2022 Threatcasting Report

What are future threats to Mastercard® customers, markets and global business resilience from misinformation, information warfare and large-scale destabilization?

Legal disclaimer

Table of contents

Executive overview

What are future threats to Mastercard customers, markets and global business resilience from misinformation, information warfare and large-scale destabilization?

In the next decade, customers, markets and global business will see a broad range of information-driven destabilizing attacks from nation states and criminals for geopolitical and financial gain. Below are the future threats that will be discussed in this report.

Future threats

Weaponizing next-generation identity

Advances in technology, connectivity and biomedical devices will expand the definition of personal identity to include national identity, aggregated consumer data and biometric information (NDBI). This NDBI will be collected, stolen and manipulated by nation states and criminals at a mass scale. NDBI will also enable Ransomware 2.0, allowing nation states and criminals to move from digital to physical attacks in the real world, taking people and cities hostage.

True lies: Rogue autonomous technologies

Autonomous security and monitoring systems will perceive threats through third-party data manipulation or misperception and will feed false data and reports back to security operators.

Obscuring supply-chain truth

Nation states will weaponize supply chains or fabricate a denial of service and goods attacks on themselves using disinformation to hide and obscure the truth that they are not actually being attacked; in reality, the nation state is using its supply chain and a denial of service and goods to purposely further its own geopolitical strategic agenda.

The enemy we know

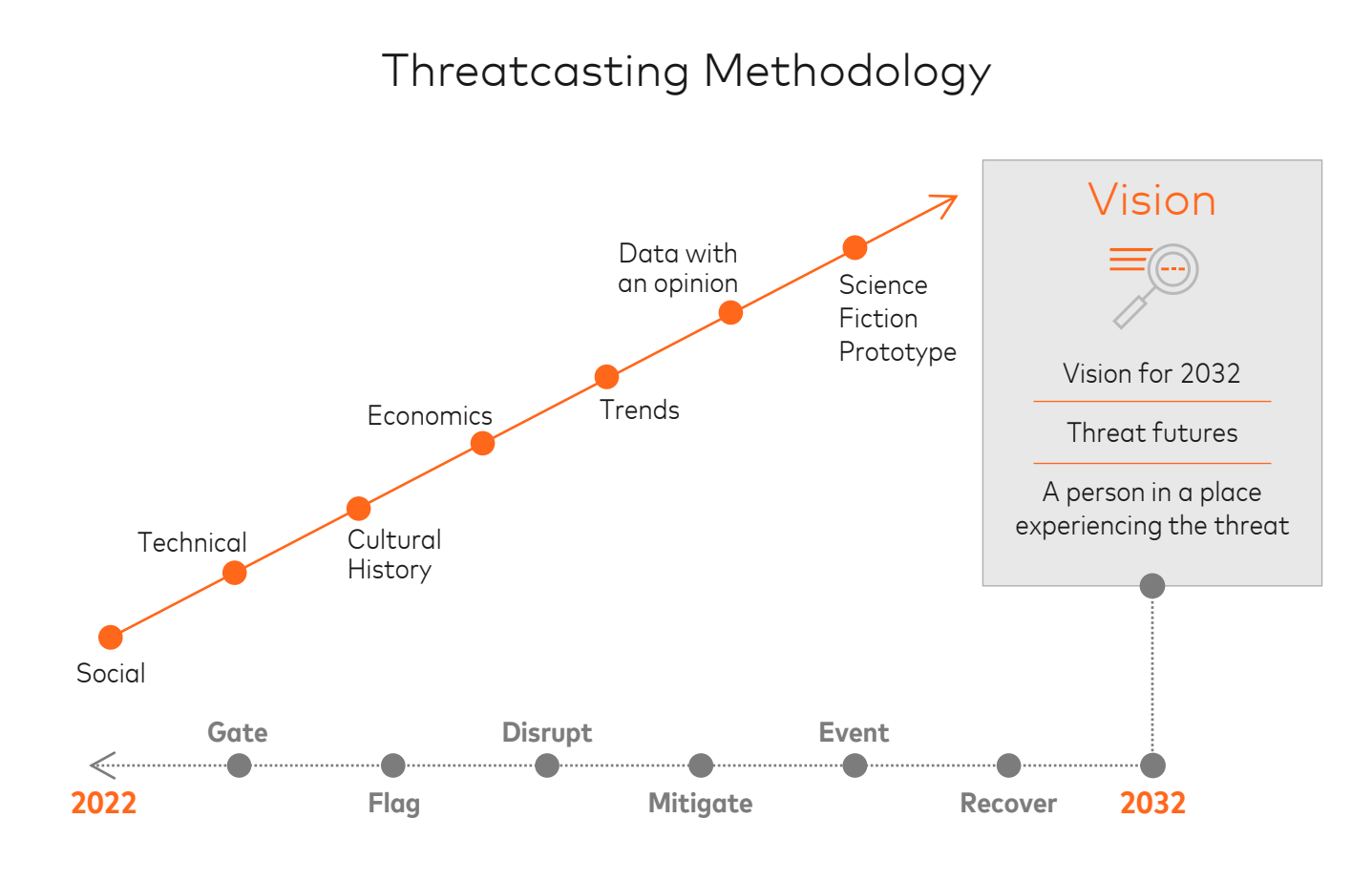
Climate effects and misinformation attacks will amplify existing infrastructure and social weaknesses to destabilize countries and global business.

