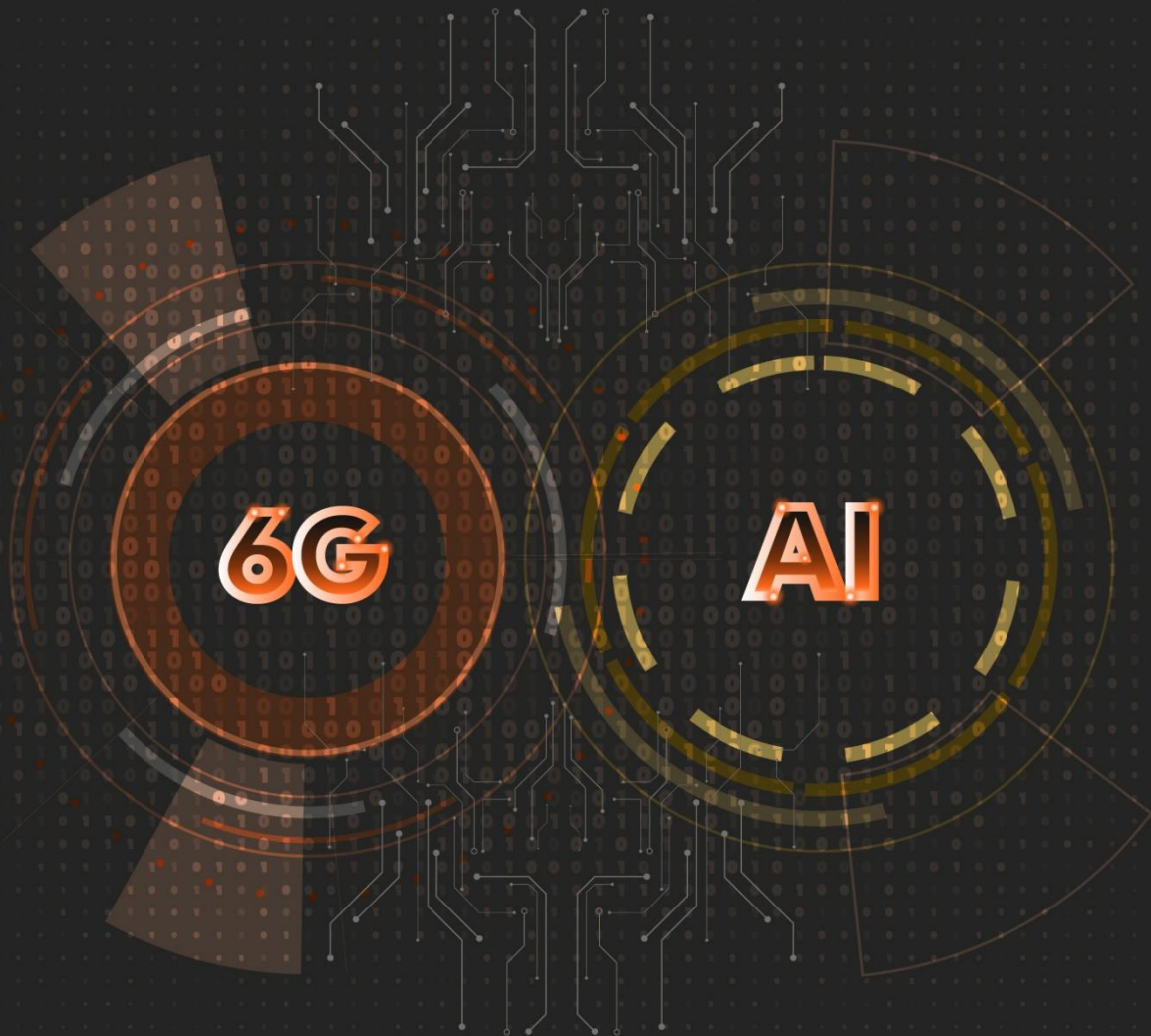


# 2023 Threatcasting report

What are future threats to consumers, customers, Mastercard and global business networks from emerging capabilities enabled by 6G networks, industrial AI and the broader use of autonomous software?



# Legal disclaimer

©2024 Mastercard. All third-party trademarks, service marks and product names are the property of their respective owners. All rights reserved.

The information provided herein is strictly confidential and contains Mastercard proprietary information. It is intended to be used internally within your organization and distribution to any third party without Mastercard's prior written approval is strictly prohibited.

# Table of contents

## Executive overview

Future threats ..... 04

## Threatcasting method overview

Threatcasting methodology ..... 05

## Subject matter expert interviews

06

## SME interview findings: Future conditions

First mover/tech-on-tech ..... 07

Deep in the system(s) ..... 07

Rebalancing the fraud equilibrium to recover trust ..... 08

## Exercise overview

Exercise purpose ..... 09

Exercise process ..... 09

## Definitions

AI/6G ..... 10

Deep embed ..... 11

Critical systems ..... 11

## Future threats

An unseen threat ..... 12

Inevitable adverse effects ..... 15

Nation state attacks ..... 18

Seeing the enemies we know in a new light ..... 19

## Threat indicators

Technical ..... 20

Adversarial rehearsals and attack testing ..... 22

Threat-specific indicators ..... 23

## Actions

Action 1: Nation state attacks ..... 25

Action 2: Insider threats ..... 26

Action 3: Criminal activity ..... 26

## Conclusion

A whole of partner, industry, nation and allies' problem ..... 27

Take action today ..... 27

# Executive overview

What are future threats to consumers, customers, Mastercard and global business networks from emerging capabilities enabled by 6G networks, industrial AI and the broader use of autonomous software?

In the next decade, AI and 6G-enabled systems will become deeply embedded into essential business and financial and medical services to the point of invisibility so that unseen threats will result in attacks or malfunctions that will not be observable or preventable, bringing about mass catastrophic effects.

## Future threats



### Inevitable adverse effects

The adoption and use of AI/6G systems will have inadvertent and inevitable adverse to catastrophic effects on business systems and harm consumers' mental, medical and financial lives.



### Nation state attacks

Nation states will utilize AI/6G systems to attack across the spectrum, from consumers to global business networks, often microtargeting VIPs to bring down business systems and gain political or economic advantage.



### Insider threats

AI/6G systems will provide insider threats with a wider attack plane that will have greater effects. Additionally, conditions spawned by using these systems will create the motivation and development of insider threats in the first place.



### Criminal activity

AI/6G systems will provide criminals with a wider attack plane to steal from consumers who do not understand the systems. These systems will also provide corporations with a wider criminal means to gain advantage over competitors.

