Mastercard Threatcasting Report

WHAT ARE THE FUTURE CYBER THREATS TO CRITICAL FINANCIAL AND COMMUNICATIONS INFRASTRUCTURE SPANNING GLOBAL GROUND SYSTEMS TO SPACE-BASED ASSETS?

Legal Disclaimer

Table of Contents

Table of Contents

Executive Overview

What are the future cyber threats to critical financial and communications infrastructure spanning global ground systems to space-based assets?

In the next decade, the expansion of financial and communications critical infrastructure (FIN/COM CI) — from global ground systems to space-based assets — will generate a unique set of future conditions. These conditions could multiply the scope, scale and speed of future threats by taking advantage of rising privatization and militarization and by undermining situational awareness of the operating environment. The rapid cascading effects of these threat multipliers could turn FIN/COM CI into a Minimum Viable Target for nation-states. Nation-state FIN/COM CI consumer-centered attacks will have a destabilizing chain reaction across systems and markets, leaving attribution nearly impossible and retaliation an unlikely option.

Future Threats

Threat Multipliers with Cascading Effects

Increased scope, scale and speed of future threats with cascading effects across business and consumer networks generate a destabilization of confidence and trust

Becoming the Minimum Viable Target (MVT)

Offering nation-states and their proxies maximum benefit with minimum effect and little chance of attribution or retaliation

Next Steps

Socialize

Monitor

Partner

Advocate

threatcasting

What is Threatcasting?

Threatcasting is a conceptual methodology (Figure 1) that enables multidisciplinary groups to envision and plan systematically against threats 10 years into the future. Analysts explore how to transform the future they desire into reality while avoiding an undesired future.

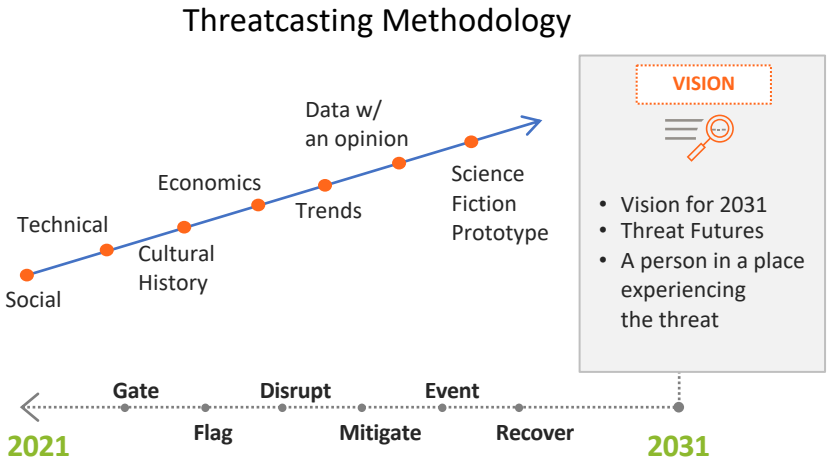
Threatcasting uses inputs from social science, technical research, cultural history, economics, trends and subject matter-expert interviews. The diversity of inputs allows us to predict potential future conditions; some of these futures are desirable, while others are to be avoided.

The results of the threatcasting process and workshop provide a new and innovative perspective on the broad range of potential threats at the intersection of technology, culture and economics. The methodology also identifies what flags or "warning events" could appear that would indicate progress toward a particular threat future.

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

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

Figure 1



threatcasting

Mastercard 2021

Threatcasting Workshop Overview

Workshop Purpose

Through our threatcasting workshop, Mastercard sought to identify possible cyber threats to critical financial and communications infrastructure spanning global ground systems to space-based assets up to 10 years into the future. Additionally, the assembled participants determined what organizations and ecosystems could do to disrupt, mitigate and recover from these possible threats.

Workshop Process

Mastercard worked with futurist and Arizona State University Professor Brian David Johnson. Johnson invented the threatcasting methodology a decade ago and served as the lead researcher, analyst and author for this report. Mastercard tapped into Johnson's outside perspective to both challenge and validate current research inputs, approaches and findings.