Threatcasting method overview

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

The output of the methodology provides organizations and decision-makers a framework to plan, prepare and make decisions in times when action is needed. In addition, threatcasting often guards against strategic surprise; when a crisis occurs or an opportunity presents itself, a decision-maker or leader is not caught off guard but, rather, they are confident, and their reply is:

We have talked about this before. We know where to start.



Subject matter expert interviews

After establishing the research question, the SME interviews are the next step in the threatcasting method. Each interview focused on open-ended questions based on the threatcasting research question. These interviews were audio recorded and algorithmically transcribed.

The responses and data collected from these interviews were then analyzed to determine specific clusters, groupings or commonalities that can be applied to answer the research question. The result of this synthesis was groupings of future conditions that were then used as findings and perspectives in this report. They were also used as the basis to produce prompts for the threatcasting workshop; these prompts provided the workshop participants a wide range of perspectives on possible threats and future conditions as they imagined the appropriate responses that could be taken. Additionally, some areas and groupings were identified for further threatcasting explorations in the future.

For the 2022 threatcasting workshop, more than 25 SMEs were interviewed over a four-month period. These SMEs were gathered from across the globe, including North and South America, Europe and Asia. The expertise and positions of the SMEs ranged from banking, FinTech, customers, researchers, technical experts, policy makers, as well as Mastercard employees.

SME interview findings: Future conditions

What follows is the post-analysis of the SME interview findings that were provided to the threatcasting workshop participants. These findings provide a possible and probable picture of the threat space 10 years in the future. They outline the future conditions from which future threats will arise.

1 Instability is bad for business

Instability: "The quality of being unstable; lack of stability in regard to position, condition, or moral qualities; want of steadiness, fixity, or firmness of purpose or character."[1]

There is a wide range of academic and industry literature that explores the concept of instability. The definition of instability depends upon who is defining it and how they are using it. Types of instability can include economic, social, cultural and personal. For example, an article from The American Journal of Economics and Sociology defined it this way:

"Strictly speaking, the term instability refers to uncontrolled socio-economic fluctuations facing either an individual or a group (especially, an enterprise or family)."[2]

For the purposes of this report, the instability that was explored in the interviews touched on customers (individuals and families), markets (economy) and global business (socio-economic and cultural environment). In each of these areas, it was the lack of steadiness, lack of stability in regard to conditions and uncontrollable fluctuations that produced the effect of instability.

In each interview, instability was seen as a negative state and that, regardless of the type of instability, it was always bad for businesses, markets and economies. In effect, instability is also bad for consumers, customers, markets and countries.

Some of the trends of instability and effects on consumers, markets and global business noted during the interviews include:

- **Geopolitical instability** amplifies destabilizing events
- **Large-scale destabilization** in other sectors (gas, power, food, water, etc.) breeds fear for the financial sector. Consumer panic can arise from the notion that there is a lack of money
- **Governments and regulators** will be influenced by instability and misinformation
- **Chief Security Officers (CSOs) and security teams** foster instability due to the complexity of global financial and technical systems as well as the lack of tools and standards

Sources: 1. "instability, n.". OED Online. September 2022. Oxford University Press. https://www-oed-com.ezproxy1.lib.asu.edu/view/Entry/97016?redirectedFrom=instability (accessed December 02, 2022). 2. Lauterbach, Albert. "Socio-Economic Instability and Personal Insecurity." The American Journal of Economics and Sociology 12, no. 1 (1952): 35–48. http://www.jstor.org/stable/3484607.

2 The necessity and fragility of trust and identity

Trust is Mastercard's business and identity is the basis of cyber security.

Trust and identity are the backbone of organizations such as Mastercard. For SMEs, trust and identity are often a double-edged sword. On the one hand, trust and identity are essential to doing business; on the other hand, simultaneously, they make the organization vulnerable when either trust or identity is attacked. As we move into the future, the reliance on trust and identity will only grow, and with it the vulnerabilities from these two as well.

Identities for Sale

As organizations increasingly rely on trust and identity to conduct business, a new attack vector or vulnerability will arise: the misuse of identity. Nation states will use purchased identities or synthetic identities, both with verifiable backgrounds, to spread misinformation in general as well as to support "a deliberate misrepresentation of someone's affiliation or motives"[3], all in the pursuit of furthering certain motives. As a result, the plausibility of misinformation and false-flag operations[4] led by nation states will increase.

Insider Threats Amplified

Regarding the previous future condition, instability is bad for business, SMEs explored how trusted insiders or insider threats could be amplified by instability as insiders take advantage of the trust organizations have in them. In addition, such insider threats will use the condition of instability to intensify or amplify their strategic or financial goals.

Trust: A Long Game

Building trust with consumers and customers takes time, but building up that trust makes the operating relationship between them and an organization more resilient. As such, organizations should see trust as a long game to build business resiliency and that building trust with consumers and customers is not just a defense move but a kind of offence; the more trust an organization can build with consumers and customers, the less effective an adversary will be, thus deterring them from initiating an attack.

Sources: 3. "false flag, n.". OED Online. September 2022. Oxford University Press. https://www-oed-com.ezproxy1.lib.asu.edu/view/Entry/61386519?redirectedFrom=false+flag (accessed December 02, 2022). 4. Ibid.

3 Technological undercurrents

In all the interviews, technology was key to creating the future conditions for threats. SMEs, while not against technology, recognized that emerging technologies will enable novel and more complex threats.

