks, organizations themselves are vulnerable to attacks. The organizations may be businesses in private industry, but can also include governments, non-profits, and/or advocacy groups.

- Examples of vulnerabilities of computer systems and networks are:
  - Small companies with small security budgets, and
  - Large organizations with legacy systems that are not incentivized to update or replace for financial reasons.
- How they are vulnerable:
  - The “cyber world” allows for a quantity of small thefts instead of targeting large thefts.[20]
  - Individuals who are vulnerable may rely on a single device, which leaves no redundancy or back-up system to access information.
  - Personal investment portfolios can be exposed to attack and theft when not completely secured.
  - An individual’s lack of wealth may motivate them to take more risks.
  - Individual 'trust' relies on the amount of knowledge and time IT teams can invest in security.

18 Law Insider, *Vulnerable Communities Definition.*
19 People subject to authoritarian regimes enacting CBDC controls scenario: Team Talton 2 imagines how Olayinka Adebayo, a respected investment banker from Lagos, Nigeria, is watching his country become consumed and dominated by Chinese politics. Because Nigeria runs the only accepted African digital currency backed by a central government, this effectively gives Chinese businesses de facto control over much of Nigeria’s, and by extension, Africa’s economy.
20 The “cyber world” allows for a quantity of small thefts instead of targeting large thefts scenario: Team Drachma 1 imagines Sam, a hardware store owner in Chicago who combines his personal and business funds to access high-speed trading algorithms. Not only does Sam make bad business decisions, but he also discovers that the trading company he is using has signed him up through an algorithmically-based phishing scheme that looks for small business owners seeking loans. The illegal trading company is subsequently hacked and all his personal and customer information is leaked online.

THE EFFECTS OF CEFCS ON VULNERABLE COMMUNITIES

The magnitude of the effect on a victim usually determines whether someone will go after a bad actor or not. Often "the juice isn't worth the squeeze" for financial companies or even for individuals with a modicum of security. If small amounts of money are taken, and it is difficult, frustrating, and/or time consuming to try to get the money back or to get retribution, victims may just move on. Adversaries have historically tried to get as much out of one victim as they can because of the effort and time needed to respond by isolating and targeting them effectively. But with countless vulnerable individuals now easily accessible through cyberspace, the time needed to respond rarely exists. Therefore, a bad actor can achieve greater results without triggering a response.

NEW CRIME(S)

Much of the emerging criminal activity is projected to fall under existing definitions of financial crime, yet the CEFC landscape will allow for "new crimes" to emerge. These new crimes are anticipated to arise from the combination of technologies and societal practices that materialize over the next decade.

It is helpful to think of this activity as "new" because it falls outside of the traditional definitions of financial crime. The nature of this difference, shifting from previous definitions to new definitions, will be enabled by the emerging CEFC environment -- providing variations of traditional crimes as well as new classifications. Here is a recent example of a new crime today, how it has become mainstream, and which points to the potential continued evolution of criminal behavior:

A (recent) operation coordinated by INTERPOL, codenamed HAECHI-II, saw police arrest more than 1,000 individuals and intercept a total of nearly $27 million of illicit funds, underlining the global threat of cyber-enabled financial crime.

In total, the operation resulted in the arrest of 1,003 individuals and allowed investigators to close 1,660 cases. In addition, 2,350 bank accounts linked to the illicit proceeds of online financial crime were blocked. More than 50 INTERPOL notices were published based on information relating to Operation HAECHI-II, and 10 new criminal modus operandi were identified.

Far from the common notion of online fraud as a relatively low-level and low stakes type of criminality, the results of Operation HAECHI-II show that transnational organized crime groups have been using the Internet to extract millions from their victims before funneling the illicit cash to bank accounts across the globe.[21]

21 Homeland Security Today, *Massive Cyber-Enabled Financial Crime Crackdown Included 'Squid Game' Trojan Horse.*

The following are examples and indicators of the New Crimes explored during the Threatcasting workshop:

- **Impact** - The CEFC environment will enable bad actors to have a larger impact in the future, because they have the capacity to act as a multiplier. Having a multiplier effect enables crimes to spread quickly among victims and across the globe. This increased impact will also make the CEFC environment attractive to nation-states and their proxies, as a place to have a wider destabilizing effect.
- **Speed, Scope, and Scale** - The CEFC environment will provide bad actors with efficiencies in speed, scope, and scale. These will accelerate a crime's impact and create the capacity to build upon original crimes to create new opportunities and New Crimes.
- **Cultivated Synthetic Identities At Scale** – Traditionally, hijacking or impersonating a person's identity has been a cornerstone of financial crime. However, the CEFC environment, specifically the use of biometrics and AI, is expected to provide attackers the ability to create custom-built synthetic identities at scale. These identities will be "grown" or "groomed" for specific purposes to evade detection for long periods of time or possibly all together.
- **Synthetic Identities in the Physical World** - When synthetic identities are connected to their cultivated biometrics and linked to the growing network of IoT (e.g., in the case of carrying out financial transactions), the synthetics will start to have an observable presence in the physical world. Their biometric and IoT presence will make them even harder to detect when digitally monitored and verified.

ECONOMIC WARFARE

An outcome of CEFCs is projected to be large target, economic warfare attacks by nation-states and their proxies to destabilize economies and erode trust.

The economic warfare threat shifts the target of the criminal activity and the intent of the crime to destabilization.

Threatcasting definitions of the manipulation and corruption families of financial crimes are used as the basis for understanding economic warfare. The manipulation family includes those who attempt to influence markets and prices, and further encompasses cyber-attacks for follow-on fraud and theft operations. Corruption crimes are those that invoke force, fear, or payments for favorable treatment, including ransomware attacks.

These families of financial crimes share strong dependencies on rapidly evolving technologies, crypto-assets, poor or absent regulation and oversight. In addition, they can happen at both the individual and aggregate level. Disruption – even temporary – is the goal, and sowing distrust or chaos can be as valuable as actual financial theft.

Economic warfare is a large umbrella term that legal experts traditionally describe as "economic and financial hostilities as activities that fall below the threshold of warfare."[22] This can also be described as "gray zone warfare" or actions taken by both state and non-state actors, just short of a kinetic conflict. Threatcasting Lab findings revealed a growing concern that financial hostilities, either purposefully enacted by adversarial nations, or accidentally aggregated through targeted small crime activities, should be considered in a different light.

Recent economic problems in America and Europe illustrate how connected individual financial institutions are to both the private consumer and national economies. National and global financial interdependencies have resulted in systemic risks, often framed by policymakers as "too big to fail," "too connected to fail," and "too fast to save".[23] This means that small concerns at one end of the system can lead to catastrophic economic consequences at the other end.[24]

The Financial Stability Board, an international body that monitors and

makes recommendations about the global financial system, assesses that as crypto assets become adopted at more financial institutions, their linkages to the broader financial system will be more profound. This means that the ladder linking of small and large target crimes allows for stronger scaling up of the impacts of CEFCs. Attacks against individual consumers will have an aggregated impact on crypto-backed economies. Similarly, as financial institutions add crypto assets to their portfolios, they assume risks as if they were an individual consumer. Blockchain transactions do not recognize whether the parties involved are a "Mr. Smith" or a large financial institution.

The Financial Stability Board assesses that "If current trends continue, and are absent effective regulation and supervision, financial stability risks may emerge as crypto-assets become increasingly interconnected with the wider financial system. This is especially the case in emerging market and developing economies (EMDEs) where crypto-assets may in some situations replace the domestic currency, or offer opportunities to circumvent exchange restrictions, and capital account management measures." [25]

Economic destabilization might occur in numerous areas, including:

- National economies,
- National or international businesses,
- Microtargeting campaigns,
- Mass identity theft,
- Transnational financial crime rings,
- Business databases,
- Business supply chains,
- Online shopping/retail businesses,
- Energy grids or supply chains,
- Loss of faith in financial institutions,
- Loss of faith in federal currency,
- Stock markets,
- Global aid relief, and
- Nation-state economic and currency competition.

With a broader goal, perpetrators of financial crimes shift from criminals and criminal organizations to nation-state actors or their criminal proxies. Because of this shift, the classification of the crimes moves from financial crime to economic warfare.

22 Lin, *Financial Weapons of War*, 1377–1440.
23 Ibid.
24 The "Flash Crash" of May 6, 2010 witnessed unprecedented market instability and loss of market value estimated at $1 trillion in less than thirty minutes. See Bowley, *Lone Sale of $4.1 Billion in Contracts Led to 'Flash Crash' in May.*
25 Financial Stability Board, *Assessment of Risks to Financial Stability from Crypto-Assets*.

THE IMPORTANCE OF UNDERSTANDING TRUST

The idea of trust, either explicit or implied, was present throughout the workshop. Participants often built scenarios that included mitigation of crime through legal authorities. Participants' trust in law enforcement would sufficiently put an end to an imagined crime scheme they developed in the workshop. Their imagination built complex and theoretical future crimes. But ultimately, when backcasting the scenarios, participants often relied upon traditional law enforcement, empowered by new authorities or technology, as the primary cure to crimes.