In June 2021 a cross-functional group of Mastercard practitioners, partners, customers and security practitioners from across government, industries and academia gathered virtually over the course of a week to create models of threat futures. Drawing research inputs from a diverse data set and from subject matter-expert interviews, participant groups synthesized the data into workbooks, curated with Johnson specifically for Mastercard's purposes.

FIN/COM CI

threatcasting

FIN/COM CI

Background

Before the workshop groups could begin exploring future FIN/COM CI threats, participants had to define and explore the conditions of this environment a decade into the future.

To derive 2031 FIN/COM CI future conditions, the groups interviewed more than 25 subject matter experts (SMEs) over four months. The interviewers posed open-ended questions based on the Threatcasting Workshop Research Question (e.g., As you look 10 years into the future of financial and communications critical infrastructure, what are areas of concern?). Each interview was audio recorded and algorithmically transcribed.*

The transcribed interviews were synthesized then analyzed as future conditions that were later used as prompts for the workshop. Additionally, some areas and groupings were identified for later threatcasting exploration.

Defining a Unique Attack Surface

The synthesis and analysis of SME interviews began to clearly define the conditions and environment of two key components of critical infrastructure.

Italicized passages are excerpts from the Cybersecurity & Infrastructure Security Agency's (CISA's) website. CISA provides the government's definition of critical infrastructure and critical infrastructure in the finance and communication sectors.

Critical infrastructure describes the physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety. The Nation's critical infrastructure provides the essential services that underpin American society.[1]

There are 16 critical infrastructure sectors whose assets, systems and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. This directive supersedes Homeland Security Presidential Directive 7.[2]

*Transcripts available in project folder

[1] https://www.cisa.gov/infrastructure-security

[2] https://www.cisa.gov/

CISA's 16 Critical Infrastructure Sectors

Figure 2

Financial and Communications Critical Infrastructure Combine

As a part of this threatcasting project, the groups combined two of CISA's Critical Infrastructure Sectors: Financial and Communications. This combination creates a unique attack surface for future threat actors.

Financial Services Sector[3]

The Financial Services Sector includes thousands of depository institutions, providers of investment products, insurance companies, other credit and financing organizations, and the providers of the critical financial utilities and services that support these functions. Financial institutions vary widely in size and presence, ranging from some of the world's largest global companies with thousands of employees and many billions of dollars in assets to community banks and credit unions with a small number of employees serving individual communities. Whether an individual savings account, financial derivatives, credit extended to a large organization, or investments made to a foreign country, these products allow customers to:

- *Deposit funds and make payments to other parties*
- *Provide credit and liquidity to customers*
- *Invest funds for both long and short periods*
- *Transfer financial risks between customers*

[3] https://www.cisa.gov/

Communications Sector[4]

The private sector, as owners and operators of the majority of communications infrastructure, is the primary entity responsible for protecting sector infrastructure and assets. Working with the federal government, the private sector is able to predict, anticipate and respond to sector outages and understand how they might affect the ability of the national leadership to communicate during times of crisis, impact the operations of other sectors and affect response and recovery efforts.

CISA specifically calls out that the Financial Services Sector is closely linked to The Communications Sector: "The Financial Services Sector, which relies on communications for the transmission of transactions and operations of financial markets."[5]

FIN/COM CI

As a term, "FIN/COM CI" captures the unique qualities at the intersection of finance and communications, closely linked sectors of critical infrastructure. Currently, this is not an official designated sector, like the Financial, Communications or Energy sectors, but for the purposes of this report, establishing the specific boundaries and conditions for this combined sector allows for specific threat mapping and for indicators to be monitored.

The combination of the financial and communications portion of CISA's Critical Infrastructure Sectors allowed us to focus on these two areas in detail.

[4] https://www.cisa.gov/

[5] Ibid

Future Conditions

Future Conditions Overview

The SME interviews and research helped identify future conditions for the FIN/COM CI environment from which a series of future threats could arise. The future conditions identify possible vulnerabilities and attack surfaces.