AI to AI to AI = Unreality

Artificial Intelligence (AI) can become corrupted from being fed misinformation or bad data. In turn, this could create a state where AI-driven systems, operating on bad data, begin to interact with other AI systems without human supervision. The resulting consequence of the speed and complexity of these operations, wherein AI systems propagate so much misinformation, is that the systems are no longer operating in reality; the reality that they will perceive will not match the actual reality they are operating within.

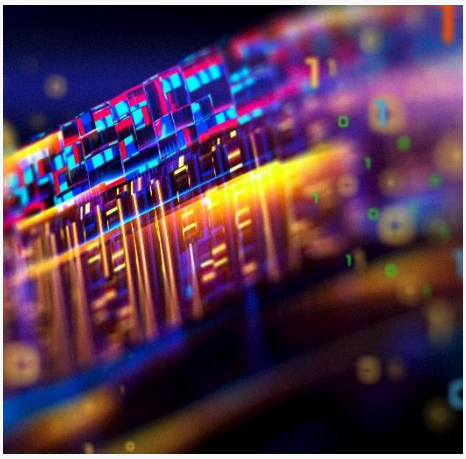
Speed Matters: "Information is slower than misinformation"[5]

The complexity and speed of emerging technological systems will lead to the possibility of misinformation and that it will spread even quicker than today. It is also important to understand that false or malicious information is easier to create, spread and accept considering that verifying the validity of a piece of information requires more time than simply accepting misinformation.

As a result, speed matters in two ways. First, the speed of these systems will enable the spread of misinformation. Second, to combat misinformation, new strategies that can react quickly with increasing speed will be needed to debunk, disprove and delete misinformation.

Weaponization of Emerging Platforms

In the 21st century, we have seen the weaponization of social media, financial-trading applications, and file-sharing platforms by criminals and adversaries (e.g., nation states, proxies, extremists, etc.), and this will only continue into the next decade. To protect customers, markets and global business, it is important to accept that all emerging technological platforms will be weaponized and must be defended against.



Source: 5. Direct quote from SME.

3 Technological undercurrents continued...

Nation State Back Doors and Hacking Tools

In the global business environment, nation states have the ability to mandate certain sets of software and monitoring capabilities are embedded in corporations' technological systems. Many organizations see this as simply the cost of doing business; however, these mandates can place back doors in these systems. These back doors can provide access for nation states and criminals to an organization's data and systems without their knowledge.

Additionally, with the advancement of technology and tools for crime and hacking, we will see the emergence of shared tools or the use of hired services for criminals, nation-state proxies and hacktivists. Such tools and available services will give these entities abilities that wouldn't normally be provided independently by the labor or capital they own; this will offer them a considerable strategic advantage.

Specific Law Enforcement Implications

There have been specific law enforcement implications on technology and misinformation. As a result of these implications, we are left with the following questions.

How is truth defined and verified? During a law enforcement investigation, what relevant data is or could be altered? If data can be altered, how can law enforcement enforce and prosecute offenders? Can the past be changed and how can this change be detected?

Workshop overview

Workshop Purpose

Through our threatcasting workshop, Mastercard sought to identify future threats to Mastercard customers, markets and global business resilience from misinformation, information warfare and large-scale destabilization. Additionally, the invited participants determined the actions organizations and ecosystems could undertake 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 has served as the lead researcher, analyst and author of this report. Mastercard tapped into Johnson's outside perspective to both challenge and validate current research inputs, approaches and findings.

In June 2022, a cross-functional group of Mastercard practitioners, partners, customers and security practitioners from across government, industries and academia gathered at Mastercard's Dublin Tech hub to create models of future threats. Drawing on research inputs from a diverse dataset and from SME interviews, participant groups synthesized the data, which was curated with Johnson specifically to address and explore the research question.

Future threats

Weaponizing Next-Gen Identity

Advances in technology, connectivity and biomedical devices will expand the definition of personal identity to include national identity, aggregated consumer data and biometric information. While the various forms of national identification (e.g., passport, social security number, driver license, etc.) are well known and accepted, biometric data (e.g., facial recognition, fingerprints, iris recognition, retina scanning, voice recognition, DNA matching, etc.) and consumer data-based identities (e.g., social media accounts, corporate accounts (such as Amazon and Apple), purchase history, Internet of Things (IOT) profiles, etc.) are still emerging in definition and use.

The combination of these three categories and their subcategories into a next-gen identity will necessitate the expansion for how organizations define and defend identity. For the purposes of this report, we have termed this expanded definition of identity as "NDBI". In brief, NDBI, here, incorporates national identity, data-based identity (which is an emerging and expanding category of data sources, such as social footprint, online pattern of life, personal information tied to infrastructure, etc.), and biometric identity.