The public also relies on the safety of banking systems and trusts that they can be protected by them. Likewise, they place their trust in law enforcement to stop crime when banking systems fail to offer protection. Bad actors display trust in another form. They trust that electronic banking networks are built upon systems that can be exploited for financial gain. Lastly, law enforcement relies upon legal authorities to provide the ability to investigate, mitigate, and levee punishment against criminal behaviors.

LADDER TO CHAOS

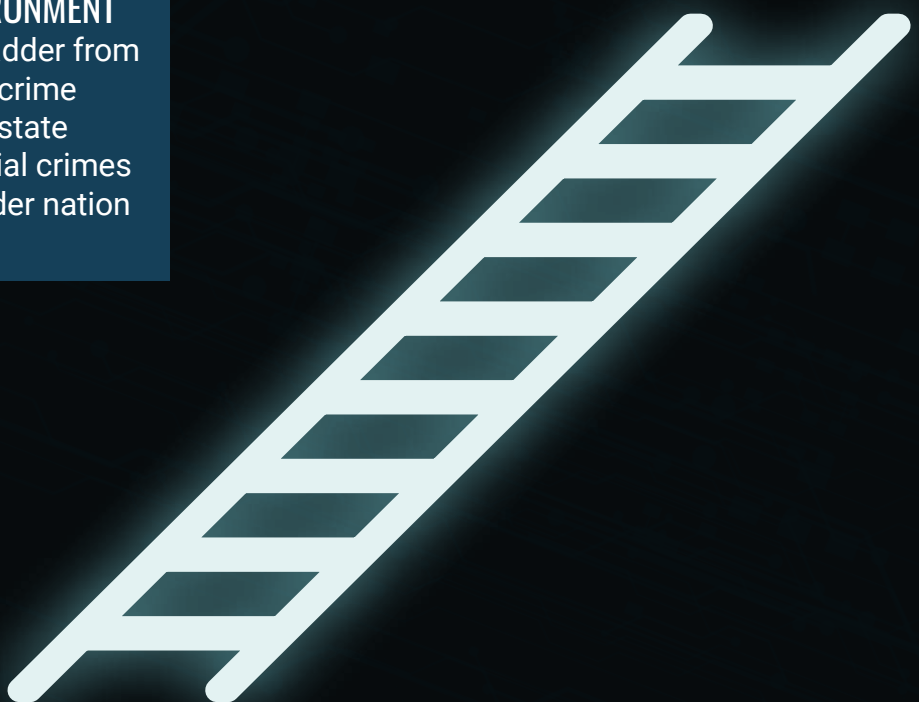
A criminal activity that first appeared in the workshop with the goal of financial gain from VCs, highlighted a unique threat space. This first appearance was referred to as Threat 1. The impact, speed, scope, and scale of the attacks began to show that this criminal attack was masking a larger economic warfare assault, which was labeled Threat 2.

As the criminal activity escalated, a Ladder to Chaos was identified as Threat 3, affecting more people with the goal of destabilizing organizations, markets, and countries.

Effects Trigger

It may be possible to observe when personal financial crimes are masking a larger nation-state attack. This can be identified through the nature and effects of the attack. When the volume of the personal financial crime reaches a certain level (i.e., a high volume of attacks in a specific place or industry), the "effect" of the attack also shifts. In other words, the goal of the attack is assessed to move from financial gain to larger nation-state destabilization. The volume of attacks and the eventual broader destabilizing effect becomes a potential trigger that can identify the nature of the attack.

THE CEFC ENVIRONMENT will provide a ladder from small financial crime to large nation-state targets. Financial crimes will mask broader nation state attacks.



CEFC CONDITIONAL STATE AND THE PRE-CRIME PARADOX

CEFCs will create a conditional state with a vacuum for criminals to expand New Crime and for nation states to wage geopolitical economic warfare. This will necessitate a greater focus on the underlying conditions, rather than on the perpetrator or singular crime.

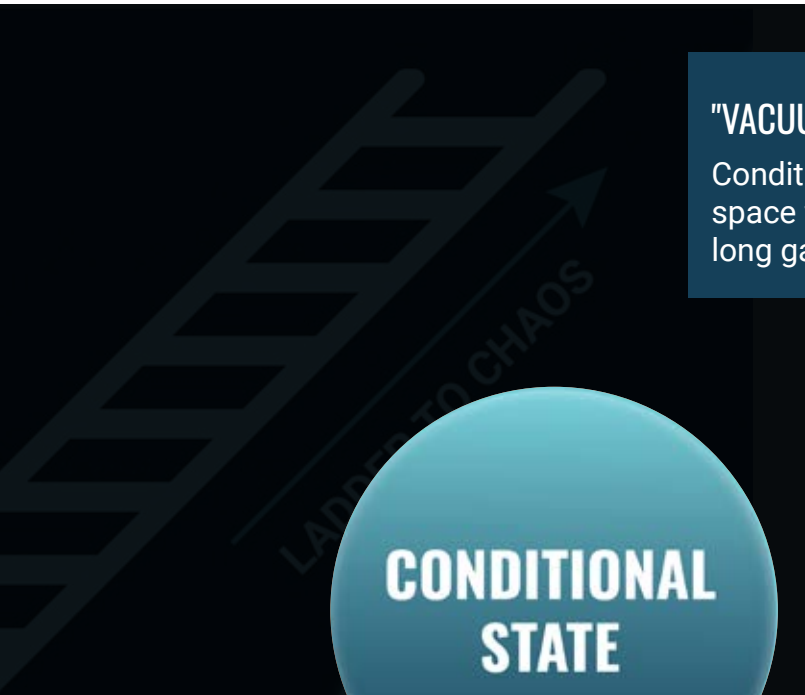
Pre-Crime Precedents

The notion of "pre-crime" can stimulate science fiction visions of the future, like those portrayed in the 2002 Steven Spielberg thriller, "Minority Report". Based on the Philip K. Dick book of the same name, the story centers around an oppressive police state that uses "precogs" or humans with the ability to foresee possible future crimes, prompting arrests of suspects before they have committed the actual crime.

However, in reality, "pre-crime" is an emerging study of societal and natural conditions, which has the potential to give rise to a higher frequency of specific sets of crimes perpetrated on specific sets of people.

Pre-crime laws and practices can be organized into the following four categories that fall within the definition of 'substantive coercive state intervention targeted at non-imminent crimes'[26]:

- Pre-emptive criminal classification imposed on young offenders,
- Crimes of association and encouragement,
- Detention or restrictions on the basis of capability, and
- Interventions based on suspicion of intent.



"VACUUM FOR BAD ACTORS"

Conditional State that creates a space for criminals playing the long game of Geopolitical conflict.

Another example of pre-crime activities can be seen in Norway and the exploration of the implications of mass migration on crime rates. Norway and Europe were concerned about an increase in migrants and follow-on effects of open borders. Concerns about increased crime, reduced public safety, and a lack of identity checks led to more control measures within the Intra-Schengen program. Border control practices in Central and Western Europe become more protective and securitized.[27] Norwegian police updated their police intelligence doctrine and launched Operation Migrant as the very first national intelligence project. The idea of a crisis "encouraged worst-case scenario thinking that generated suspicion and unease, especially among politicians, about potential criminal repercussions of this increase in migration."[28]

The Pre-Crime Paradox

Pre-Crime vs. Post-Crime

For law enforcement, this pre-crime type of thinking could be considered counter-intuitive to traditional approaches that address crime reactively. A recent example of the emerging exploration of pre-crime as opposed to post-crime is illustrated by Australia's response to the 9/11 terror attacks.

"Prevention in Australia's domestic legal response to terror has ushered in a host of 'pre-crime' measures that permit the state to intervene and restrain an individual on the basis of an anticipated future harm, rather than past wrongdoing (Zedner, 2007a: 259). Prevention by liberty restraint is a feature of many anti-terror initiatives, most notably control orders and preparatory offences (Divs 101, 104, Criminal Code Act 1995 (Cth) 'Criminal Code'). These measures deviate from the traditional retrospective and 'post-crime' orientation of the criminal justice system, where the state reacts and responds to harm by prosecuting and punishing criminal acts on the basis of evidence gathered about past events (Roach, 2010; Zedner, 2007a: 259, 2009: 73). 'Pre-crime' measures are predictive and rely upon intelligence 'about future threats to security' gathered through surveillance practices and 'pre-crime' policing (Roach, 2010: 52; Walker, 2011: 56)."[29]

26 Gobeil and Justin. *Review of McCulloch, Jude, and Dean Wilson and Pre-Crime: Pre-Emption, Precaution, and the Future. Surveillance and Society.*

27 Jansen, *Pre-crime and Policing of Migrants: Anticipatory Action Meets Management of Concerns,* 90 –10.

28 Ibid.

29 Tulich, *Prevention and Pre-Emption in Australia's Domestic Anti-Terrorism Legislation*, 52.

A NEW LENS THROUGH WHICH TO VIEW CRIME

The following compares and contrasts two differing approaches to crime – "Static" and "Evolving." The Static approach sees crime as finite, meaning that crime will come to an end if addressed. The Evolving approach, however, employs a different lens through which to view crime. It sees crime as ongoing and constantly changing, as long as there are opportunities.