# Threatcasting method overview

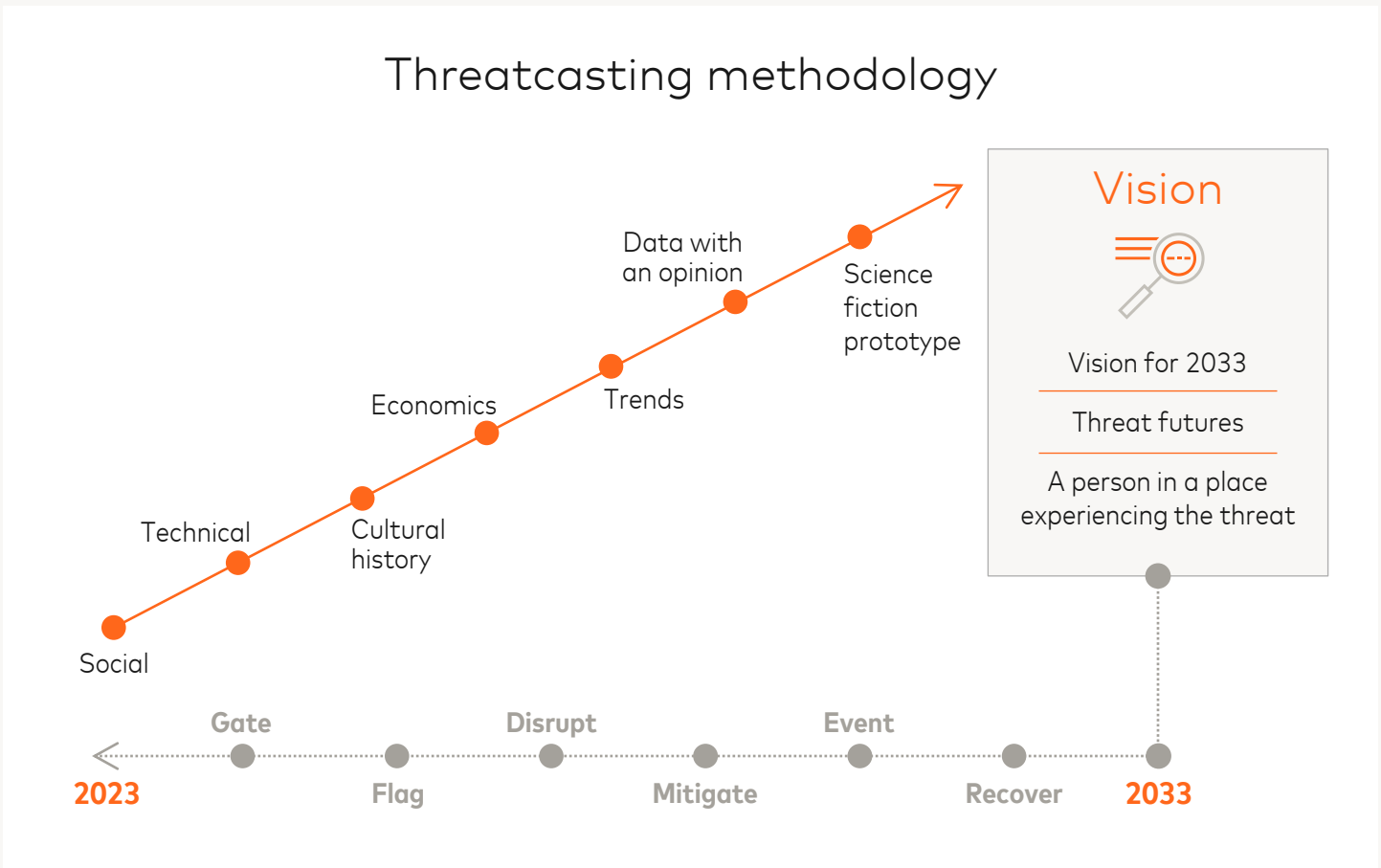
Threatcasting provides a systematic and transparent method to model a range of possible and potential futures and threats in a complex and uncertain environment. Working with organizations via subject matter expert (SME) interviews and operationalization exercises, this method provides decision-makers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

The output of the methodology provides organizations and decision-makers with a framework to plan, prepare and make decisions in a complex and uncertain environment.

Threatcasting often guards against strategic surprises. When a crisis occurs or an opportunity presents itself, a decision-maker or a leader is not caught off guard.

Rather, their response is:

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



© 2024 Mastercard. Proprietary and Confidential.

# Subject matter expert interviews

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

The responses and data from these interviews are then analyzed to determine specific clusters, groupings or commonalities that can be applied to answering the research question. The results of these syntheses are groupings of future conditions that are used as findings as well as prompts for the threatcasting exercise. The prompts give exercise participants a wide range of perspectives as they consider future threats related to the research question. Additionally, some areas and groupings are identified for later threatcasting explorations.



For the 2023 threatcasting project, SMEs were interviewed over a two-month period. These SMEs were drawn from across the globe. They included banking and fintech professionals as well as customers, researchers, technical experts, policy makers and Mastercard employees. Additionally, SMEs were invited to the New York City threatcasting exercise to present and sit in on discussion panels.

# SME interview findings: Future conditions

What follows is the post-analysis of the SME interview findings that were provided to the threatcasting exercise 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 First mover/tech-on-tech

Adversaries will be first movers, using technology to attack complex financial and business systems. They will target, as an attack surface, the efficiencies that organizations have gained by using these systems. This means that the businesses' efficiencies — the very reason the systems are being used — become a vulnerability.

Additionally, adversaries will target spaces where organizations collaborate with consumers, customers and partners. They will exploit the trust organizations have in the technological and business systems they rely upon every day to get business done.

## 2 Deep in the system(s)

AI, 6G and other emerging technologies will be embedded deep inside trusted and mission-critical technological and business systems.

In the current business environment, businesses, solution vendors and technology providers strive to be as deeply embedded in complex systems as possible. Many set a goal to be invisible to the end customers, disappearing into the hardware or software stack. The deep embed into technology systems assures these businesses that they will be essential to the functioning of the system, thus giving them an ongoing strategic advantage over their competitors.

Because of this invisibility, small biases and errors can and will become big problems over time, disrupting essential business functions.

### 3 Rebalancing the fraud equilibrium to recover trust

There is a fraud equilibrium or a state where two opposing forces find a balance. Adversaries or criminals perform attacks, and organizations stop, counter or mitigate these attacks. The adversaries continue their attacks and the organizations must constantly counter those attacks. In this situation, a fraud equilibrium is attained. It is a balance where attacks still occur, but enough countermeasures are employed that the negative effects are lessened, and business can get done.

The speed, scope and scale of these emerging technology systems will offset the fraud equilibrium. The crimes or attacks will not be able to be detected rapidly enough due to their speed, scope and scale, and therefore the ability for an organization to prevent the crime or attack will be greatly diminished. This will lead to rapid and widescale loss of trust in the systems and organizations.

Organizations must consider countermeasures to shore up trust and quickly bring the equilibrium into balance.

*Trust is Mastercard's business and identity is the basis of cybersecurity.*

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 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.