Future Conditions

1. The Unexpected and Unknown: Speed, Scope and Scale
2. Increasing Privatization and Militarization
3. Operating in the New “Unreality”

The 2021 Threatcasting Report explores some of the possible and potential threat futures; however, the depth of the future conditions provides a data set for more threatcasting explorations. Three additional areas were identified for further threatcasting exploration.

Future Conditions Detail

The Unexpected and Unknown: Speed, Scope and Scale

- Increasing technological and partner complexity
- The perils of speed
- Dangers in the cloud
- Weak links with partners
- Technical safeguards replace physical safeguards
- Adversarial parity
  - Attack capability
  - Development location
- Insider threats persist

Increasing Privatization and Militarization

- Privatization
  - In space, failure is an option — “fail and replace”
  - Dangerous bedfellows — hybrid software stacks
  - There’s just no room — increasing deployment and junk
  - Policy environment continues to be gray
- Militarization
- Nation-state and proxy attacks on infrastructure
  - Financial gain
  - Destabilization
- Acts of spectacular terrorism
- Physical attacks
  - Weather and the sun (ground and space)
  - Cable cuts and other similar physical attacks
  - Satellite killers

Operating in the New “Unreality”

- Emulation attacks
- Time and space manipulation
- The dark web expands
- Zombie/parasite satellites and networks
- Failures of attribution

Areas for Further Threatcasting Exploration

Identity Crisis

- The perils of future transactions when identities can be hacked, stolen and verification is impossible
- Q4 2022 rapid threatcasting

The Quantum Menace

- Emerging threats from quantum computing and hybrid environments technical safeguards replace physical safeguards

Cryptocurrency and the Privatization of Money

- Cryptocurrency is moving the balance of power as well as the power of the state and fundamentally changing how transactions are conducted

FIN/COM CI
Threat Futures

threatcasting

Threat Futures

Overview

In the next decade, the expansion of FIN/COM CI from global ground systems to space-based assets will generate a unique set of future conditions that will multiply the scope, scale and speed of attacks, taking advantage of rising privatization and militarization as well as undermining situational awareness of the operating environment. A new set of evolving future threats will rise from these conditions, taking advantage of threat multipliers with rapid cascading effects and advancing FIN/COM CI as a Minimum Viable Target for nation-states. These FIN/COM CI consumer-centered attacks will have a destabilizing chain reaction across systems and markets, leaving attribution nearly impossible and retaliation an unlikely option.

The actors in the Primary Threat Futures were the usual suspects: criminals, lone wolves and state-sponsored attacks. However, we determined that the goal of their threats will not be for financial gain.* The aim of their attacks will be to destabilize industries, consumers and governments via loss of confidence and trust to the advantage of criminals, businesses and geopoliticals. In some consumer-centric cases, the goal may even be to incite civil and business chaos.

Secondary Threats

Along with the Future Conditions, there were two Threat Futures. These are identical for both Primary Threat Futures, but their influence on the attack as well as how they can be detected and disrupted are unique.

Threat Multipliers with Cascading Effects

- The Rise of Hybrid Attacks (Physical/Digital)
- The Insider: Shortest Path to Attack

Becoming the Minimum Viable Target (MVT)

- The Insider: Shortest Path to Attack
- The Rise of Hybrid Attacks (Physical/Digital)

*See APT Bank Attacks (C2GD, C2GE) were examples of criminal activity

Threat Future 1

Threat Multipliers with Cascading Effects

The increased scope, scale and speed that will exist across FIN/COM CI act as a threat multiplier, where a single attack can quickly propagate across networks with cascading effects across business and consumer networks generating a destabilization of confidence and trust.

The concept of a "threat multiplier" built from the definition of a force multiplier. "In military science, force multiplication or a force multiplier refers to a factor or a combination of factors that gives personnel or weapons the ability to accomplish greater feats than without it."[6] In other words, the future conditions that will exist across FIN/COM CI mean that a single attack can take advantage of this threat-multiplying effect to accomplish greater damage far beyond the initial attack. Additionally, these effects will surpass a linear chain reaction, moving to cascading effects across multiple networks.