This Static approach typifies the traditional law enforcement method and mental model for understanding how to combat traditional financial crime. Historically, law enforcement uses the categories of victim, perpetrator, investigation, and prosecution. Laws, law enforcement policies, and insurances approaches to managing financial crimes are pinned to this categorical model. However, the future of CEFC requires a new mental model. Law enforcement needs to update the lens through which it sees crime as Evolving in the CEFC landscape.

For small crimes, the Static approach usually makes sense. There is a victim, a criminal, and a set of activities by lawmakers to investigate and prosecute. In this case, the victim has a sense of justice. But this approach only works for the Fraud and Theft categories of crime.

The Evolving approach requires a different mindset. The speed, scope, and scale of future crimes has the potential to evolve into whole-of-government, economic warfare. Many of the same indicators as small target crimes are expected to be present, but with a wholly different intent behind them, and the responses to them cannot be the sole responsibility of law enforcement agencies.

STATIC

- Federal Agencies use of terms and defined goals
- "Impose consequences"
- "Change behavior"
- "Investigate violations"
- "Increase voluntary compliance" with tax laws IRS
- Disinformation/propaganda
- Prosecution of individuals as a goal
- Accountability to foreign bad actor
- Accountability or sanctions against foreign nation
- Regulations and standards put in place by law enforcement
- "Put an end to crime" as a goal
- Same tactics with new technologies
- Social net replaced by technology

EVOLVING

- White collar crime motivation "to obtain or avoid losing money, property, or services or to secure a personal or business advantage"
- Frequent use of "investigate" by federal law enforcement agencies
- Small operations intended to determine weaknesses and vulnerabilities
- Disruption, distrust, and chaos of economic security rather than theft
- Negative economic influences
- Loss of wealth growth, not the same as theft of wealth
- Manipulation of digital currency markets
- Dynamic nature of digital crime
- There is no 'bad op' when something is learned or discovered
- Organized criminal organizations persistence beyond the capture of one leader
- "Do even better next time" as a goal
- Tier 1 countries resistance to change (or slow change) allows enemies to attack the same defenses repeatedly
- A sense of security in believing you know someone as well as believing you know the technology. As always, belief in security is the thief's best friend.

THREAT OUTLIER - AN ADDITIONAL THREAT AREA OF INTEREST

The Perils of Cyber-Enabled Social Support

There is one interesting outlier that does not explicitly answer the Threatcasting research question, but analysts recognized it as a critical nexus of financial insecurity. It occurs when cyber-enabled social support fails. As automation technologies converge with ubiquitous digital financial systems and social support systems (e.g., welfare, prescription drug payments, child support), there is a possibility that vulnerable populations will be locked out of their support system(s) and their vulnerabilities will be further exacerbated. This could be considered a type of financial crime that the government inadvertently commits as its leadership places more trust on automated systems.

Threat Overview

In the CEFC environment, public benefits and payday loans are digitally issued and at risk of hacking, confiscation, and/or becoming inaccessible due to internet connectivity.

Below is a hypothetical case study that illustrates the effects of this threat.

Lisa is a low-income and food-insecure, single mother of an only child who lives in deindustrialized Gary, Indiana. There, crime rates have increased, and social services are diminishing. She is a part-time retail worker with unpredictable shifts, unreliable transportation, increasingly expensive childcare, with a previous history of substance abuse. She is also far from close family members.

In her life, Lisa has experienced a series of personal relationship setbacks. With few options for reliable, well-paying employment, Lisa is dependent upon government benefits for her and her child's survival in low-income housing.

Lisa's example shows the following vulnerabilities

- A "perfect storm" of erroneous information in government databases and unreliable internet access due to local power grid outages. Disputes with digital payday lenders has also resulted in Lisa not being able to access the meager funds she needs to pay for expenses.
- The creditor for her car has remotely deactivated it, and she is forced to walk as even public transportation requires digital payments.
- Government service algorithms have determined that her financial life patterns are endangering her child and instruct the dispatching of Child Protective Services to place her son in temporary foster care.

In summary, the convergence of digital payments that dominate her life, and the over-reliance on AI to allocate services and civil punishments, has left her destitute and hard-pressed to improve her situation. She has become one of the "digitally disadvantaged". Any attempt by relatives to provide funds are fleeting because as soon as the funds hit her digital wallet, they are seized.[30]

In this threat example of digitally-issued benefits and loans, it's evident that there are extreme vulnerabilities in a completely cyber-enabled social safety net of products and services. Lisa is part of a VC with little support and a fragile day-to-day existence. Her socioeconomic condition and over reliance on a digital infrastructure make any disruption (e.g., criminal, environmental, conditional, etc.) highly dangerous. The very nature of the cyber-enabled social safety net makes the VC more vulnerable, and the cyber portion acts as an amplifier of the threats, the risk, and the impact.

30 Threatcasting Lab workshop: Team Obol 1.

INDICATORS (FLAGS)

FLAGS DEFINITION

The Threatcasting process maps out possible and potential threats 10 years into the future. It also identifies the "flags" that indicate a specific threat future is underway and/or may come to pass. Sometimes referred to as "signals", [31] they can give an early warning that a potential attack is in-flight or beginning to form.

GENERAL CEFC TRENDS

Flags can be categorized in multiple domains (e.g., technical, cultural, social, economic, regulatory, etc.). Each flag described below is a micro-indicator that the threats outlined in this report are emerging. They are often built off of one another, and by doing so, provide multiple early-stage indicators to prepare for the threat

1. Improved Detection and Attribution:

This flag is a natural evolution of current AI transparency, research, and policy as well as a gatekeeper action identified in the next section. The threat futures from the workshop indicate a need for detection in small-target financial crimes, especially those enabled by AI. When scaled to the masses, AI-enabled crime becomes a tool for nation-states and their proxies. For instance, the more that AI is involved with crypto transactions, the faster their speed, scope, and scale. This can rapidly escalate, causing market fluctuations that appear to be at the level of economic warfare - even if the intent was not to cause economic warfare effects. Because of the ubiquitous use of algorithms in financial systems, there will naturally be a buildup of technologies to improve detection and attribution of financial transactions and illicit behavior.

2. Lagging Technical Knowledge:

For the foreseeable future, the technical knowledge of the average public about crypto and digital economies is expected to

remain low. The speed at which new digital coins can be minted sets up opportunities for unaware users to be lured into a scam, fraud, and/or losing proposition. This will be even more apparent as developers attempt to innovate the next type of virtual currency or decentralized finance (DeFi) platform to attract new investors.

3. Speed, Scope, and Scale:

The development, adoption, and innovative uses of cryptocurrencies, decentralized ledgers, blockchain contracts, and other elements of DeFi technologies will explode in scope and scale. The speed of these algorithms may require new mathematical and cryptographic models.

4. Attraction of "Un-Reality:"

It is anticipated that there will be growth in the attraction to what the Threatcasting Lab calls "un-reality" or the belief that a technology, such as digital currencies, crypto investment, virtual reality worlds or online communities will automatically solve societal concerns, such as economic instability and discomfort in social situations. Un-reality attempts to replace real life with a constructed vision of a comfortable life that ignores the imperfections and failings of being human and living a human existence. Those seeking a new reality through technology might promote the growth of policies and laws that overlook basic human rights. Those seeking to escape the realities of life might also spend unhealthy amounts of time, money, and attention on virtual existences that ignore international politics or ethnic and nationalistic conflict. Aggressor nation-states looking for opportunities to exploit another country's vulnerabilities may seek to change realities to match their desired world views. Often this has been and will be achieved through misinformation campaigns that influence the target(s)' understanding of reality for strategic advantage.

5. Thwarting Identity Verification:

One of the most troubling flags will be an attempt to alter, subvert, gain control over, or bypass identity-verification methods. Considerable resources are projected to be allocated toward efforts to influence people to part with their private keys or seed phrases. Similarly, there are currently bots watching the crypto exchanges for specific fluctuations, offerings, and contract executions - sometimes called front runners - that are programmed to seek out opportunities before the rest of the network has the ability to catch up.[32] While a front runner bot may not technically bypass identity authentication measures, it may be able to move faster than the consensus protocol and create transactions that are unfavorable to one party -- simply because the party trusted the verification methods of the network to be completely safe.

31 Webb, *The signals are talking: Why today's fringe is tomorrow's mainstream*.
32 Samczsun. *Escaping the Dark Forest.*

6. All or Nothing Technologies:

Another flag with deeply concerning implications occurs with all-or-nothing shifts to certain technologies that lack a way to revert to an earlier known preferred baseline state. Digital banking, online shopping, and personal smartphones are examples that demonstrate adoption of technologies that are largely irreversible. This will increase the divide between those who can adopt technologies knowing the implications, and those who are forced to make the change and are disadvantaged because of it. This will also likely increase the number and scope of venture capitalists.