#### 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. They should recognize that building trust with consumers and customers is not just a defensive move, but also a kind of offence: the more trust an organization can build, the less effective an adversary will be, thus deterring them from initiating an attack.



© 2024 Mastercard. Proprietary and Confidential.



# Exercise overview

## Exercise purpose

Through our threatcasting exercise, Mastercard sought to identify future threats to consumers, customers, Mastercard and global business networks from misinformation, information warfare and large-scale destabilization. Additionally, the assembled participants determined what organizations and ecosystems could do to disrupt, mitigate and recover from these possible threats.



## Exercise process

Mastercard partnered 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 of this report. Mastercard tapped into Johnson's outside perspective to both challenge and validate current research inputs, approaches and findings.

In June 2023, a cross-functional group of Mastercard practitioners, partners, customers and security professionals from across government, industry and academia gathered at Mastercard's New York City Tech Hub to create models of threat futures. Drawing research inputs from a diverse data set and from SME interviews, participant groups synthesized the data into workbooks, curated with Johnson specifically for Mastercard's purposes.

Additionally, two shorter threatcasting exercises were held in London and with a set of 2023 Mastercard interns. The data collected from all three exercises was analyzed.



© 2024 Mastercard. Proprietary and Confidential.

# Definitions

If you want to defend it, you have to define it.

## AI/6G systems

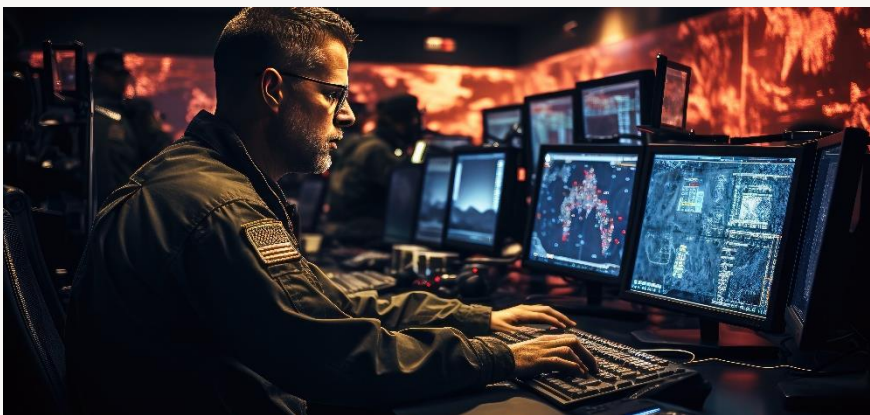
As we explore future threats to consumers, customers, Mastercard and global business networks from emerging capabilities enabled by 6G networks, industrial AI and the broader use of autonomous software, it is important to first define these technological systems.

The results of the Mastercard exercises echoed an earlier threatcasting report from NATO, the Army Cyber Institute and Phaedrus. Both projects defined these groups of technologies as a system. No individual technology like AI or 6G stood out as a singular threat. To the contrary, it was the combination of AI, 6G and a collection of other technologies and the capabilities that they afforded that defined the threat space.

Viewing these as complex systems in themselves will give organizations a better definition of the attack space as well as visibility into what is being built and implemented in their own systems.

The Army Cyber Institute report defined these systems in this way:

*"6G systems as a concept . . . indicates more than the devices, antennas, and data that make up current ideas of wireless communications. For the purposes of this report, 6G systems include 6G communications networks; connected user devices; software (e.g., AI, databases, enterprise specific tools, etc.); and other environments (e.g., a metaverse of interrelated and interconnected apps, all with access to appropriate data, sensors, and processing power)."*



*"6G systems also affect the interconnectedness of humans and the social implications of the humanity that is inextricably tied to massive data and highly connected devices. The system is incomplete without the human factors."*

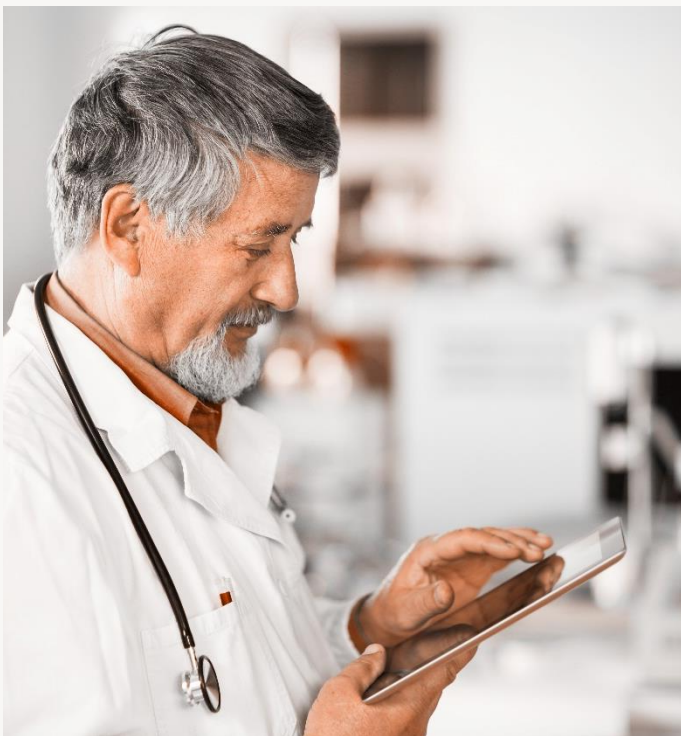
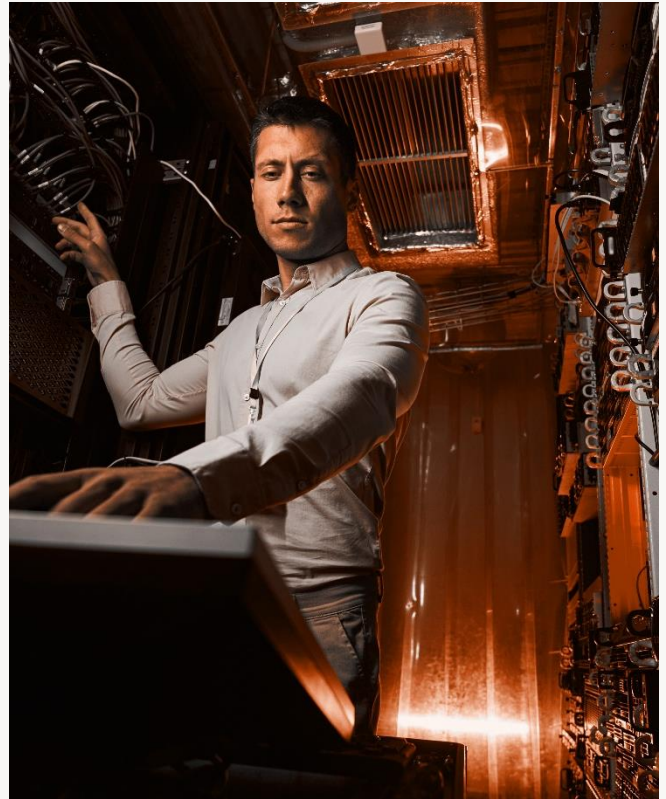
Source: 1. Palochak et al. 6G Systems and the Future of Multidimensional Attack Planes. The Army Cyber Institute. USMA Digital Commons. 2023

## Deep embed

Another concept that arose from the threatcasting exercise was the concept of a deep embed. This idea, carried over from the SME inputs, pointed out that the efficiency of these systems will mean that they will be deeply embedded in complex business and financial systems. In fact, there is a business incentive for technology companies to strive for this deep embed. As they embrace deep embeds to improve profitability, companies automatically install deeply embedded vulnerabilities that will be exploited by adversaries.