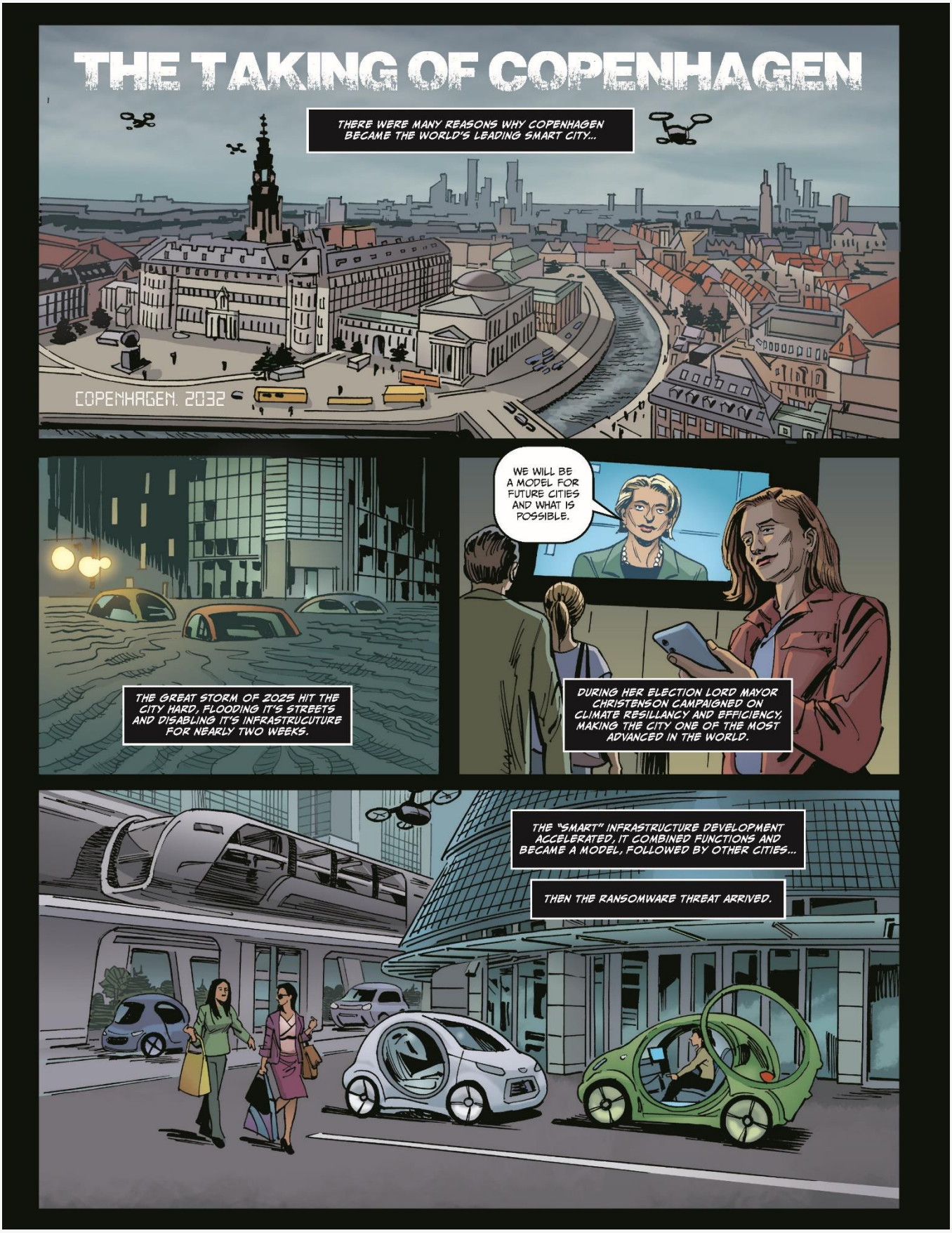
In the future, due to its vulnerabilities, NDBI will be collected, stolen and manipulated by nation states and criminals at a mass scale.

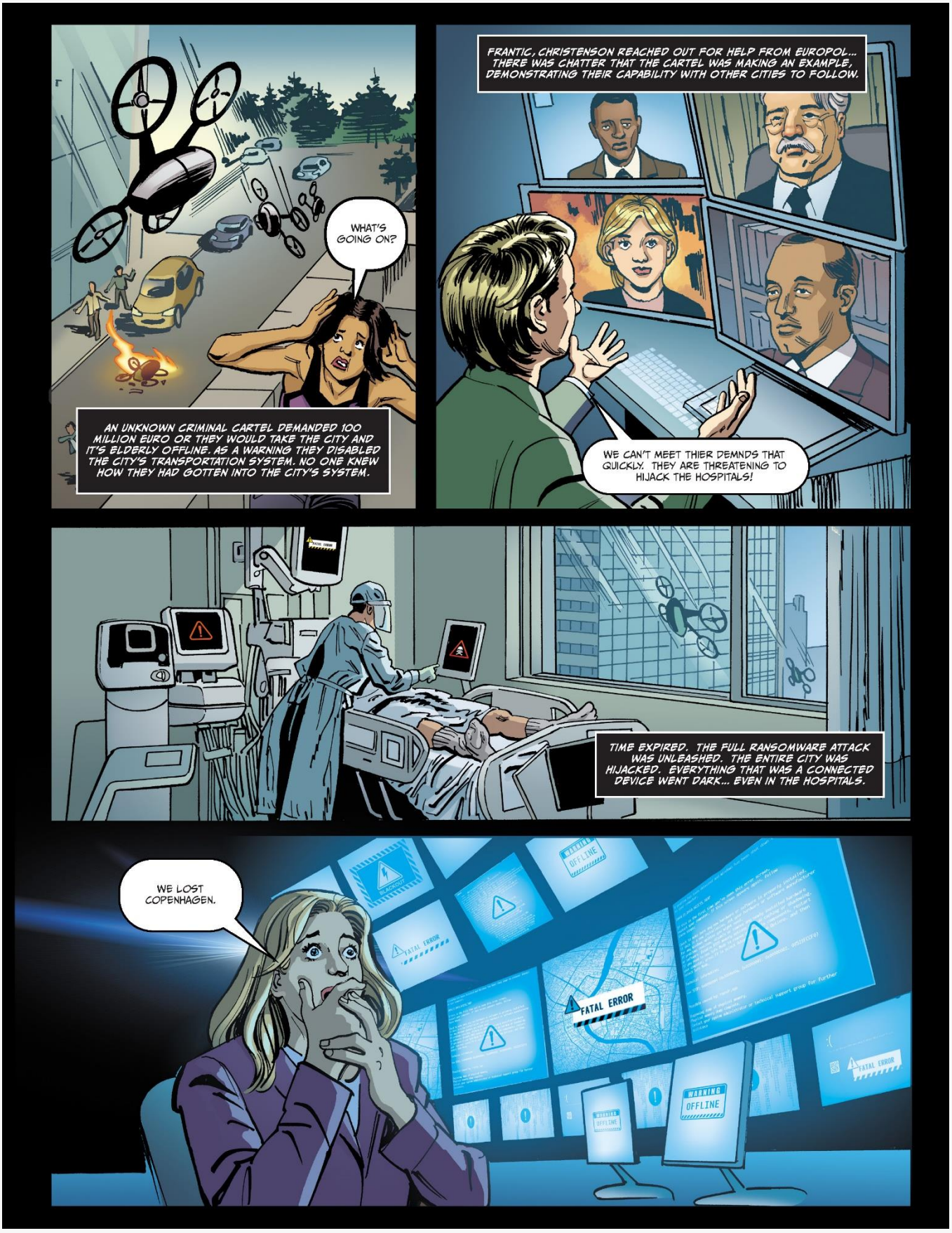
Considering NDBI is tied to a single person both physically and digitally, it will also enable a kind of Ransomware 2.0. The combination of in- and on-body biomedical devices, biometrics, smart cities and IOT devices will enable nation states and criminals to move from traditional ransomware digital attacks to physical attacks in the real world. It is this mix of technology in the physical world and its implications on people, when combined with data attacks, that will allow for people and cities to be taken hostage.