Additional trends that might influence the CEFC environment include:

- Increased breaches of health data, such as biometrics that is useful to bypass authentication controls.
- Non-universal adoption of updated industry standards and practices.
- Centralized processing of digital currencies as opposed to decentralized intentions of cryptocurrencies.
- Social conditions breeding new scammer variants.
- Expanded reliance on Chinese services, technologies, standards, and policies.
- Unexplainable crypto-asset value fluctuations.
- Hidden real intent within information campaigns.
- Sponsored digital currency "hackathons".
- Formation of new online communities (e.g., pro- and anti-digital currency, centralized vs. decentralized control, NFT marketplaces).

CONDITIONS

Workshop participants joined with post analysis staff to gather and document a wealth of conditions and specific indicators that will enable CEFC. These conditions differ from flags in that they are much broader, generally overlap, and can be subjective. These conditions provide a broader range of areas to monitor the progression of the CEFC environment and possible threats.

CEFC Conditions

- **The Emergence of Well-Funded Adversaries** - An increase in funding for bad actor(s) - whether from larger criminal collectives, due to the lucrative nature of the CEFC environment, or from nation-states who want to engage in economic warfare.
- **Reliance on Digital Only Payments** - A shift from a hybrid, digital, and physical approach to digital only payment practices in both government and industry.
- **Increasingly Robust Digital Personal Profiles and Information** - Along with digital payments, personal information is kept mainly in digital forms that can be traded, hacked, and purchased.
- **Adversaries Cultivating a Talented Workforce** - In the race for talented labor, criminals, and nation-states

increasingly recruit talent for the CEFC environment.

- **Lack of Understanding or Awareness of Digital Risks and Digital Security** - Driven by profit and convenience, industries and consumers continue to lack understanding of the threat space.
- **Interconnectivity of Applications with Disparate Information** - Expanding business and government use of the CEFC-vulnerable environment (e.g., IoT, 5G) also requires a connection with an increasing number of devices that gather information. Varied business practices and fragmented governance mechanisms cannot completely manage the risk of interconnected devices and massive data.
- **The Shift to All Digital** - - The CEFC environment becomes the primary space for daily activity, such as online banking, gaming, dating, and entertainment. Driven by industry, these spaces are monetized, and provide an easy entry point for consumers to engage.
- **Delays and Blindness to Hacks and Breaches** - The increasing complexity of the CEFC environment will provide cover for criminals and nation-states. As adversaries hide in the complexity of the environment, awareness of an attack could be delayed or obscured completely.
- **Increasing Ability and Tools to 'Spoof' Virtual Identity** - The collection of biometrics and use of AI, and other CEFC-enabling technologies, provides criminals and nation-states with a standardized approach to identity. This standardization will come from the industry and governmental needs to standardize use and costs. This standardization will expand tools and services to spoof and hijack identities.
- **Lack of Safety Net Leading to Disparate and Uninformed VC Risks in Crypto Applications** - The increasing use of the CEFC-enabling environment gives VCs a fear of missing out, pushing them to “get in now or risk missing out” (e.g., investing in cryptocurrency and adopting new digital tech).
- **Persistence of 'Zero-Day Bugs'** – New bugs impact any system or application, which gives rise to a larger market to find them, exploit them, and/or sell the solutions.

ACTIONS TO BE TAKEN (GATES)

GATES DEFINITION

In addition to uncovering threats and flags, the Threatcasting workshop participants identified actions that could be taken to help mitigate, disrupt, and/or recover from the threats. These actions constitute a “whole of society” approach to problem-solving and have been applied to specific domain areas where detailed steps can be taken. To be most effective, the actions must be fluid to adapt and shape the future applications of technology.

GENERAL ACTIONS TO BE TAKEN

Organizations can take actions at two points in time: 1) before a threat event occurs to avoid, disrupt, or mitigate its effects, and 2) after an event occurs to increase speed of recovery.

Pre-event (Prevention) Actions:

Enhanced encryption for digital currency rollout - Four threat models from the workshop indicated a measured approach to how a nation should introduce a central bank digital currency (CBDC). This approach is proposed to emphasize encryption standards as part of the preventative defensive mechanism against criminal activity – presupposing that if the lock is strong enough, criminals cannot get in. This encryption-based approach implies locking up several things, such as personal data, the private key, and the currency itself.

Proactive regulation - A significant emphasis was placed on developing federal level regulation. Some of the specific regulatory recommendations included:

- Deliberate and clear reporting as well as an award process for individuals and companies that report financial crimes. This should include clauses that minimize retribution and retaliation against whistleblowers.
- A red line policy for conflict escalation against nation-state actors. Lawmakers must consider when the U.S. would be allowed to conduct military action against economic warfare efforts from a nation-state or its proxy.
- A robust insurance industry to compensate victims. There is a need for more studies about how the private insurance industry can be regulated to protect consumers from CEFC.
- Expanded sandbox opportunities that are modeled after financial technology (FinTech) experiments to understand the implications of CBDC, crypto investment, and other cryptocurrency applications.
- Agile government regulation practices, specifically designed to increase resiliency of cryptocurrency investment and smart contract markets.
- Leveraging non-governmental sources to assist with regulation. Several of the threat models included increased U.S. participation with world banking systems as a necessary step to stabilize the multinational ripple effects of digital financial crimes.

Identity management - Identity management technology and policies were at the center of several threat models. This topic relates to current “know your customer” (KYC) requirements for the cryptocurrency economy, although future financial crimes will attempt to circumvent KYC policies. What may improve the visibility on the lack of KYC standards for some CEFC applications include an improvement to background checks and the designation of identity verification as a "National Critical Infrastructure” to accompany power, transportation, and water. By doing this, the seriousness of long-term threats to national security taking place through cyber-enabled financial crimes is addressed.







Detection technology and policies - This is arguably the largest category of possible actions recommended by the workshop's threat models. Much of the detection of CEFC must be done automatically and algorithmically. Most models used broad wording to describe detection, which in laymen's terms, essentially means "figuring out a way to see the bad guys doing bad things". Other recommendations include:

- The development of a "financial crimes analysis science". This might be a branch or extension of threat finance science, or how analysts and detectives "follow the money". Purposeful training and university degrees could combine network science, AI-assisted triage, and intelligence procedures to make detection and recovery much faster.
- Before smart contracts are executed, apply algorithmic detection by developing tools that monitor contract attacks and learn how to triage the threat, contact key decision makers, and isolate the malicious ones. For example, the article, "Escaping the Dark Forest" provides details of how a volunteer vulnerability researcher mobilized his contacts to recover nearly $10 million dollars in threatened cryptocurrency in less than 24 hours. This is the speed and type of response that federal law enforcement must aspire to in order to stay ahead of future criminals.

Education - Almost half of the threat models from the workshop recommended some type of user-level education program. Mostly, the models imagined how criminals might take advantage of gullible and vulnerable people. This likely correlates to the high amount of theft and fraud crimes that are directed at individuals at the small financial crime end of the ladder. As a preventative measure, much more education is needed on unique cryptocurrency, digital economies, and the threats that come with these technologies. Actions will need to go beyond "digital literacy" and "digital hygiene". The recommendation included additional research to discover better ways to protect individuals from CEFC.

Understand the emerging environment - As digitalization continues to move real-world value to digital assets, it's necessary to understand how to describe the changing environment, including how to apply legal concepts to digital spaces.

Maxim Kon, CEO of Cheksy, a blockchain investigation and compliance consulting firm in Switzerland, currently sees non-fungible tokens (NFTs) as a high-risk category of digital assets that eases money laundering operations. He recommends a number of actions be taken to reduce the impact of money laundering through NFTs including:

- Regulators and forensics analysts carefully watching NFTs as a separate

type of crypto asset.

- NFT marketplaces implementing an industry standard KYC and Anti-Money Laundering (AML) policies.
- NFTs being regulated, so that they cannot be generated anonymously.
- Metaverse and the online gaming industry thinking ahead about the impact of NFTs and how these industries may play a part in the future of AML.[34]

During/Post-event (Consequence Mitigation/Recovery) Actions:

"In-the-moment" actions – Actions recommended as the threat event occurs:

- Provide a counter-narrative or an "official" perspective about what is happening, keeping in mind that this is also the same space that disinformation campaigns flourish. While trying to act in the window between event and post-event, the messaging should rely on the science and best practices of counter-disinformation. Creators and distributors of the information should also anticipate the consequences of counter-counter-narratives.
- Establish and use clear requirements and channels for reporting. Clear reporting must be accompanied by trust that action will be taken to remedy the current situation and create a

33 Samczsun. *Escaping the Dark Forest*.
34 Kon and Cheksy, *NFTs: The ultimate money laundering tool?*

sense that retribution against those victimized will not be tolerated. In other words, victims of ransomware should be confident that they can turn to a specific named agency and not be penalized for reporting a crime.