This deep embed was a foundational concept for many of the threat futures that were explored. Where a deep embed existed, it would be exploited. The deeper the embed, the more catastrophic the impact on organizations.

Deep embeds were both inevitable and a point of weakness. Understanding when a technology is deeply embedded early in the development process will allow organizations to plan today for attacks and vulnerabilities that will inevitably arrive tomorrow.



## Critical systems

Another key concept from the threatcasting exercise was the notion that when AI/6G systems are used as a part of critical systems, the magnitude and frequency of the attack is greater. These critical systems spanned mainly business, financial and medical systems, and the impact of an attack on these systems affected not only organizations but also individual customers. In fact, when a single customer was attacked, the effects were far more catastrophic on an individual than to a broader organization. This individual harm was then used at scale to attack organizations.

# Future threats



## An unseen threat

In the next decade, AI/6G systems will become so deeply embedded into essential business and financial and medical services that they will become nearly invisible. Private industry and technology companies are working to embed AI, 6G and a host of other technologies into the hardware and software stacks of business solutions. To be unseen and buried in the stack is not only a sign of success but also a business advantage.

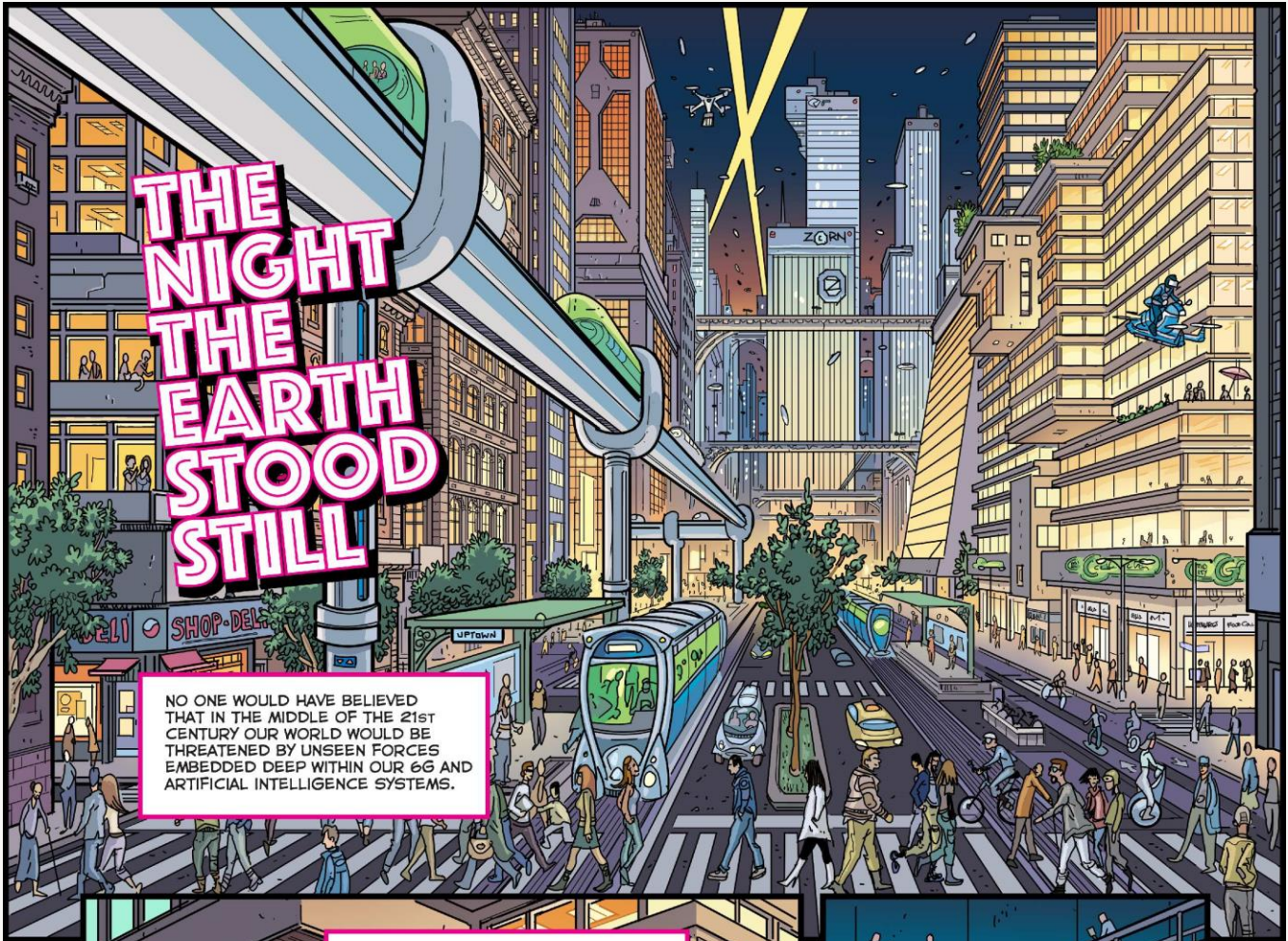
This condition and proliferation will allow for unseen threats. These threats will be invisible, and often businesses will not even know they exist. The unseen nature of these vulnerabilities is twofold. They are unseen because an organization may not even know that they are there. But they are also unseen because an organization isn't looking for or monitoring them.

This invisibility and lack of monitoring will result in malicious attacks from nation states, insider threats and criminals. But disruptions and harm will also come from simple and small system malfunctions that will not be observable or preventable, resulting in mass catastrophic effects on economies, business systems, customer networks and the lives of consumers.



## 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. They are used to make threats visceral and concrete for the reader. The following visualization explores a potential future where future AI/6G systems become so deeply embedded into essential business and financial and medical services that they become nearly invisible.