The future conditions one and two (Unexpected and Unknown and Increasing Privatization and Militarization) were key drivers for this threat. In this landscape, each technology, node and partnership affords attackers a powerful attack multiplier with the added benefit of cascading effects across business and consumer networks. These attacks are amplified and magnified by the speed, scope and scale possible in the conditions. It is this amplification that hastens and broadens the destabilization of confidence and trust.

Many of these effects will lead to not only financial loss but also loss of consumer confidence and trust — possibly leading to a level of commercial and consumer chaos. It is the amplification and cascading effects that occur so fast, far and uncontrolled that means the attack is less about financial gain and more about destabilization and chaos.

[6] https://en.wikipedia.org/wiki/Force_multiplication

Threat Future 2

Becoming a Minimum Viable Target (MVT)

FIN/COM CI presents nation-states with an MVT that affords them the maximum benefit with the minimum effect and more importantly a lessened probability of attribution and retaliation.

The idea of an MVT builds off the concept of a minimum viable product. "A minimum viable product is a version of a product with just enough features to be usable by early customers who can then provide feedback for future product development."[7] Minimum viable products are a staple of Silicon Valley Tech development. It is attractive to developers and investors because it means that a company can get the possible benefit of the proposed product with the lease amount of effort.

Applying this concept to an MVT means that a nation-state can use FIN/COM CI to attack another nation-state or adjacent industry to gain strategic advantage. However, because the attack is in the private sector means that the amount of effort will be less, as there is a wider array of attack opportunities.

Attacking the weaker edges of FIN/COM CI will be easier than larger more sophisticated parts of the ecosystem. However, FIN/COM CI is more attractive because the attack originates at the business or consumer level, making attribution difficult to impossible and ensuring that retaliation will be likely. For nation-states, these factors make FIN/COM CI geopolitically attractive, specifically down to the consumer level.

[7] https://en.wikipedia.org/wiki/Minimum_viable_product

Threat Facilitators

The Insider: Shortest Path to Attack

For activists, extremists and nation-state actors, the complexity of the networks as well as the countermeasure undertaken by the industry make the insider threat the shortest path for an adversary or their proxy to attack and gain strategic advantage.

The Rise of Hybrid Attacks (Physical/Digital)

The complexity of the FIN/COM CI will stretch across digital networks and physical infrastructure as organizations move to purely digital security measures. This will open new physical vulnerabilities for global ground systems (e.g., IoT, autonomous transportation, smart cities) as well as space-based assets (e.g., satellite clusters, decommissioned equipment).