Return the "system" to pre-attack functionality – The following actions are recommended to be taken to improve functionality:

- Employ data redundancy and data backups as technical tools to allow companies affected by a financial attack to restore some sense of functionality. It is not clear how this would work for individuals.
- Develop an “analog currency” backup available to restore functionality if a digital currency has technical difficulties. This implies having the ability for an individual to have “cash under the mattress” in the event of an emergency, but what this scenario looks like in a fully digital economy is unclear.

Enacting justice – This is the most varied category of recovery and may not have immediate ties to the original financial crime that perpetrated the loss. Recommendations include:

- Develop mechanisms for threat attribution and the rehabilitation of former criminals with a focus on the actor part of the triangle.
- Recover personal assets through insurance payments, federal stimulus payments, or identity recovery procedures that represent the second part of the Crime Triangle. Using insurance as a recovery method implies (and demands) that the insurance industry be prepared to tackle crypto and the fallout from future financial crime. It also implies that the insurance industry has studied the ways this could happen and has assigned risk assessment scores. Any discussion of insurance as a recovery plan of action must also assume that steps need to be taken before the event to set up the processes and procedures. This could occur through traditional markets or deliberate federal programs.
- Develop plans and possible actions the government would take to retaliate against economic warfare. For instance, are there policy red lines that would authorize military (e.g., cyber and kinetic) actions or economic warfare actions against a nation-state or proxy? While not discussed in the workshop’s threat models, current policies in cyberspace warfare could be relied upon as a baseline.

ACTIONS SPECIFIC TO FEDERAL LAW ENFORCEMENT

To disrupt and mitigate these threats, Federal Law Enforcement should consider:

- Utilizing a functional definition of CEFC technology and adjacent practices. The definition should include an understanding of the distinction between traditional financial crime and new crimes - where the increased impact, speed, scope, and scale of CEFC will expand to impact Federal Law Enforcement.
- Empowering, protecting, and performing outreach to VCs (e.g., consumers, companies, computer systems) with lawful monitoring systems that understand the importance of identity, confidentiality, integrity, and availability.
- Tracking and monitoring emergent CEFC through the sharing of best practices across federal and local law enforcement, as well as the DoD. In addition, specifically:
    - Determining how to identify if the attack behind the financial crime masks a broader nation-state attack.
    - Developing processes to pass the identification and intelligence of the CEFC from law enforcement to DoD when jurisdictionally appropriate.
- Further exploring CEFC's "pre-crime conditional state" with indicators to watch for and actions to take. This type of approach has been used for other conditional states, such as natural disasters (e.g., hurricanes, wildfire, etc.) to identify vulnerable people and situations that might see an increase in specific crimes (e.g., identity theft, fraud, etc.).
- Treating crypto like property, as described by Aidan Larkin, CEO of Asset Reality. He shared insights that courts are treating crypto as property, which can be seized and recovered to generate income just like any other seized asset. With that said, officials who seize crypto assets must create a plan for storing and safeguarding this type of property. Larkin likened the seizure of crypto to recovering a stolen high-end piece of art, "…you don't just throw a Rembrandt or a Bansky into the back of a police van." Agencies must develop storage and transfer procedures that are secure and accessible at the point of seizure, so that the crypto is immediately locked down.[35]

35 Larkin, *Demystifying crypto asset recovery.*

1. **Bitcoin Magazine: Bitcoin News, Articles, Charts, and Guides** - news, expert commentary, and information on Bitcoin and the Bitcoin blockchain technology.
2. **Blockchain Data Platform** - a for-profit company that provides blockchain analysis services and regularly conducts independent research on key crypto, blockchain, and digital economy issues.
3. **Cryptocurrency and Fincrime Compliance** - getting started, going deeper, investigation tools, including searching the blockchain ledgers.
4. **DOJ Seizure AUG2020** – great vignette about DOJ and crypto / terror financing.
5. **Financial Action Task Force** – multinational watchdog trying to set international standards.
6. **Financial Crime Academy Blog** - Compliance, Anti-Financial Crime, AML - blogs of different types of financial crimes.
7. **Tech Against Terrorism** – a great platform that releases a lot of content about tech + terrorism. Often outside the blockchain space, but some overlap.
8. **Web3 is going just great** - blog and analysis of current events in crypto, NFT, blockchain world.

SUBJECT MATTER EXPERT INTERVIEW TRANSCRIPTS

This appendix contains the unedited (and machine transcribed) transcripts of interviews with five subject matter experts. The few edits we made were to correct fundamental mistakes that changed the meaning of a sentence. These experts provided their opinions on the trajectory of various trends in the cyber-enabled financial crimes environment. Their opinions are based on their own academic research, industry-related expertise, and leadership observations.

The interviews recordings were made available to workshop participants as inputs to the effects-based modeling phase.

Anne T. Griffin, Columbia University

So, I have, I have a couple thoughts. But one area I wanna talk about today is in the realm of like digital assets, which can be crypto, it can be NFTs. It can be like any digital assets, but I'll probably touch more on crypto today. And some of these things are problems we're starting to see now, but they are on a smaller scale because right now, like for example, like most, most of my money is in traditional us currency. Right? Not, not a big issue. Like, you know, it's in a bank, it there's some sort of, you know, it's, the bank is insured. Like that's, that's not an issue. Right. But we're start what we're starting to see. And hopefully some of the people who are watching this are somewhat aware of are these scams where people are getting like scammed either out of their cryptocurrency or people who have cryptocurrency are getting robbed.

So, like on the small scale, like I used to work at a blockchain startup. A lot of people have crypto or well, and criminals also assumed that people working there had crypto. So, they would do the scam where they take over your phone and they try to hold of like, you know, all your apps and that kind of thing, and your wallet to get access to your crypto. So, they can steal your crypto. And, you know, once you do a transaction with most crypto, that's

not a reversible action when we're talking about like decentralized cryptocurrencies, and we're starting to see again, this is usually like targeting certain individuals that is bad. But most of the time it's like, oh, maybe you got like a couple thousand dollars from this person. Most people who have a couple of thousand dollars in crypto right now, it hurts to lose it, but it's not the end of their world.

Right. Where I think we're seeing in what we've seen since, like, I think it's 2012 when the Bitcoin white paper came out is despite the fact that we keep seeing this as a fringe technology, we're only seeing the adoption pick up and we're starting to see, you know, the, the concept of digital central banks, which means that we're going in a direction, not saying that crypto is gonna replace all currency, but it's gonna become a lot more commonplace and like an option, like how Visa, MasterCard, like anyone who qualifies, you know, either for a debit card or credit card has one, if they can use it because there's so many places now that are cashless, right. And we're gonna get to a place where, you know, you don't have to pay in crypto, but it is an option. And like possibly a very prevalent one.

And what I really see this as is when we get to that point, whether that's five years from now, 10 years from now, is that theft on a much larger scale. And we're not really seeing, like I said, like one of the common ways is people will hack into someone's phone. We're not really seeing the cell phone numbers do a lot for security. There there's the pin, but I've also heard many stories of the cell phone company saying like, oh, well, whoever called us said they forgot their pin. So, it's actually like a fairly easy hack. And that's not really, there's not really a lot there that you know, the cell phone companies get in trouble for. And also it's, if we're talking about again, decentralized money that's not insured once it's gone. It is gone. For example, if someone got a hold of like both my checking and my 401k, they drained it tomorrow.

And there was like no way to reverse it. And it wasn't insured. I'd be in a lot of trouble. And, you know, while we're not necessarily seeing a ton of people putting their retirement assets as like digital assets as we're starting to see people's, I guess, like spending money or what they, what they pay bills or going out that kind of thing as becoming more of that as being handled with crypto, we're gonna be able to see a lot more people having, being targeted for crypto. Like the way we see a lot of people actually get their like credit card or debit card skimmed at a store. Well, it's gonna be so much easier if you wanna do something like that with crypto, because it's like, if I figure out like, you know, okay, this is that person's wallet. I can just take your, your crypto and you can't get it back.

So, we're gonna see that at a larger scale. And the other thing that I really see as a risk here is again, like, as there's increased adoption, we're starting to see like the larger institutions, you know, exploring like, okay, what do we do with digital currency? Some of

them are saying, we, we have our own digital currency, which would be centralized, which, you know, then that would probably, obviously they they're working a lot with, you know, legislatures and other people to figure out like, how do we do this in a way that's legal and safe. You know, and isn't like screwing over our customers, but they're also institutions who are figuring out how do we let our customers, like, let us like hold their Bitcoin. Right? And once we get to that state, it also kind of becomes a problem because again, traditional money goes bank to bank.

The banks are the intermediaries, but if the bank is like kind of an optional intermediary and it's like, well, I know let's say I don't, I don't understand how traditional crypto wallets work. I have JP Morgan Chase. I wanna get into this thing called Bitcoin. And I buy it through them and they hold it. Right. And then let's say somebody does something and they hack in and they're able to steal like the Bitcoin outta my account. Well, okay. If it's, if they are able to like hack into the, and specifically target the digital assets, right. That's probably gonna go to a private wallet. And once it goes to private wallet yeah. Like JP Morgan chase can probably find the identity of the wallet. They can send that to the authorities, but it's gonna be a lot easier for them to take it outta that wallet into a bunch of other wallets, which becomes like a big game with tag, which is a lot more work for them to follow that through a bunch of established banks that have, you know, known laws in different countries or wherever these bank accounts may be and like how they're going to handle this type of situation.