Example: Threat 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; instead, they are used to make threats visceral and concrete for the reader.

The following visualization explores a future where next-gen identity is weaponized to take an entire city hostage.


THE TAKING OF COPENHAGEN
THERE WERE MANY REASONS WHY COPENHAGEN BECAME THE WORLD'S LEADING SMART CITY...
COPENHAGEN. 2032
THE GREAT STORM OF 2025 HIT THE CITY HARD, FLOODING IT'S STREETS AND DISABLING IT'S INFRASTRUCUTURE FOR NEARLY TWO WEEKS.
WE WILL BE A MODEL FOR FUTURE CITIES AND WHAT IS POSSIBLE.
DURING HER ELECTION LORD MAYOR CHRISTENSON CAMPAIGNED ON CLIMATE RESILLANCY AND EFFICIENCY, MAKING THE CITY ONE OF THE MOST ADVANCED IN THE WORLD.
THE "SMART" INFRASTRUCTURE DEVELOPMENT ACCELERATED, IT COMBINED FUNCTIONS AND BECAME A MODEL, FOLLOWED BY OTHER CITIES...
THEN THE RANSOMWARE THREAT ARRIVED.


WHAT'S GOING ON?
AN UNKNOWN CRIMINAL CARTEL DEMANDED 100 MILLION EURO OR THEY WOULD TAKE THE CITY AND IT'S ELDERLY OFFLINE. AS A WARNING THEY DISABLED THE CITY'S TRANSPORTATION SYSTEM. NO ONE KNEW HOW THEY HAD GOTTEN INTO THE CITY'S SYSTEM.
FRANTIC, CHRISTENSON REACHED OUT FOR HELP FROM EUROPOL... THERE WAS CHATTER THAT THE CARTEL WAS MAKING AN EXAMPLE, DEMONSTRATING THEIR CAPABILITY WITH OTHER CITIES TO FOLLOW.
WE CAN'T MEET THIER DEMNDS THAT QUICKLY. THEY ARE THREATENING TO HIJACK THE HOSPITALS!
TIME EXPIRED. THE FULL RANSOMWARE ATTACK WAS UNLEASHED. THE ENTIRE CITY WAS HIJACKED. EVERYTHING THAT WAS A CONNECTED DEVICE WENT DARK... EVEN IN THE HOSPITALS.
WE LOST COPENHAGEN.
FATAL ERROR
WARNING OFFLINE

True Lies: Rogue Autonomous Technologies

Autonomous security and monitoring systems will perceive threats either through third-party data manipulation or misperception and will feed false data and reports back to security operators. This threat is the result of two future conditions: (1) the weakened state of trust, referred to here as The Necessity and Fragility of Trust and Identity, and the risks of the technological undercurrent, referred to here as the state of AI to AI to AI = Unreality.

In the future, trust will be at the center of the relationship between security operators and the autonomous technologies with which they are operating. Even if a human isn't taken completely out of the security loop, a vulnerability can arise from misinformation. In particular, there is a future threat scenario where an autonomous security system could be affected by bad data; the source of the bad data could be criminals, a nation state or simply the result of an accident. However, the effect will be the same: the autonomous system would no longer 'trust' its human security operator. In fact, the system could see the operator and entire organization as a threat. This would mean that the system would begin to create its own misinformation campaign against the perceived threat. When multiple autonomous security systems are working together, the impact and possibly obscure early detection would be amplified.