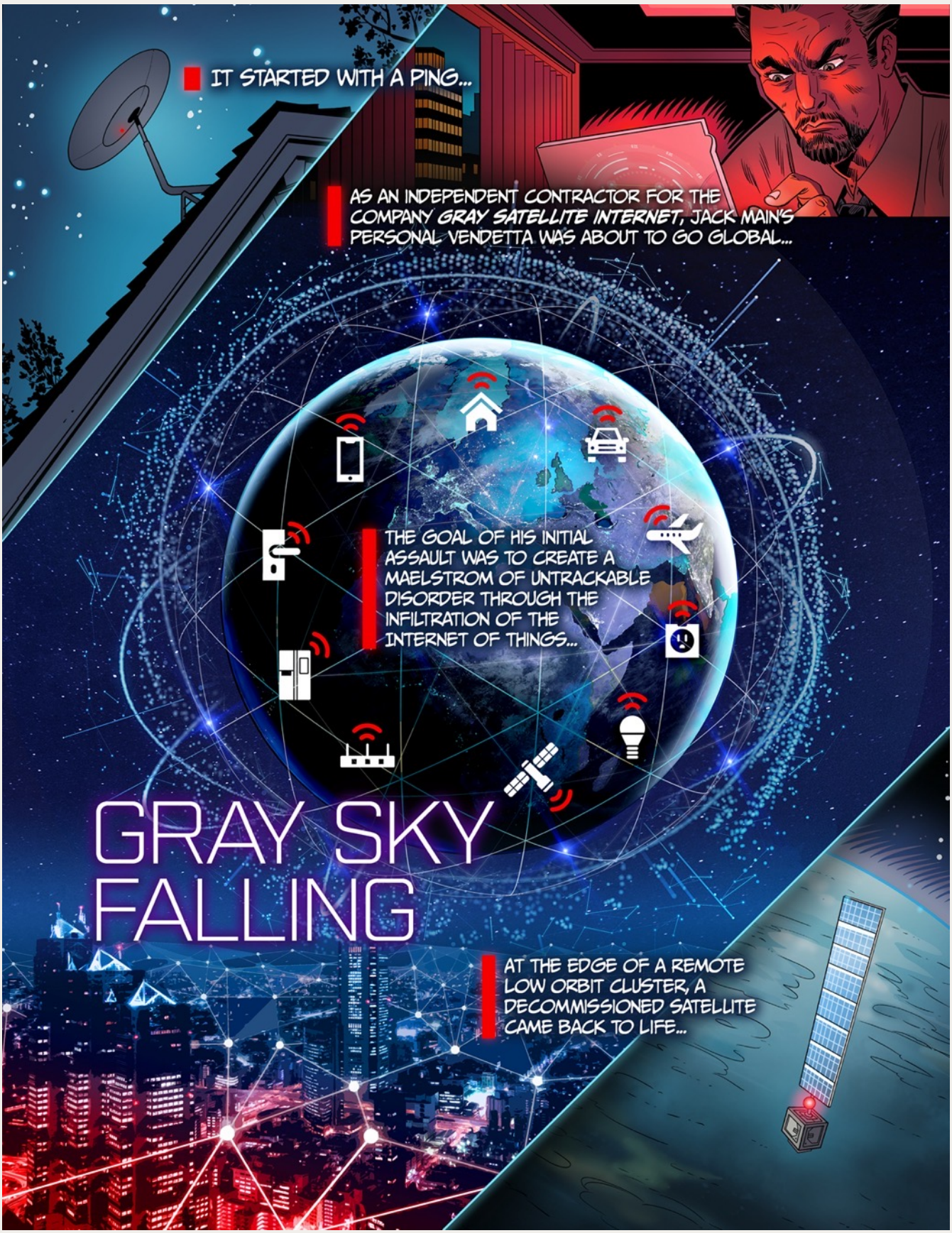
Threat Future 1

Threat multipliers with cascading effects

Increased scope, scale and speed of future threats with cascading effects across business and consumer networks generate a destabilization of confidence and trust

Threat Future Visualization

Science fiction prototypes are visualizations based on research, future models and current activities. These visualizations are purposely not sensationalized depictions of possible and potential threats. They are used to make threats visceral and concrete for the reader. The following visualization explores a future where a single attack is enhanced by a threat multiplier in FIN/COM CI with cascading effects.



threatcasting

threatcasting

Threat Future 1 Indicators

Flags

Threat Indicators

Threat indicators are meant to give an organization early warning and clear signals that a specific threat is beginning to manifest. They can be used so that organizations do not react too early or too late to global events. Fundamentally, these signals are clear, observable, quantifiable evidence upon which strategies can be built.

Overview

Threat 1 — “Threat Multipliers”

- Technology/Networks
  - Anomalies, reports of compromise, short outages and uncertainty in AI development
- Organizational/Cultural
  - Rising isolationist tech regulations and practices, new entrants and similar attacks in other industries
- Identity
  - Data consolidation, early discussions, activities and consolidation

Threat 2 — “Becoming an MVT”

- Geopolitical
  - Shifts in manufacturing, markets and controls
- Consumer
  - Blended personal and corporate hacks, IoT-based identity crime, disruptions and theft
- Industry Monitoring
  - Shifts in adversarial chatter, workforce, technology reliance