And also just rules about like how banks, I think there's gonna be the big question of like how banks will be insured, if at all, for like these type of digital assets. Because right now they're really handling things that are, you know, like fiat currency. And once we start thinking about things as like, you know, these digital assets where some of the use again are decentralized, but they are enough traction that people are gonna keep wanting to use them, even with alternatives of more centralized ones, like you know, central banks having their own digital currency. Those are things that we need to consider. And then I also think the other thing that we also are gonna see is when we have you know, Tesla very famous was like, we're gonna start accepting crypto. And I thought that was very interesting because I don't think they ever intended to accept crypto long term.

I really think that this was a short term thing because I think they wanted it as an asset, but they didn't wanna purchase any of it. And that's why I think they actually cut it off where they were like, okay, cool. Like we got what we wanted and we're, we're done now. We didn't have to purchase any of the crypto. It was just given to us. But the thing with that is depending on how Tesla did that, right? Like, I'm sure that's sitting in a wallet or wallets for Tesla, but does that now make them like, like a honey pot or like, does that make them a target because now you have this like a company that now has a larger amount of crypto

and there's again, like, I'm sure that they're doing a lot for security, but there are a lot of things where, you know, it, it is lot newer than how we've been dealing with, you know, digitizing banks with fiat currency.

And so I think will also be really interesting as institutions start accepting crypto them figuring out like, how do we, how do we best secure this? Because obviously if tomorrow you know, somebody took a big chunk of money from apple. Like, you know, Apple's probably gonna be fine, but that's still not great. And that starts getting into, like, if you target it enough of these companies you know, that starts becoming somewhat of a national security of threat. If you're able to kind of say like, "Hey, we're gonna target like Apple, Microsoft, Google, whatever, for like, you know, their specifically their digital assets," like all at once and like do things that are gonna seize that up. So, there's a lot of things that I think you know, like cuz how it impacts the economy and some of our bigger like companies that it becomes like really complicated.

And I also think that the laws will also need to catch up in terms of like, how, how are we gonna handle this? Because the adoption is continuing to climb. I don't see countries like the us, like banning this or outlawing this. And frankly at this point I think would be a big mistake if they did that. But like, you know, the laws and it's tricky because New York came along where it was like, "Hey, we don't want people doing this and we're gonna find you if you don't have a license." And people say that that really hindered innovation in blockchain and crypto in the state of New York when they did it. And it was kind of, they it's kind of agreed upon now that was too much regulation too early, but also too little regulation too late in this of once it becomes more mainstream, I think also has a lot of risks.

And there are other things where I also have seen where, you know, as you see more adoption, I really see the scam businesses that are saying like, "Hey, we wanna help you do this. We wanna help you do that" growing. It could get to that point in 10 years with crypto because you know, a lot of the people it's been around enough where it's like people who are about to be middle aged you know, are starting to get into it. So, in 10 years from now, we're gonna have people where it's like, they're a lot closer to retirement than they are towards the beginning of their career. And they're gonna be like, oh man, I really need to like put some gas in, in my retirement. Right. You know, having gone through like two recessions in a pandemic and everything else, and you're gonna see like I'm gonna reference a local channel here, like on New York one instead of the, like get into this annuity thing, if you're getting retired or da, da, da, da maybe that's not a scam, but it's kind of like, this is towards people who don't really understand about investing on and like being on a fixed income.

And I really see that as like for people in some of the, in like millennial generation and some of the older gen Zs who maybe didn't quite catch on in this wave. And maybe didn't quite understand them being targeted towards like, “Hey, you're about to retire.” There's a whole TV commercial. But by the time people realize it's like a scam, you know, the TV, commercial stop running, those people disappear. And if the laws and other things about these things don't catch up, you're gonna have people who are gonna be like, well, I was told if I put my retirement savings in an, in this thing that I would do great. I really see the algorithms, their biggest risk is we already see so many people excluded from our current financial system. And as things have been becoming more digital, like in terms of money, we are seeing that divide increase.

Because people are like, they don't really need to go to the ATM. So, you don’t need an ATM on every corner. Right? Like sometimes I go places and they're like, oh, the nearest ATM is like way over there. Right. it's just not necessary to carry around cash with you anymore. And so, as things become more and more digital you know, there's also the decision making element where as we're introducing more algorithms into our financial systems, things where, okay, we're trying to now get these people who have been traditionally excluded and having the algorithms saying like, oh wait, no, like not that person, like they, they, they don't qualify for this or they don't do that. Or like they're too high of a risk. And I know there's companies out there that are starting things to try to mitigate that. But it's really like, the question will be like, how scalable is that?

Because there are so many people, especially people with our, you know, our whole immigration problem where they're paid only in cash and they really have no way to turn this pay fiat money into digital money and have that accepted anywhere. And also it becomes a problem of like them getting robbed and it's there become less and less avenues for them to be able to pay with cash, you know, they will continue to become excluded. And, you know, that puts that population at like you unique risks as we're using more and more of these algorithms, whether it's in, you know, individuals accounts or whether it's, you know, at a much larger trading volume for much wealthier people, I really see also the potential for, you know, that market manipulation and people not real it until it's like, oh, by the way, like six months ago, somebody messed with our algorithm.

And as long as your assets are fine, we're fine and you're fine. But also like that was probably not like a good thing. Because we're seeing, I think like the more famous one is the, like the more manual version of fit with like those Reddit threads and Game Stop [and] AMC. But imagine if, you know, you could do that on a much wider scale and manipulate markets, like in your favor, especially if you're like a nation state or like that kind of thing, or basically do something to crash, you know crash something, or maybe not, could maybe do a whole economy, but you could do a lot of bad things. At very inopportune times.

Dr. Lydia Kostopoulos, Technology Innovator

The question at hand is what will future cyber enabled financial crime perpetuated by either cyber criminals or nation states look like 10 years from now. But before answering that question, I think that it's important to reflect on where we are today in the financial world. Today, we have constant cyber attacks against banks against multifactor authentication on banking apps. And this is just the beginning of it. The core infrastructure of the financial industry is also being threatened [like] by attacks on SWIFT. This has really great implications, the international financial infrastructure, as we look to see what kind of future cyber crime we would have in the financial sector 10 years from now, we need to also understand where we are in terms of our industrial revolution. Right now, we're in the fourth industrial revolution. One that is characterized by IOT (internet of things), fast internet, 5g, AI, quantum, all of these technologies are changing the paradigm in which we operate across every single industry.

And because of that, we also need to rethink not just the way we do transportation, the way that we do medicine, but also the way that we do finance, the way that we exchange goods 10 years from now, we can imagine that we will see different forms of currencies, so cryptocurrencies, stable coins, but also state backed digital currencies. These will be very important in having a backup to the fiat currencies of today and that infrastructure right now that we do use today, that is threatened. So, what will the future of cyber enabled financial crime look like 10 years from now? The ideas I have are as follows: one, cryptocurrencies and stable coins, as these become more popular and used in conjunction with Visa credit and fiat currencies. This will be a type of finance that will be lucrative to steal by different cybercriminal organizations. Similarly, there are rogue nations who will seek to use cryptocurrency even more so that they can bypass the international system. This already exists today. But they will be able, they will be using this more and, and more in 10 years from now.

Two, looking at the fiat currencies, we talked about earlier, how right now the financial infrastructure we have today can be threatened quite severely by cyber attacks. And there is a need to go digital. There are nation states right now that are already looking into a digital coin or a digital currency that would be state backed. So, a national currency right now China's already experimenting with that as are other countries, 10 years from now, this will be a source of competition between nation states, but also an area where one nation could commit financial war against another nation by attempting to digitally attack or undermine the cyber currency of a different nation that is backed by a different nation.

Three, the ways that we are going to be authenticating ourselves to pay are going to be very different 10 years from now. We're going to be using biometrics our face, our eyes,

our fingerprints, but also we'll be using our mobile phones with different social media profiles that we can use to pay or other authentication methods that are internationally accepted, such as, for example, Apple Pay or Google Pay. And if, and when these organizations decide to create their own digital currency or own form of credit, this will really change the paradigm in which monetary goods are exchanged, but from a cyber crime perspective, stealing profiles will be very lucrative in this sense. Identity fraud will become much more serious when we start to use our bodies and our social media profiles or any kind of digital profile to pay for goods and services. The future is definitely hard to predict, especially in this current environment, but I hope these thoughts could be of use as you explore the potential threats in the financial cyber crime space. Thank you.