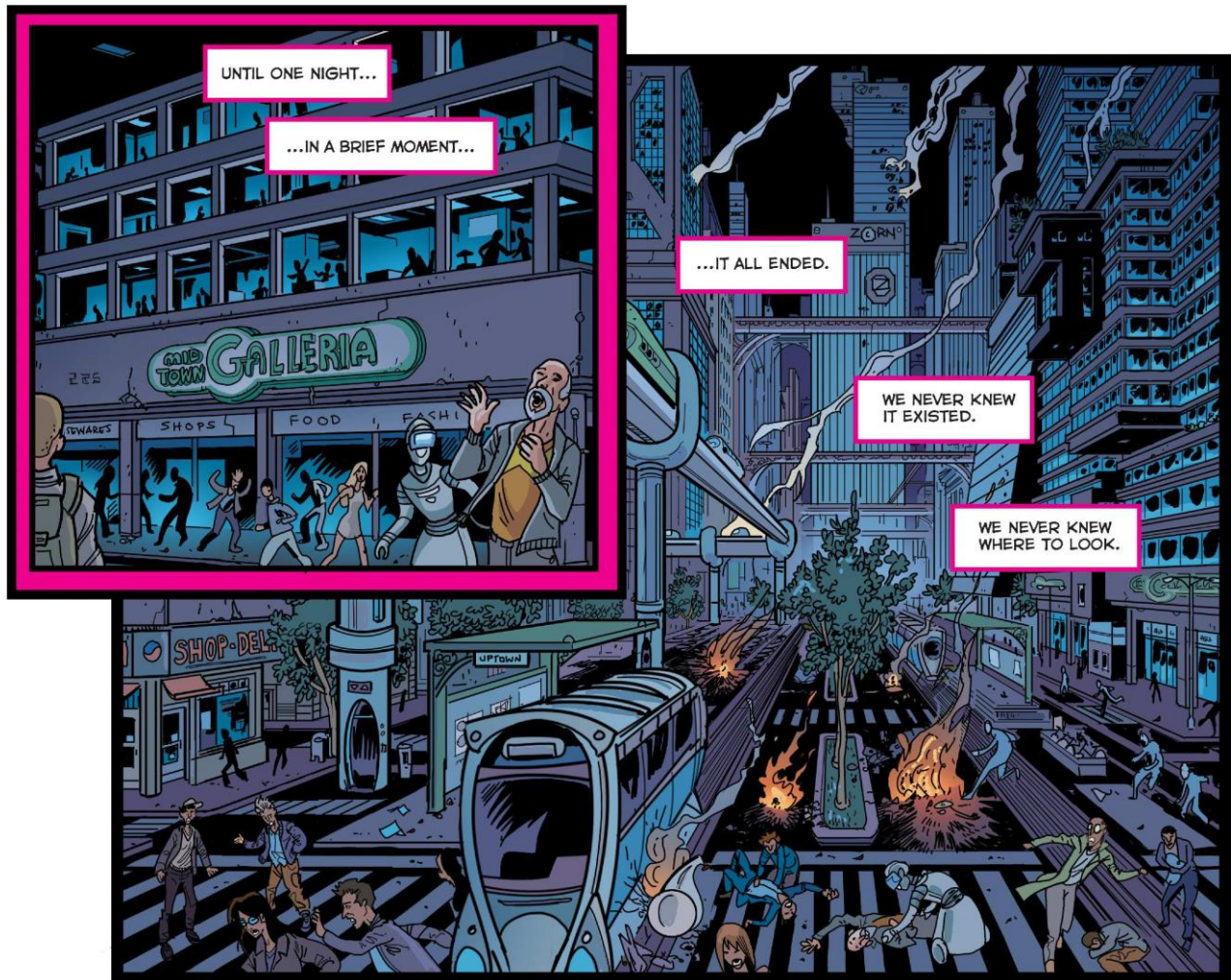
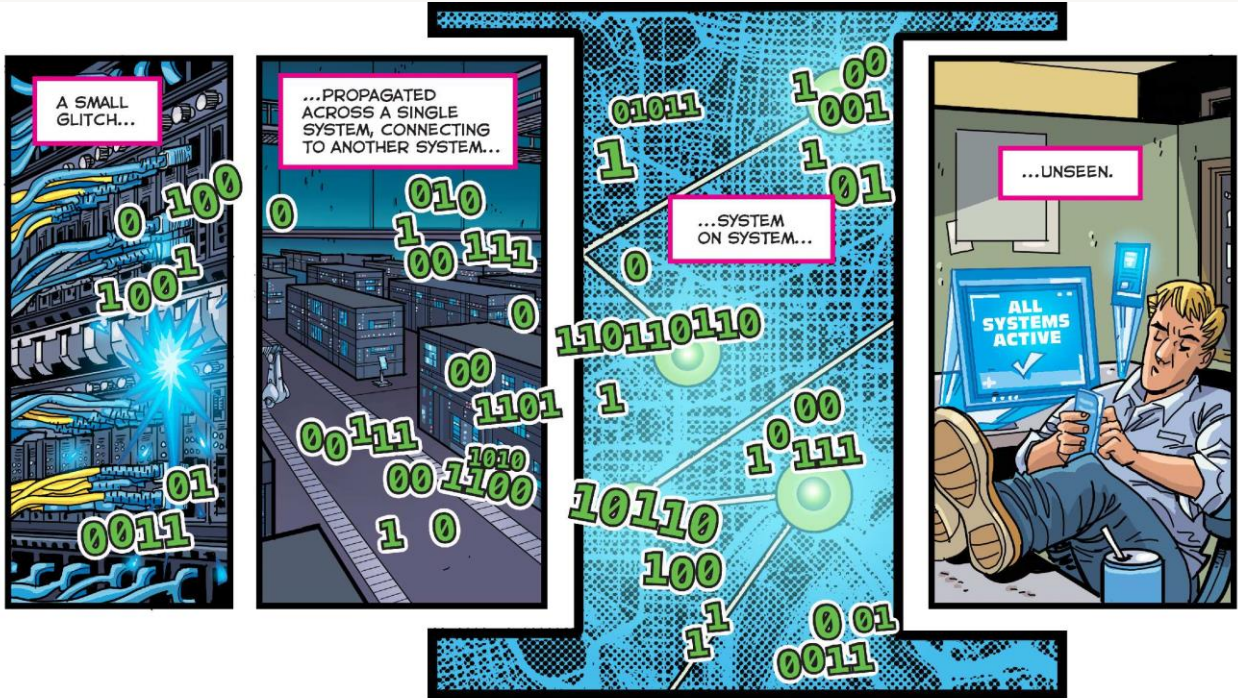
NO ONE WOULD HAVE BELIEVED THAT IN THE MIDDLE OF THE 21ST CENTURY OUR WORLD WOULD BE THREATENED BY UNSEEN FORCES EMBEDDED DEEP WITHIN OUR 6G AND ARTIFICIAL INTELLIGENCE SYSTEMS.