Indicators Detail

Technology/Networks

- Anomalies in space-based portion of edge system
  - Flow disruption at onset of transaction
  - Inability to track payment completion
  - Other generalized anomalies
- Reports of compromise and incidents of space communications infrastructure
- Proliferation of Low Earth Orbit (LEO) networks with easier access for new operators
- Short window outages of space-based systems (e.g., Drop-in services)
- AI development and evolution continue with uncertainty
  - AI acting in uncertain way
  - Unexplainable AI outputs
  - Anomalous behavior

Organizational/Cultural

- Rising anti-foreign tech movement; active and structured
- Event that creates doubt in terrestrial communications, driving reliance on statistics (e.g., natural disaster)
- Similar data integrity manipulation attacks in other industries
- Entry of new countries and companies into space data networks

Identity

- Consolidation of identify control measures into fewer, more easily targeted systems
- Activity from "out of region" indicating potential identify theft
- Dark forum discussion on authentication bypass techniques
- Fraudulent activity on personal platforms and business accounts
- Increased instances of sophisticated identity theft

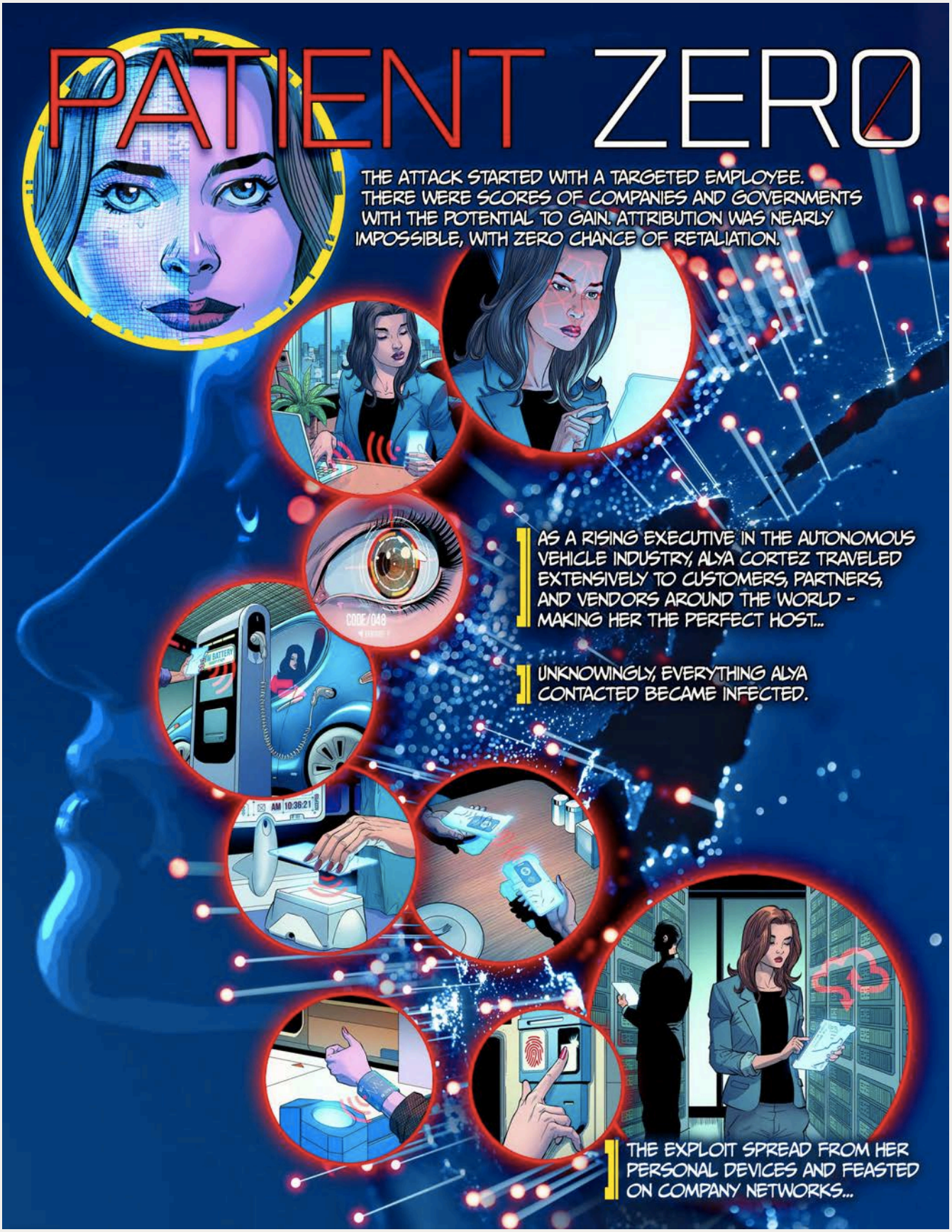
Threat Future 2

Becoming the minimum viable target (MVT)

Offering nation-states and their proxies maximum benefit with minimum effect and little chance of attribution or retaliation

Threat Future Visualization

Science fiction prototypes are visualizations based on research, future models and current activities. These visualizations are purposely not sensationalized depictions of possible and potential threats. They are used to make threats visceral and concrete for the reader. The following visualization explores a future where a targeted attack on an unknowing insider threat that moves from personal devices to corporate systems eventually destabilizing an entire industry and beyond. Because the attack is initiated with an individual and utilizes FIN/COM CI, there is little chance of attribution or retaliation.



threatcasting


THE ATTACK ADVANCED ACROSS THE INDUSTRY. ROLLING TRANSACTIONAL FAILURES, SUPPLY CHAIN BLACKOUTS, AND UNRELIABLE PAYMENTS DESTABILIZED THE INDUSTRY.
SUPPLY CHAIN DISRUPTION