Mei Ling Fung, Chair of the People Centered Internet

We should be really worried about very enthusiastic people thinking here's better ways to make the world better. Because I was one of those people 30 years ago I had been at Intel and I was the alpha test user for that marketing system. And I had before been an assembler programmer. So, when Tom Sibel at Oracle came and said, we're going to reinvent business customer relationships. I said, I've already done it at Intel. And then for two years, I had the time of my life. <Laugh> really, as the pioneer of CRM, we did it, Tom Sibel sold it. It has now become a $40 billion industry, but by the mid-nineties, the flaws were already starting to happen. But people were using this technology, which I had hoped would really benefit businesses and customers to exploit customer is to manipulate business management and, and some of these awful things.

The first one was customer surveys, which only asked questions where you could give high scores because the MBOs of the person designing it needed high scores. So, you never ask a question with a low score answer. That was just the beginning of what was just an awful nightmare. As I watched something, which I felt was my baby turned into a serial killer and that's what's happening now. And that's why I founded the People Centered Internet, cuz I needed to make sure that as we do the internet, we don't get too enthusiastic about the good stuff and forget about all the ways in which it can be used for bad purposes. There are extraordinary flaws in the internet as we have it. And whenever there's a flaw, it's just like a bridge. If you wanna bring down the bridge, you look for where themes are, where things might have gone wrong.

And all you have to do is wiggle a little bit there. And the whole thing will collapse. We are at that point of danger with the internet now because the internet was magic. It gave us an idea about what was possible when the globe was connected, but it was never designed to be fail safe, never designed to keep children safe, never designed for

old people, not to be exploited by scammers. All of this is happening. Now we have an internet that's built of straw. We need an internet that's built of bricks and that effort is not understood around the world. Right now, there is an effort by the UN to do digital building blocks that are the house of bricks. But you know, people are just going along thinking, oh, it works for me now. Just because it works now, nobody anticipated the impact that COVID would have on economies, on people's lives that potentially could happen with the internet.

I'm gonna give a FISO example at the very beginning of writing the invented writing, but the pushback was so great because it changed the powers, the authorities and who had the ability to invent the future that writing disappeared for 800 years before it could be reinvented. My real fear is that our communications are so fragile, even though they look so robust that we are not doing the hard work of making sure that they are what we need them to be for people to flourish. For example, you know, startups, isn't it wonderful startups. They make lots of money. You know, one of the most promising startups today, ransomware startups, yes, there's a ransomware village in Romania where if you wanna do a really good ransomware startup, you move to that village. It's written about in a book called Kingdom of Lies. And they have like shared call centers to explain to people how you change your, your money into Bitcoin.

So, you can pay the ransom. There's all, okay, what works, this works, that works. The other works. How do you get them to pay more money? It's a whole set up village to do that. We do not have the sheriffs in town to make sure that these kinds of things are spotted and eliminated. We are in that wild west magnificent seven time on the wild frontier, but gangsters are taking over whole communities because they don't have a sheriff and the lack of ability to come globally together on something like how, what do you do when you've got a ransomware attack that comes from an unknown country, we cannot organize ourselves. Why isn't cyber Interpol doing something about it? Well, it turned out that the head of CYBERPOL didn't know anything about technology. I know about this because the inside scoop in Singapore is that CYBERPOL has lots of money to hire great cybersecurity specialists. They all come to Singapore and then get hired by the banks because there's nothing to do inside CYBERPOL.

There's a total failure by institutions around the world to fix these problems. One of the reasons we can't chase down the bad guys is because the way the internet system of addressing is organized. So, it was organized for when there were 40 computers on the internet and all he needed was the CIS admin and the tech person and the admin person. And that's it. They never thought there'd be millions of computers on the internet. And that in fact, law enforcement would have to follow them down to try and find these ransomware companies. So, the DNS, [the] name system DNS, who's system is under the

control of ICANN -- ICANN has abdicated responsibility for helping to improve it so that the right people can get the right information. ICANN is our job; [it's] what's public and what nobody can see that doesn't help chase down the bad guys. So, the People Centered Internet is really working on these kinds of fundamental issues.

Edmund L. Luzine, Jr., Ausable Funds

I think the first thing to think about is whether or not, if you are a criminal or some kind of other nefarious terrorist slap, or, or VEO violent extremist organization, do you want to use some type of crypto currency as the way in which to profit from your activities? And furthermore, do you want to use them in a way in which to invest or hold the assets you obtain through your illicit or illegal activities? And, and I think there's a mixed view on this. Obviously it is much easier from a physical standpoint to have digital assets to have things out there in the e-space however, there seems to be a growing problem with being able to access them and being able to access them when you want to and maintaining them.

So, for example you know, I think back to the original something that might have been competitive with this from many decades ago and that being bear bonds, you know, if, if you held the bond, the physical note, that was it, that was the equivalent of cash. You didn't need a code to find the bear bonds. You didn't need a computer to go and get the bear bonds. You either had them in your briefcase or in a closet or in a safe box, or maybe distributed in multiple locations around the world. So, the case at crypto you've got something, or, you know, whether it's Bitcoin or Ethereum or Doge Coin or whatever, the latest type of crypto currency is out there. You have some concerns about accessing it, and there have been multiple stories about people losing their passwords to accounts which is kind of unique.

The other thing is which, which you just saw from the hacking of the Colonial Pipeline and the ransom for it, which I believe was paid in Bitcoin, that the FBI was able to trace that Bitcoin and get some of the ransom back. I'm not sure if they're actually able to get all of it. So, if you are a criminal organization, would you really want to use extensively or rely on as your primary choice? Something like a Bitcoin. And I guess my thinking right now is no, you would not want to use that as, as your primary choice of, of an asset. And I, I won't, I don't think I'll call it an investment cuz you're not getting a return on it. It's not a security. Although it will fluctuate in value based on supply and demand in the marketplace for it.

So, you, you know, again, if I am a North Korean hacker group, if I'm a Bacan hacking group or Russian affiliated APT bear or whatever the term is for those groups, do I want all of

that Bitcoin traceable? And, and again, my thinking is, no, I, is that maybe one third, or once you get it, can you easily convert it to cash or to gold or, or something else and get it out of the electronic spear sphere where somebody can and track it or better yet where one of your colleagues in the group can steal it from you and then move it quickly to somewhere else. And then they just resign from your group or leave and move on. So, my thinking is that there are concerns, you know, going out over 10 years, how popular does this become?

Also which kind of cryptocurrency becomes more popular versus others. And those are kind of my initial thoughts on the use of crypto for hack, for cyber crime, for a nation state. So, I, I like when I look at all these digital assets, I I like to have these discussions in the most tact and polite way I can. And, and I try to say to people, imagine if we could go back to World War II or in a, in another manner, imagine if you could bring the Nazi the party forward to now and your ability to identify people at ease based on a certain, you know, certain cultural, societal, ethno, religious group, and all these things like Facebook and LinkedIn and in China, WeChat, and all these other electronic platforms that people contribute to make it much easier for a nefarious government or an ill intended government, or quite honestly, parts within a government to ID people and target them.

So, if you are a nation state, you should theoretically be very happy with the movement of more assets in general, moving into the digital realm because number one, that makes it much more easier to identify people to segregate them. And also at the end of the day to either steal from them or, or quite honestly, as you see in the case with China right now, and the crackdown with technology firms, essentially to tax them more or in what China is saying to distribute the wealth or common prosperity. So, yeah, from the government side I think there are some very unique opportunities where they want to be able to digitally track or be able to tax people much easier with all of these different types of digital currencies or cryptocurrencies. Whatever. I mean, you could just go back and think and look at any kind of extremist type of government that's existed.

Let's say over the past a hundred years, whether it's a right wing fascist type of dictatorship, like in Chile or a left wing one in, in let's say Cuba or Nicaragua, if everybody's money were digital and you kind of controlled the pipes or the communication systems, you could be able to hack in and monitor all of that. Furthermore, you could also monitor all types of relationships between people and quite honestly, if you're the party in charge you could monitor also your opposition party or parties in their financial transactions and who is involved in each of those parties. So, I, I think it provides a very from that aspect, it, it provides a very unique opportunity to conduct surveillance or gather intelligence and see who find what and where, and almost in kind of the opposite argument.

You look at the challenges that the U.S. and allies have had over the past 20 years with terrorism, finance out of Afghanistan and Iraq and other parts of the Middle East and how those efforts have made more difficult through the hawala financing mechanism, which one could argue is almost the exact opposite of the digital, the various digital currencies that are now developing around the world. Hawala financing mechanism basically only allowed for currency exchange via a physical hard copy type of notebook or ledger that was maintained in different locations, not across the Middle East, but the world. So, unless you could get your hands on one of those, it wasn't like there was a there wasn't an electronic ledger in Google Docs that every hawala dealer could go online and update. So, it made it much easier for them to finance their operations and what they were doing.