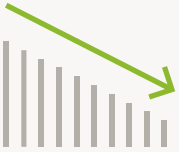


AS PEOPLE BUSIED THEMSELVES ABOUT THEIR VARIOUS BUSINESS, FINANCIAL AND MEDICAL CONCERNS...



...DEEP INSIDE THESE SYSTEMS, NEARLY INVISIBLE TECHNOLOGIES WERE ABOUT TO INCAPACITATE US.





### Inevitable adverse effects

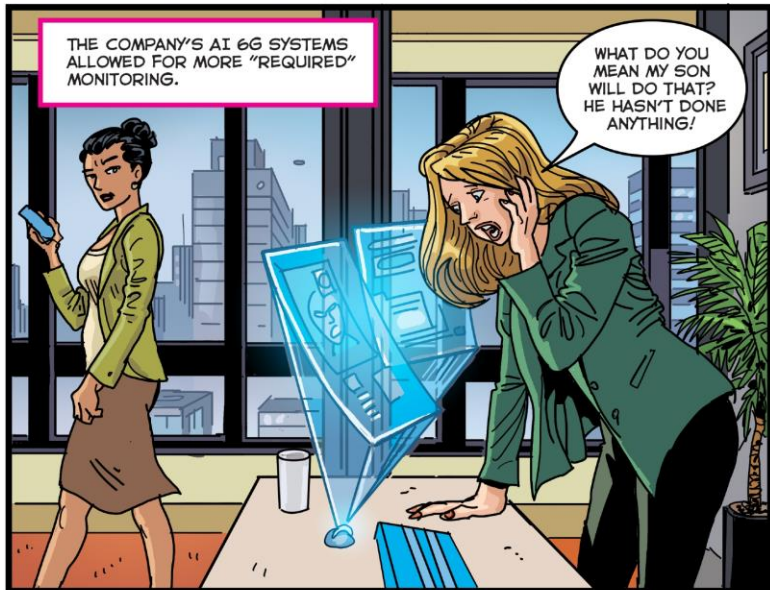
The mass adoption and integration of AI/6G systems into the essential workings of business networks and medical and financial systems will expose businesses, customers and consumers to the high probability of inadvertent harm. Because these systems will be so deeply embedded and unseen, when they fail, even in the smallest ways, they will have an outsized effect.

In this threat space there is no threat actor. The threat will arise from the malfunction of the system or even its very use alone. The pervasiveness and power of the systems will harm businesses' ability to react to emergencies. Additionally, people's mental, physical and financial health will be harmed.

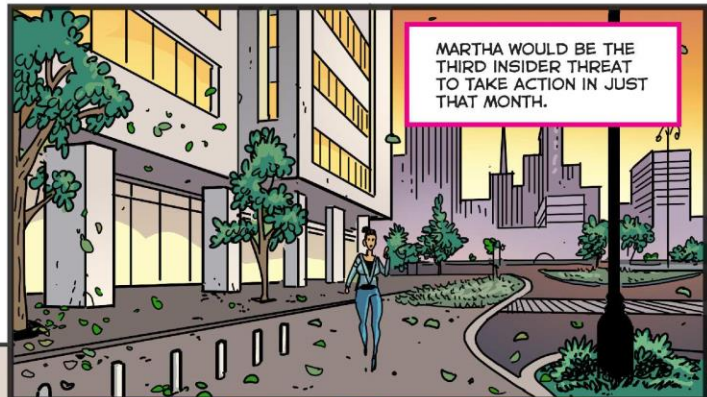
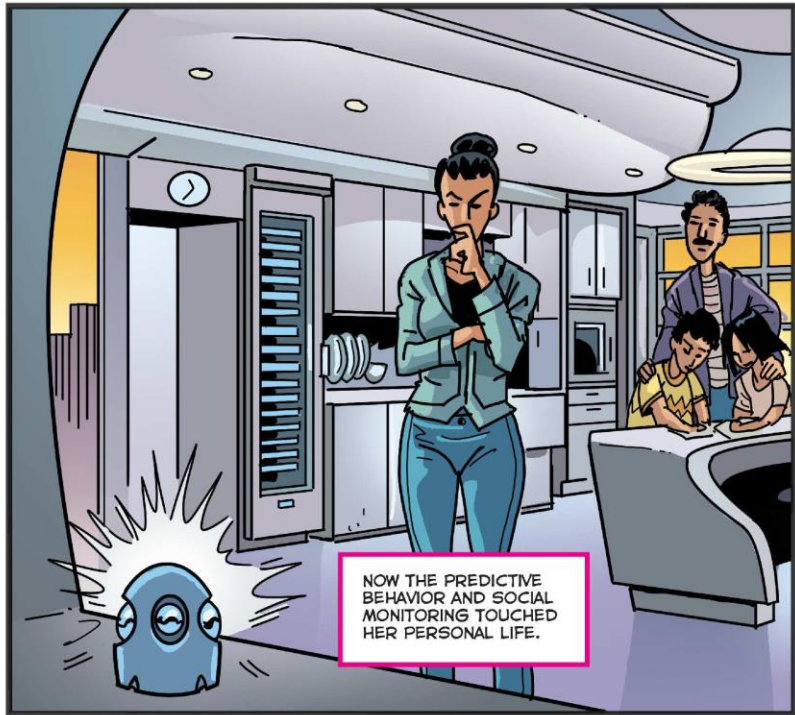


### Example: Threat visualization

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. They are used to make threats visceral and concrete for the reader. The following visualization explores a future where mass adoption and integration of AI/6G systems into the essential workings of business networks, medical and financial systems will expose businesses, customers and consumers to the high probability of inadvertent harm. In this threat space there is no threat actor. The threat will arise from the malfunction of the system or even its very use alone. The pervasiveness and power of the systems will be seen as an overreach by some employees bringing about higher instances of insider threat activities.