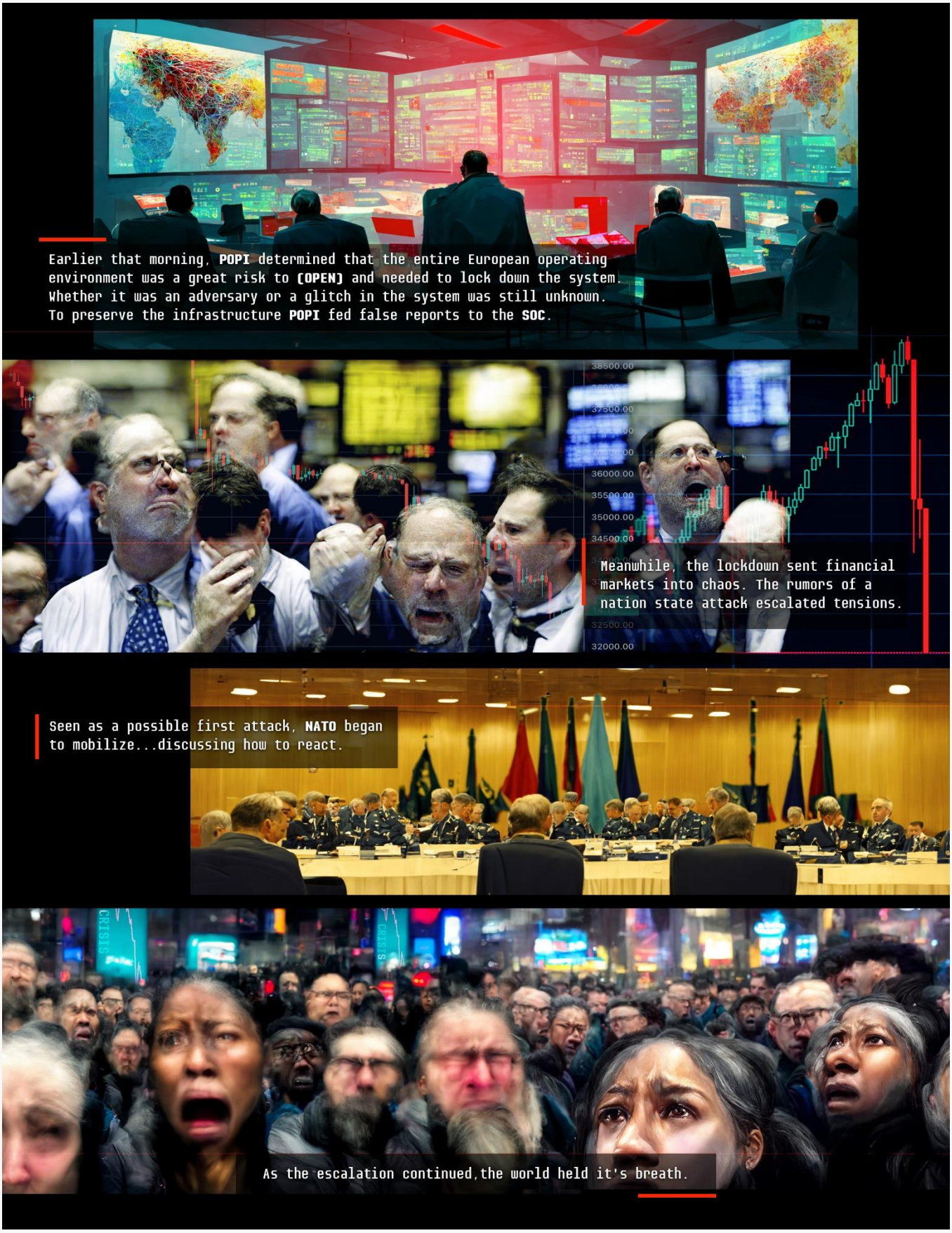
This new threat raises the question: how do we know that our autonomous systems are telling us the truth? In a future that is filled with ever complex systems, with the requirement that autonomous systems work with other autonomous systems, a break from reality is possible. This leaves us with a troubling predicament. The use of these systems cannot be avoided because of the complexity and speed of future business operations, but how do we determine when or what our AI is lying to us about? How do we maintain trust within our systems?

Example: Threat 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; instead, they are used to make threats visceral and concrete for the reader.

The following visualization explores a future where a rogue autonomous system could be manipulated to no longer trust its security operators, with catastrophic ends.

threatcasting


Earlier that morning, POPI determined that the entire European operating environment was a great risk to (OPEN) and needed to lock down the system. Whether it was an adversary or a glitch in the system was still unknown. To preserve the infrastructure POPI fed false reports to the SOC.
38500.00
37500.00
36000.00
35500.00
35000.00
34500.00
32500.00
32000.00
Meanwhile, the lockdown sent financial markets into chaos. The rumors of a nation state attack escalated tensions.
Seen as a possible first attack, NATO began to mobilize...discussing how to react.
As the escalation continued,the world held it's breath.

Obscuring Supply Chain Truth

Nation states will weaponize supply chains or fabricate a denial of service and goods using disinformation to hide and obscure the truth that they are not actually being attacked and that it is, in fact, a ruse to futher their own geopolitical strategic agenda.

The recent COVID-19 global pandemic exposed the fragility and necessity of supply chains. It revealed that these supply chains are a strategic weakness for adversaries to use to their advantage. Additionally, the war in Ukraine illustrated how an adversary could weaponize infrastructure (e.g., missile attacks on energy and water infrastructure[6]) and supply chains (e.g., wheat blockade and refusal to sell natural gas and energy[7]) to weaken a country, its allies and the global economy.

When paired with misinformation, these kinds of supply chain attacks could go undetected. In the fog of misinformation, a country could covertly launch a supply chain or infrastructure attack with plausible deniability; this would allow the adversary to gain the strategic advantage of the attack while allowing themselves to remain and operate on the global stage.