I think there are a number of things to think about, and that is if you look at you compare something that happened in Panama trying to think how long ago the Panama paper situation was, but you had, and, and you also had a similar circumstance out of Switzerland, but you had the case where all of these electronic systems allowed for the concentration of records and files and assets and how disgruntled employee internally was able to take all of those records, duplicate them, and then hand them over to the press and let them know as to, in the case of Panama, how many government officials had accounts, how many had shell corporations and more specifically, which Panama still allows for how many had numbered accounts. So, and you also had that in Switzerland. It would be interesting to see if anything ever comes like this out of Dubai where you have the same type of disgruntled person in an Arab bank in the United Arab [Emirates] that would show how much money had come out of Afghanistan or out of Pakistan or out of other places had been thus far obtained.

So, there are, I think the one thing to leave with is that there are, there do seem to be a number of mechanisms developing and platforms that allow for it, for people to, or, or groups, financial criminal groups, or nation state groups to distribute their assets in much more different and unique places, whether it's through something like Bitcoin or somehow if they get a cash in some kind of application, whether it's through like a PayPal or a Venmo and they can easily move it around outside of the traditional banking infrastructure. I think that's a very unique thing to look at it as is something like a Robinhood trading platform that allows you to trade currencies and commodities and stocks very easily with low costs, if anything there's a whole bunch of things out there that are allowing people to do more like a better word, negative or nefarious activities at a very lower cost.

But again, I, I guess, so we get back to something, one common denominator besides the occurrence, the money aspect that all of these things had is that you need access to the internet and or to phone lines. So, that makes it very easy for a nation state to be able to

surveil and collect on. And it also would also, it would also make it easier for some type of group, not necessarily intercept those communications, but interrupt them through something as simple as, as just, you know, pulling the plug on systems that they couldn't operate or maybe jamming the actual transmission of data. So, the reliance only on the digital infrastructure, I think it makes it much easier to interrupt.

Ann Cairns, Mastercard

Well, first of all, let's start with the idea of the cashless environment. I mean, I think it's very interesting because we're still in the middle of the pandemic right now. And to a certain extent, what we've seen this year is a massive shift from paper based to electronic payments a shift that ever seen the size of in, in recent times. So, obviously that's really good news from some points of view and has driven consumers to behave in a completely different way. But also if you think about things like climate change coming onto, you know, becoming much more of a reality for us with the flooding and the fires and so on you could see a time where technologically having everything automated to the level that we do with no backup could be quite catastrophic economically and sociologically for society.

So, I do think that actually the recent shift that the pandemic caused you know, could be sort of bringing us into more of a danger area. If we actually aren't prepared to deal with all of the contingencies that we're gonna need to build in because of, you know, flooding and fire and, and, and so on. So, that's one thing that I've been thinking about recent. I had been in, in the investment bank and city during the first big crash in the eighties, '87 Black Monday in October. And in my time I spent the first year or two unwinding swaps portfolios and being involved in how you actually systematically reduce your risk across investment banking, but nothing of the scale of Lehman and what you saw in Lehman were lots of different things happening, different, a patchwork quilt of bankruptcy laws across the world, which actually didn't jive with each other.

So, different administrators making different decisions about how you would deal with different parts of the bank, which as somebody who was restructuring, the holding company was quite dramatic. The other thing that you saw was, you know, you would think that very good banks who were in control of their risk would immediately take action. And that is indeed what happened. We saw some of the sort of best prepared banks actually unwinding their positions with Lehman at a very, very rapid rate. But what actually to transpired was that they were operating in the first, you know, few days and few weeks of the chapter 11 of the bankruptcy. And actually that was the most volatile period. So, while it looked like they were doing something that ha you know, was really good from

a mass risk management point of view financially, it was probably something which was a, a really could have resulted in much higher losses for them than if they had waited and unwind at a slower rate.

So, some of the things that you think intrinsically in the financial services industry --things you should do-- are not necessarily, you know, the right answer in a sort of crisis situation. And at that time you know the, I don't recall what the level of algorithmic trading is, but I think there is a link here because if you are highly automated, and if you are into say algorithmic trading and something happens in the market then what you could have is a, is a whole raft of algorithmic decisions made in sort of split seconds, which would cause much rapid, more rapid financial instability than you could have experienced if you were actually in, in more of a manual trading environment. And I think that is actually a serious risk to find financial stability in the system going forward.

If and, and, you know, the, the thing about this is that if you think about it in respect of say cyber crime and so on if you start actually having big attacks on is that are linchpins in the system then you can bring down huge sways of the financial system without too much, too much further effort. If you see what I mean, what do I, what do I mean by that? Well, for example, when Lehman collapsed I, that something in the, in the swaps area, it was about 90% of the transactions were called what they call like over the counter. And only 10% of the transactions went through the clearing houses.

So, therefore there was a lot of bilateral risk system, but there wasn't the concentration of risk. However, when transactions actually go through a clearing house then, you know, there are all sorts of other protections that are built in there. A waterfall of risk management systems kick into play, obviously the different members of the clearinghouse put in a certain margin level. There are all sorts of different rules about how you operate there's skin in the game from the operators. And, and so on. So, allowing you to take action, if you saw one player, go down to be able to, you know, manage a default process without affecting the rest of the market. Having said that though, you know, you also have to have a view that says you've concentrated risk in a, you know, an area. And so now maybe you've got 70% of your transactions now being processed this way and 30% bilaterally, and that's gonna change your whole wholesale risk.

So, as individual players get hit, you know perhaps you're in a much safer environment to manage that. And I'm sure that everybody in risk departments across the financial space have learned a lot since 2008, 2009. But you know, if you hit a hope, if you hit something that's controlling everything, then you know, obviously that's much more serious. However, having said that the level of cyber securities, you know, investment in the hopes is, is massive. And similarly with MasterCard's network, you know to my knowledge and

MasterCard's network has never been breached. Although you hear, you know, things like, oh, Target --customers of Target-- had their information shared and so on, but that's not the level of actually hitting the network that is, you know, a, a specific user of the network. Similarly, banks have been breached. We know that by financial criminals and also by state actors.

But you know, you, haven't seen sort of a major hub breach in recent times as far as I'm aware. So,, so because I, and I guess that the reason for that is that it's the layering really it's, you know, it's the outrunning, the lion <laugh>, I guess that it's easier to breach the, you know, the players who are less protected thinking about the infrastructure of the future, you know, who is actually providing the, the componentry and the ability to operate the infrastructure of the future. And what could they do with that? If the, if you were more in a state of war kind of situation, that would be pretty scary, quite honestly. And I, I think that everybody's thinking about that right now. And in respect of not just things like 5G, but it's also things like nuclear power and so on, [not] necessarily weapons per se, but things that can be turned into weapons.

And I think in the space of the next 10 years, well, I think actually right now everybody's diversifying their supply chain, and it's not just because of, you know, sort of criminal threat or state actor threats, but it's probably a good thing to do because we've probably become a bit more complacent about supply chains than we needed to be, because we haven't designed them you know, to, to cope with things like COVID or even ships getting blocked in the canal, right? So, it comes down to you're living in a digital world, but actually the physical componentry of the things that you need to operate in a digital world you know, have to be thought about as well as the general sort of health of the, the population that, you know, are operating your systems and maybe even using your systems, because, you know, we say you can't be successful at MasterCard.

You can't, you can't be successful in a failing world. So, let's, you know, our products and services reach 3 billion people on the planet and our whole, you know, infrastructure operations. And the way we run our business is all predicated and designed on that. It was also, you know, designed to cope with an incredible amount of cross border travel and so on and so forth, which has gone away, but no doubt will come back at some point. And the point about this is that, you know, if whole sways of, you know, populations get affected by one thing or the other, you know, either by crime, either by, you know, pandemics either by global climate change, then big pieces of your business and big pieces of your supply chain could actually be impacted. So, I think that's, you know, that's certainly gonna be happening more and more and more as we go into the future.

The other thing about the future is yes, people are thinking about big global systems

and their, you know, governments and state actors are thinking that they want more localization certainly of their data. And I think that affects you as a global player. There could be pluses and minuses to that, of course, because, you know, if you are, if you are more if you're more flexible in terms of the way that you've designed your networks, and you've got very many nodes there and that one node could pick up from another node, then if, if nodes say in a country was attacked and you had an ability technically to shift to another node quite quickly, that would be a good thing to, to help you attack, you know, to help you prevent you know, fraud and, and crime. And so on. Artificial intelligence of course, is, is probably, you know, the most important tool that we've got in our arsenal right now to, to address fraud because we, we deal with up to a billion transactions a day in MasterCard, and there's no way that we could process those in real time and do fraud checks without artificial intelligence.

And the thing about artificial intelligence is I think that it's now used at a level, which is still sort of pretty mundane in my view. In other words, it's not really intelligent yet. And, but with the advent of 5g, the advent of quantum computing, it's going to change dramatically. And I think sort of the intelligence of being able to see something and analyze it and detect it and, and sort of stop it spreading will be there. But at the same time, the cyber criminals are really smart and they're, you know, they'll be using artificial intelligence to do exactly the opposite. So, it's, it's a chess game. I mean, it's always gonna be a chess game, isn't it? And you know, you're gonna have to put massive investment in to actually stay that one step ahead. That's presumably what we're trying to do all the time now. So, it's gonna be a very interesting world from that point of view.