TECHNOLOGY BREACH
THE SEISMIC SHOCK RATTLED LOCAL AND NATIONAL ECONOMIES.
PROTESTS & CIVIL UNREST
CONGRESSIONAL INTERVENTION
ECONOMIC FAILURE
INDUSTRY FAILURE
I DON'T KNOW YOU ANYMORE. PLEASE LEAVE! I DON'T WANT TO CALL THE POLICE AGAIN...
IT WAS TOO LATE WHEN ALYA DISCOVERED HER PERSONAL AND PROFESSIONAL IDENTITY HAD BEEN HIJACKED. HER LIFE, HER COMPANY, AND THE ENTIRE INDUSTRY LAY IN SHAMBLES.

Threat Future 2
Becoming an MVT Indicators

Flags

Threat Indicators

Threat indicators are meant to give an organization early warning and clear signals that a specific threat is beginning to manifest. They can be used so that organizations do not react too early or too late to global events. Fundamentally, these signals are clear, observable, quantifiable evidence upon which strategies can be built.

Indicators Overview

Geopolitical

- Increasing market share for microchips outside U.S. and ally
- Increasing global market share for final goods manufactured outside U.S. and ally
- Increased control of free expression within outside U.S. and ally

Consumer Monitoring

- Personal information (e.g., financial, education, medical, etc.) is “stolen” via constant use of the IoT
- Disruption to consumer ability to make or pay for travel-based transactions
- Hacked personal information blended with corporation information that is “hacked” and stolen. (e.g., Consumer to corporation “hopping”)

Monitor

- Adversary and threat actor chatter
- Monitoring banking systems to provide specific destabilization indicators
- Increasing reliance on technology in traditionally non-tech industries (e.g., farming)
- Reduction in skilled and traditionally non-tech industries workforce
- Market manipulation activity in traditionally non-tech industries

Gates

Actions to Be Taken

Once a threat has been identified, an organization can begin to take action. Many of these actions can be taken early to disrupt the threat before it even happens. Utilizing the indicators as a signal of a threat's progression, an organization can make strategic decisions about when to invest capital and effort to mitigate or recover from the threat. The post analysis of the threatcasting data showed that there were three types of action that could be taken to disrupt, mitigate and recover from this threat future.