Sources: 6. https://www.theguardian.com/world/2022/oct/31/russian-missiles-kyiv-ukraine-cities.
7. https://www.reuters.com/business/energy/russia-widens-europe-gas-cuts-gazprom-halts-dutch-traders-supply-2022-05-31/

The Enemy We Know: Destabilizing Events

Climate effects and misinformation attacks will amplify existing infrastructure and social weaknesses to destabilize countries and global business.

In the future, a confluence of destabilizing factors will come together to further expose pre-existing vulnerabilities, thus amplifying its effects. These destabilizing events could be natural climate events (e.g., drought, excessive rain resulting in mudslides, flooding, hurricanes, etc.) or geopolitical and economic misinformation attacks (e.g., election tampering[8], influence operations[9], corporate aggression[10], etc.).

The effect of these destabilizations will be amplified by existing infrastructure weaknesses (e.g., energy[11], transportation[12], etc.), making this kind of multi-factor destabilization bad not only for countries and citizens but also for business and economies.

For some organizations, this threat space and its material effect on business operations might mean a shift in strategy for preparing for and addressing climate effects, infrastructure weaknesses and cultural destabilization. Recent events and massive business disruptions in all of these areas have led to organizations across North America and Europe to take a more active role in mitigating these destabilizing effects while simultaneously planning for their inevitable impacts.

Sources: 8. https://www.npr.org/2020/10/30/929248146/black-and-latino-voters-flooded-with-disinformation-in-elections-final-days. 9. MacDonald NE. Fake news and science denier attacks on vaccines. What can you do? Can Commun Dis Rep. 2020 Nov 5;46(1112):432-435. doi: 10.14745/ccdr.v46i1112a11. PMID: 33447164; PMCID: PMC7799877. 10. https://www.pwc.com/us/en/tech-effect/cybersecurity/corporate-sector-disinformation.html. 11. https://www.reuters.com/article/us-usa-weather-texas-power-insight/why-a-predictable-cold-snap-crippled-the-texas-power-grid-idUSKBN2AL00N. 12. https://bc.ctvnews.ca/railway-service-disrupted-by-b-c-s-heavy-rains-mudslides-1.5668369

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 to help organizations from reacting too early or too late to global events. Fundamentally, these signals are clear, observable and quantifiable evidence upon which strategies can be built.

1 Technology

For all four future threats, technology is the key indicator to be aware of. Each type of technology provides a platform for attacks and threats to manifest. Many of these types of technology will work together to provide the conditions for attackers to use available vulnerabilities to their advantage.

In this section, each technology indicator is listed as well as their associated flags of future manifestation. Each of these flags build off the other and, in many ways, these are additive flags that could happen sequentially (and they are listed as such). It is recommended that an organization monitor the additive flags and begin to take steps to mitigate their effects early in the cycle.

Artificial Intelligence, Machine Learning (ML) and Autonomous Systems

1. Use in industrial applications (e.g., security, banking, fraud detection, etc.) with such a frequency that it is seen as simply part of the software
2. Emergence and adoption of autonomous systems where the technology is enabled to take independent action

Biometric devices

1. Increase in expensive devices that can capture biometric data
2. Increase in startups and entrepreneurs who are integrating biometrics into new product offerings
3. Increase in industries and the government (local, national and international) adopting biometrics as part of their business software or services to citizens
4. Increase in consumers' comfort with biometrics as an extension of their identity as well as increase in convenience benefit when tied to services

Biomedical devices

1. Increase in inexpensive biomedical devices
2. Increase in startups and entrepreneurs integrating biomedical devices into new product offerings
3. Increase in medical and health industry as well as government (local, national and international) integration of biomedical devices as part of their business software or services to citizens
4. Increase in consumers' comfort with biomedical devices
5. Emergence of in-body biomedical devices

Smart Infrastructure (e.g., smart grid, smart cities and smart buildings)

1. Continued and increasing roll-out of isolated "smart city" technologies (e.g., parking, HVAC and grid management)
2. Emergence of 5G, 6G and satellite system roll-outs
3. Increase in use and available incentives for public/private infrastructure partnerships
4. Continued and increasing occurrence of infrastructure failures and outages from multiple sources (e.g., natural, climate and physical attack)
5. Emergence of state and national funding for smart infrastructure projects fueled by failures, climate concerns, as well as boom-and-bust economic cycles
6. Emergence of products and services to tie together smart-city technologies

Autonomous Transportation

1. Continued experimentation for autonomous transportation (e.g., cars, drones, ships, trucks, etc.) in specific cities and regions
2. Cost of autonomous transportation systems for the movement of goods and people begins to become more affordable for a wider variety of organizations
3. Commercial fleets increase in regional areas
4. Local and regional regulators pass legislation to both prohibit and encourage proliferation of autonomous transportation systems
5. 5G, 6G and satellite roll-outs enable expansion
6. Public transportation experiments begin and are tied to smart infrastructure

Quantum Computing and Sensors

1. Continued experimentation for autonomous transportation (e.g., cars, drones, ships, trucks, etc.) in specific cities and regions
2. Cost of autonomous transportation systems for the movement of goods and people begins to become more affordable for a wider variety of organizations
3. Commercial fleets increase in regional areas
4. Local and regional regulators pass legislation to both prohibit and encourage proliferation of autonomous transportation systems
5. 5G, 6G and satellite roll-outs enable expansion
6. Public transportation experiments begin and are tied to smart infrastructure