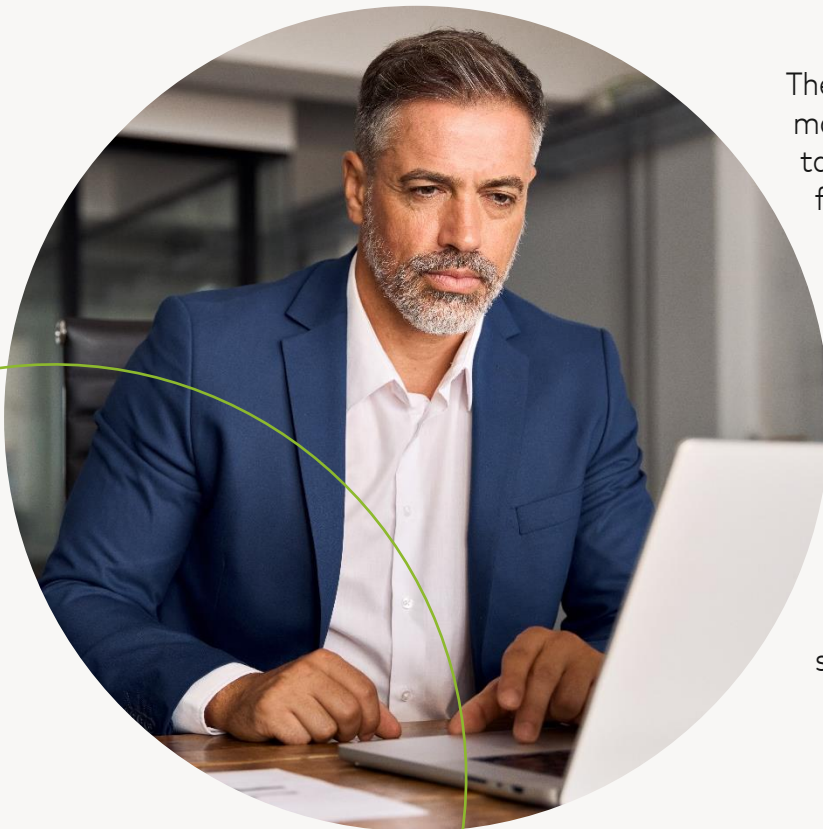
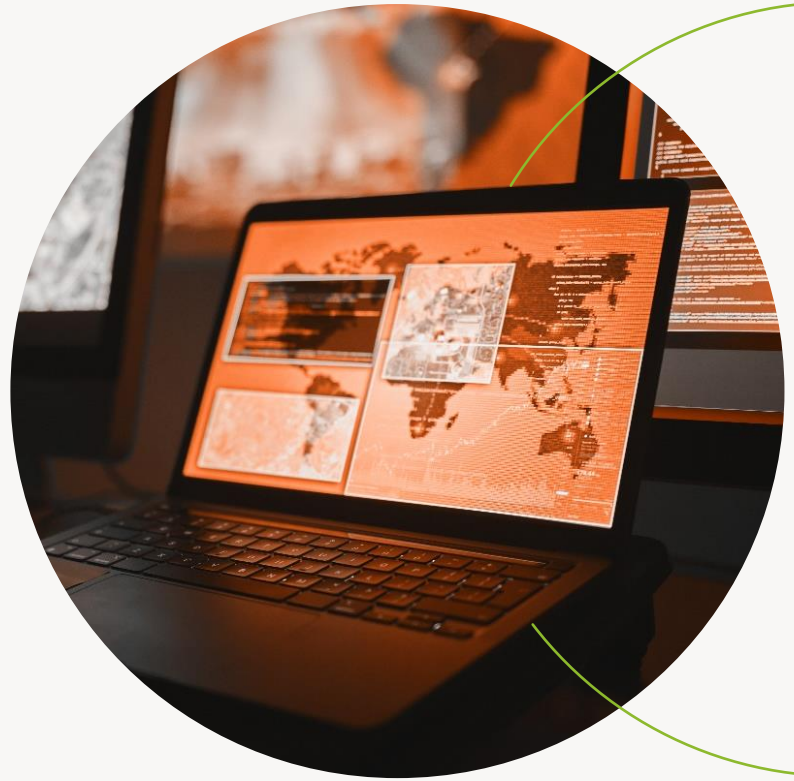




## Nation state attacks

Nation states will utilize AI/6G systems to attack across the spectrum, from consumers to global business networks. The pervasiveness of the systems will allow the attack to move quickly and have a mass catastrophic effect. The targets will include critical infrastructure (energy, financial, communications, transportation) and quickly spread to adjacent systems.

Aside from the initial effects of each critical infrastructure failure, the second- and third-order effects will result in the weakening of business and investor and public trust in these systems.



The use of microtargeting was prevalent throughout many of the threat futures. Nation states were targeting specific individuals as the first strike to a broader attack on nation states or corporations. These threat actors will use the systems to focus on specific individuals by microtargeting them. These high-value individuals (VIPs) could be government officials, business executives or strategically placed individuals (e.g., researchers, people with security access). These microtargeting attacks could also be hidden inside larger smoke-screen attacks on the broader consumer or business population to bring down specific business systems and gain political or economic advantage.

## Seeing the enemies we know in a new light

The 2023 threatcasting exercise identified two ongoing and persistent threats that have been profiled in previous reports. However, through the lens of AI/6G systems, new light was shed on the enemies that we know. The system provided new perspectives on known threats as well as evolutions of these threat spaces.



### Insider threats

AI/6G systems will provide insider threats with a wider attack plane and greater effect. Due to the pervasiveness and unseen nature of the system, a small action will result in mass catastrophic effects.

A new threat space identified by the threatcasting exercise involved the very use of these systems as the cause and incubator of insider threat activities. In this way, the systems were both the cause of the threat and the attack space.

Because the use of these systems will be seen as invasive into public privacy or cheapening the value of an individual's contribution to a nation or organization, they will in fact set down the conditions that will bring about the insider threat. When a person or employee is exposed to the conditions generated by the use of these systems over time, it will first lead to insider threat behavior before advancing to harmful actions.



### Criminal activity

AI/6G systems will provide criminals with a new, wider attack plane to steal from consumers and manipulate them. Criminals are early adopters and fast movers in the new technology space, and they will use these systems before consumers, businesses, law enforcement and militaries understand them.

The specific attack space hinged on the first mover concept originally presented by the SME interviews. Because the adversary will be the first mover, using AI/6G systems in innovative and nefarious ways, both organizations and consumers will not be ready. They will not know they are being attacked because the attack space has yet to be defined. It is the original use of the attack that will define the space. This becomes troubling not only because organizations will not recognize the attack when it is initiated, but also because the misuse of these systems will be the driving factor that defines their use.

In the corporate crime space, these systems will provide organizations with a wider criminal means to gain advantage over competitors through coordinated, rapid and mass attacks. The speed, scope and scale of the attacks will see simultaneous and coordinated attacks that hit multiple vectors such as market manipulation, disinformation and misinformation campaigns, legal actions and executive microtargeting.

# Threat indicators

Threat indicators are meant to give an organization an 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.

## 1 Technical

The primary mover and indicator of threat progression for AI/6G systems will be technological development, adoption and proliferation. This provides us with a host of technological indicators to monitor.

Each of these indicators build off the others, and in many ways, they are additive indicators that could happen sequentially. Seen in this way, an organization can monitor the indicators and begin to take steps to mitigate their effects early in the cycle.

The following indicators were originally outlined in the 2022 Mastercard threatcasting report. They remain relevant for monitoring and tracking emerging threat spaces, including AI/6G systems.