FIN/COM CI Threat Future

Actions to Be Taken Overview

- Threat 1 — “Threat Multipliers”
  - Guard against and slow down the cascading effects
  - Audit partners and launch events
  - Insider Threat Program
  - Increased industry corporate and government partnerships
- Threat 2 — “Becoming an MVT”
  - Increased industry corporate and government partnerships
  - Promote resiliency beyond the network to a resilience of confidence and trust
  - Educate and harden the edges of the network and ecosystem
  - Monitor rehearsals

FIN/COM CI Threat Future

Threat Multipliers

Actions to Be Taken (Detail)

- Guard against and slow down the cascading effects
  - Begin to use and install “Circuit Breakers” (e.g., algorithmic trading on the stock market)
  - Test containers: create test environments for technology and partnerships
  - Specifically threat-trained AI
    - To stop anomalous behavior to limit damage and spread
    - Provides early detection and alerts to minimize damage
  - Identity theft monitoring and services (e.g., Dark web surveillance)
- Audit partners and launch events
- Inform Insider Threat Program of possible expanding threats
- Partnerships
  - Develop high assurance of digital identity based upon common, enforceable standards
  - Share with Central Bank to help protect their infrastructure through bilateral agreements in place but could be geography challenging
  - Backstop and assist stand-alone countries and organizations to increase and mature their processes (e.g., A bunker backup when disaster strikes)
  - Work with FCC or other government bodies to regulate new satellites could increase or decrease requirements of new satellite constellations
  - Establish liaison with Space Command and Space-ISAC
  - Coordination with G7/G20

FIN/COM CI Threat Future

Becoming the MVT

Actions to Be Taken (Detail)

Partnerships

- Work with U.S. Intelligence Community to access adversary plans and operations
- Establish public-private intelligence community partnerships
- Expand joint wargaming into possible and potential threats
- Plan and rehearse use of alternate/contingency communications methods
- Across markets understand Government stance for each nation's IoT security
    - Likely to have varying levels because of privatized or militarized
- Foster consumer and partner vested interest in maintaining security

Monitor Adversary Attack Rehearsals

- Insider threat rehearsals on organization network
- Watch for indicator of physical/digital hybrid hops

Partnerships (Geopolitical, Intelligence, Industrial)

- Monitor, research and identify early signs of the “attack behind the attack”[8]
- Expand information sharing
- Monitor and share information for insider recruitment by nation-states
- Expand and focus wargaming
    - System and partner responses
    - Public, business and civil response

Promote Resiliency Beyond the Network to a Resilience of Confidence and Trust

Educate and Harden the Edges of the Network and Ecosystem

- Harden and educate the edges
- Encourage consumer to take every precaution to protect their own information while working global
- Create a social media method to encourage reporting of system interruption
- Build security into software and hardware (phone, computer, yet-to-be-developed human interfaces) that consumers and companies can rely on

[8] Mastercard 2020 Threatcasting Report.

FIN/COM CI Threat Future

The Rise of Hybrid Attacks (Physical/Digital)

Actions to Be Taken (Detail)

- Exploring the “physical” threat even if it’s in space (a long way away)
- As the industry moves to digital/virtual solution, it is important to remember that we still live in a physical world
- Today the industry has a proven track record for securing the physical world (e.g., facilities, cable). This was evident in multiple SME interviews where many dismissed many physical future threats (e.g., cable cut).
- The organization is currently working to help partners and smaller portions of the ecosystem to harden their digital security. In the future, as the larger players in the industry move away from physical security to digital solutions (e.g., cloud), extra measures should be taken to make sure that the “edge physical” and small players are hardened.

FIN/COM CI Threat Future

Insider Threat

Actions to Be Taken (Detail)

- Organizational Inside Threat Program
- Collect best practices from other industries and organizations (e.g., DoD)
- Widen and conduct industry sharing on insider threats and activities
- Government partnership to monitor and research nation-state insider threat activity

Next Steps

Socialize

Monitor

Partner

Advocate

Internal Actions

Further Research