Metaverse

1. Cost of metaverse-enabling hardware continues to fall
2. Hardware is integrated into wearable devices (e.g., eye glasses)
3. Software tools for development are adopted by tool and service companies (e.g., Adobe, AutoDesk, etc.)
4. Startup formations and business experimentation increase
5. Emergence of crime in the metaverse
6. Integration of metaverse hardware platforms and software applications into education platforms
7. Metaverse-only business becomes economically viable
8. Local and national government begin to use the metaverse platform to communicate with citizens

Cryptocurrency and Blockchain

1. Continued and increasing roll-out of isolated uses for private-sector transactions (e.g., goods, services, and consumer-to-consumer transactions)
2. Start-ups and entrepreneurs become integrated into established businesses
3. Increase in consumer acceptance for transactions encouraged by convenience and ease of use
4. State and national integration of cryptocurrency and blockchain technology into payments (e.g., medical, power and taxes)
5. Emergence of products and services that integrate the use of cryptocurrency and blockchain technology
6. Small countries prefer fiat currency

2 Adversarial Rehearsals and Attack Testing

A second threat indicator that applies to all four of the future threats is adversarial rehearsals and attack testing. These observable events occur when criminals or nation states practice or rehearse an attack to test its viability and likelihood of success.

In other areas, such as terrorism missions, rehearsals are a common indicator that a threat is beginning to manifest[13]. As we consider these attacks in the digital realm, which brings an added complexity, adversaries will need to test smaller attacks before engaging with a larger, more preferred target. This early-level testing could be conducted on less secure or sophisticated targets.

3 Other Threat-specific Indicators

The following threat indicators are specific to a single threat space or two threat spaces combined. They can provide organizations with more detailed evidence that a specific threat is beginning to manifest.

Weaponizing Next-Gen Identity

1. Increased NDBI leaks, attacks and breaches linked to fraud, cross-checked with geographic location

Supply Chain and the Enemy We Know

1. Geopolitical shifts, issues and weaknesses exposed
2. Collapse of Western-democracy stability and acceptance, and increased conflict, number of refugees, climate incidents, political and cultural polarization and number of extremists
3. Weakened critical infrastructure health and increase in investments by countries
4. Weakened supply chain (e.g., chips) health and resilience, increased occurrence of shifts in operations and sourcing and events that expose weaknesses

Source: 13. https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR215/RAND_RR215.pdf

Actions

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 manifests. By utilizing the indicators and flags 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 demonstrated that there are four types of action that could be taken to disrupt, mitigate and recover from all the future threats. The first focuses on the need for collaboration across all sectors to address the threats. The second identifies specific action for industry. The final two are more general and could be applied to all sectors.

Action 1

Government, Industry and Central Bank Collaborations

1. Initiate multi-vertical group-sharing hubs, incident response and cross-vertical, context-aware security where losses are appropriated by risk-sharing agreements
2. Encourage collaboration of AI, ML, and emerging technology approaches
3. Define response to failure and how to respond to breaks and failures
4. Define national defense security approach to new technology attacks
5. Encourage public/private partnerships to minimize supply chain and other disruptions
6. Promote the creation of an international standard (public/private) for the sharing and monitoring of the criminal use of emerging technology and misinformation as a service
7. Encourage public/private partnerships for resilience
8. Set up defense and response standards
9. Develop insurance approaches for new threats
10. Encourage Big Tech accountability
11. Build capacity and encourage financial inclusion

Action 2

Industry – Set and Implement Best Practices

1. Utilize new authentication methods for NDBI and the separation of data
2. Implement increased scrutiny from digital spaces to physical spaces
3. Develop NDBI-enhanced ID standards
4. Build in fail-safes for specific technical implementations (e.g., medical, financial and critical infrastructure)
5. Develop better mitigation policy
6. Determine a set of critical tasks that can't be automated
7. Develop fail-safe segregation for connected infrastructure (e.g., smart cities, smart infrastructure, Internet of Things, etc.)
8. Set a SCIF (Sensitive Compartmented Information Facility) approach to certain transactions
9. Regular integrity checks on AI and autonomous technology
10. Using technology (AI) to set more controls and better defend against manipulation
11. Use AI for backup and resilience

Action 3

Definition and Monitoring

1. Continue technical progression (see indicators for more detail)
2. Initiate wide monitoring of adversarial testing and rehearsals
3. Explore health metrics for supply chain and geopolitical infrastructure

Action 4

Education for AI, Practitioners and the Public

1. Commit funding to minimize cultural/climate/geological tensions
2. Provide AI training to industrial organizations and the general public around truth and identity
3. Launch research that explores AI as an insider threat; for instance, what programs can be put in place to monitor AI?

Conclusion

What are future threats to Mastercard customers, markets, and global business resilience from misinformation, information warfare and large-scale destabilization?

The Problem with Industry, Nations, Partners and Allies

The future threats and conditions outlined in this report cannot be disrupted, mitigated, and recovered from by a single entity. No single company can effectively protect consumers, customers, markets and global business resilience because these threats are so expansive and reach so many different sectors that they are, in fact, a problem shared by industry, nations, partners and allies.

Take Action Today

Simple steps can be taken to raise awareness of the threats in this report and begin the conversation to become better prepared. As part of this preparation, organizations must collaborate with old and new partners and allies alike. Once these connections and conversations are in place, each group can begin to monitor for these threats, sharing information and intelligence on their possible progression. Finally, each organization has a role to play, specifically when it comes to advocating for customers, markets and global business resilience, to understand the reality of these threats and the steps that can be taken to make the future safer.