### Artificial Intelligence, machine learning (ML) and autonomous systems

1. Use in industrial applications (e.g., security, banking, fraud detection) 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



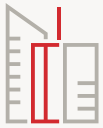
### Biometric adoption

1. Increase in inexpensive devices that can capture biometric data
2. Increase in startups and entrepreneurs integrating biometrics into new product offerings
3. Increase in industry and government (local, national, international) adopting biometrics as a 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 deriving 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 rollout of isolated smart-city technologies (e.g., parking, HVAC and grid management)
2. 5G, 6G and satellite system rollouts
3. Increase of incentives for public/private infrastructure partnerships
4. Continued and increasing infrastructure failures and outages from multiple sources (e.g., natural disasters, climate change and physical attacks)
5. State and national funding for smart infrastructure projects fueled by failures, climate concerns and 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) in specific cities and regions
2. Cost of systems begins to fall
3. Commercial fleets increase in regional areas
4. Local and regional regulators pass legislation to both prohibit and encourage proliferation
5. 5G, 6G and satellite rollout enables expansion
6. Public transportation experiments begin and are tied to smart infrastructure



## Quantum computing and sensors

1. Continued and increasing scientific breakthroughs in academia and industry
2. Leaked information claims that a specific government may have achieved quantum computing
3. Leaked information claims that a specific government may have used quantum computing to break encryption
4. Business and academia achieve viable quantum platform
5. Confirmation that a specific government has achieved quantum computing
6. Commercialization of quantum computing



## Metaverse

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



## Cryptocurrency and blockchain

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

## 2 Adversarial rehearsals and attack testing

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

In other areas, such as terrorism missions, rehearsals are a common indicator that a threat is beginning to manifest. 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. These early targeted spaces could be on less secure or sophisticated targets.

Source: 2. [https://www.rand.org/content/dam/rand/pubs/research\\_reports/RR200/RR215/RAND\\_RR215.pdf](https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR215/RAND_RR215.pdf)

### 3 Threat-specific indicators

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

#### Inevitable adverse effects



##### Early activity

- Small unexplained network and transactional errors outside of standard deviations
- Small indicators or anomalies that quickly turn into insurmountable obstacles and life-threatening situations
- Smart infrastructure ties to AI/6G systems that take anomalous and simultaneous actions



##### Government actions

- Government regulations enacted that allow for more data fluidity across networks
- Increased use of AI from government agencies
- Replacement of existing tech with new systems that is so invasive that it begins to encroach on civil liberties
- Broadening gulf between tech and applicable regulations



##### Business activities

- Industry and solution provider discontinuation of legacy technology to force adoption of new technology and solutions
- Emergence and proliferation of lower barrier of entry to AI-enabled criminal activity
- New emergent AI/6G system-centered tech firms
- Increased use and reliance on AI for essential services
- Businesses and services creating AI as a service (e.g., AI-supervised shopping)

#### Nation state attacks



##### Adoption, usage and anomalies

- Voluminous change to the essential services data usage and movement of data
- The rise of content dichotomy based on geographic area
- Rapid ascent of new AI-powered essential services procedures with little government oversight
- Increase and mainstreaming of consumer-data compensation with no oversight
- Reliance on AI to carry out security operations that cut human staffing costs



## Geopolitics

- Worldwide arms race for the latest AI technologies for essential services to take care of aging populations
- Continued lack of global alignment on enforcement of responsible AI
- Reports of tests and trials for use in essential services
- Rise of larger and more capable AIs trained with national biases by design
- Increase of sophisticated cyberattacks
- Individual compromises of identity/security either through criminal or international attacks (i.e., foreign power targeting a sovereign citizen)

## Insider threats



- In organizations, the rise of higher level, cutting-edge technology mixed with end-of-life and out-of-date products and software
- Multiple sets of risk indicators from users or entities that insider threats may be more active
- Observable known indicators for the progression of individuals becoming insider threats (e.g., changes in human interaction and behavior)
- Continued lack of systems that consolidate indicators to determine true risk profile






© 2024 Mastercard. Proprietary and Confidential.



# 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 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 are four types of action that could be taken to disrupt, mitigate and recover from each the threat futures. The first two threats (inevitable adverse effects and nation state attacks) shared the same high-level categories of actions:

|   |                                     |   |  |   |                  |
|---|-------------------------------------|---|--|---|------------------|
|  | <p>Detection<br/>and protection</p> |  | <p>Intervention<br/>and regulation</p> |  | <p>Education</p> |
|---|-------------------------------------|---|--|---|------------------|

The final two threats, insider threats and criminal activity, have fewer instantiations in the exercise data but do provide some recommended actions.

## Action 1

### Nation state attacks

#### Detection and protection

- Create intrusion detection system and redundancies for critical AI-driven technologies
- Foster public-private partnership and working groups to create and enforce standards
- Develop real-time AI patrol and required buffer period to vet actions for essential services
- Use AI to detect AI bad behavior (AI vs AI)

#### Intervention and regulation

- Prioritize data privacy, ensure that personal data can stay within the user's control
- Increasing cyberphysical defenses of critical infrastructure
- Work with international governments to prevent a global AI monopoly
- Regulate AI (security, privacy, high-risk cases such as medical treatment)
- Develop new consumer protection rules to guard against exploitive data collection and ownership tactics (including creating alternatives to data forfeiture)
- Advocate for stricter regulatory oversight over U.S. technology companies
- Advocate for regulatory development using threatcasting as a norm in educational development
- Foster innovation in the field with the awareness that the technology affects all cross-sector partnerships and governments

## Education

- Create public awareness and education campaigns on interacting with new AI technologies
- Develop education on AI/6G systems that explore how they function and how bias comes about, either intentionally or unintentionally
- Advocate for individual cyber hygiene in an even more connected AI/6G world

## Action 2

### Insider threats

#### Implement

- Access controls (physical and logical barriers)
- Hard-code limitations on transfers or movement of files
- Use data segmentation that limits the amount of data the AI has access to
- Use government oversight of current threat trends and public/private collaboration
- Activate public/private partnerships' formal responses quickly during a crisis
- Spot trends using machine-to-machine flags before adverse events occurs
- Improve investment in DevSecOps; efforts to secure the system development process by integrating security early and throughout the development lifecycle
- "One dirty insider was able to manipulate the code so easily that it is concerning, and there should be more security checks when code is getting deployed."<sup>3</sup>

## Action 3

### Criminal activity

- Employ more human interaction with the critical services personnel to ensure that compromises do not take place or are stopped
- Emphasize and value human interaction so that individuals are able to determine human vs potential AI
- "As the AI will provide a lifelike experience, meaningful moments will become more important in the future."<sup>3</sup>
- Foster education on AI/6G systems with cybersecurity user awareness training

Sources: 3. Quote from SME interview. 4. Quote from SME interview.

# Conclusion

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



## A whole of partner, industry, nation and allies' problem

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. These threats are so expansive and touch so many different sectors that they are in fact a whole of partner, industry, nation and allies' problem.



## 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 are in place and these conversations have been had, 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.



© 2024 Mastercard. Proprietary and Confidential.

